





Implemented





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.



Suggested citation:

ECPAT, INTERPOL, and UNICEF. (2022). Disrupting Harm in Ethiopia: Evidence on online child sexual exploitation and abuse. Global Partnership to End Violence against Children.

Copyright \odot ECPAT, End Violence Partnership, INTERPOL, UNICEF, 2022. Use of this publication is permitted provided the source is acknowledged and that the publication is not used for commercial purposes.

Funding from the Global Partnership to End Violence against Children, through its Safe Online initiative, does not constitute endorsement.

CONTENTS

Foreword	4
Executive summary	6
Disrupting Harm methods	9
About online child sexual exploitation and abuse	13
About Ethiopia - demographics and internet usage	15
Overview of legislation and policy	19
1. Children Online in Ethiopia	23
1.1 Internet access and barriers	24
1.2 Children's activities online	27
1.3 Perceptions and experiences of risky online activities	28
2. Online Child Sexual Exploitation and Abuse in Ethiopia	34
2.1 Law enforcement data	36
2.2 Children's experiences of child sexual exploitation and abuse in Ethiopia	41
2.3 Other experiences of children that may be linked to OCSEA	55
2.4 Insights about victims and offenders from known OCSEA and CSEA cases	58
3. Responding to Online Child Sexual Exploitation and Abuse in Ethiopia	60
3.1 Formal reporting mechanisms	61
3.2 Law enforcement response	64
3.3 Access to justice and remedies	66
3.4 Coordination and collaboration	67
4. How to Disrupt Harm in Ethiopia	68
Acknowledgements	75

FOREWORD

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 <u>General Comment No. 25 adopted in 2021</u>. 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 recorded in the form of digital images or videos, which are very often distributed and 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, it is evermore 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. Such safety by design must be informed by evidence on the occurrence of OCSEA; *Disrupting Harm* makes a significant contribution to that evidence.

The Global Partnership to End Violence against Children, through its Safe Online initiative, invested seven million US\$ in the *Disrupting Harm* project. *Disrupting Harm* uses a holistic and innovative methodology and approach to conduct a comprehensive assessment 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 the now developed and tested methodology be 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 national levels and has resulted in 13 country reports and two regional reports. It provides the comprehensive evidence of the risks children face online, how they develop, how they interlink with other forms of violence and what can be done to prevent and reduce 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, INTERPOL, and UNICEF Office of Research – Innocenti worked in partnership to design and implement *Disrupting Harm* – a research project on online child sexual exploitation and abuse (OCSEA). This unique partnership brings a multidisciplinary approach to a complex issue in order to see all sides of the problem. OCSEA refers to situations that involve digital or communication technologies *at some point* during the continuum of abuse or exploitation; it can occur fully online or through a mix of online and in-person interactions between offenders and children. The *Disrupting Harm* research was conducted in seven Eastern and Southern African countries, including Ethiopia, and six Southeast Asian countries. Data is synthesised from nine different research activities to generate each national report which tells the story of the threat, and presents clear recommendations for action.

While the findings and recommended actions of the *Disrupting Harm* research have relevance for a broad global audience, the desired outcome of this report is to provide baseline evidence for stakeholders in Ethiopia including government, law enforcement, civil society and other stakeholders to effectively tackle OCSEA and strengthen support to children.

Children and caregivers' internet access

One in four children in Ethiopia between the ages of 12 and 17 is an internet user, with 12–13-year-olds much less likely to use the internet (8%) than 16–17-year-olds (46%). There is a clear urban-rural digital divide; on average, 45% of 12–17-year-olds in urban areas were internet users, compared to 21% in rural areas.

The vast majority (98%) of internet-using children who took part in the household survey indicated they accessed the internet using smartphones; very few respondents used computers or tablets. More than half of the internet-using children in Ethiopia owned the devices they used to go online, while 45% of them shared a smartphone with someone else. Younger children were almost twice as likely as 16–17-year-olds to share a smartphone, and girls were more likely than boys to use a shared device.

The household survey indicated that only 13% of internet-using children in Ethiopia could access the internet without any barriers. The main barriers to access included infrastructural obstacles such as a slow connection and poor signal, followed by the high cost of data and limited electricity.

Risky online behaviours

A vast majority of the caregivers who took part in the household survey were highly concerned that their children might talk to unknown people online, or encounter sexual images. Fifty-two percent of caregivers said that talking to unknown people online was 'very risky'. Internet-using children were less likely to be concerned about this with only 26% judging this same behaviour as 'very risky'.

Do children actually engage in these potentially risky behaviours? In the past year, 42% of the internetusing children surveyed added people they had never met before to their contact lists, and 33% of these children shared their personal information with someone they had never met face-to-face.

Crucially, more than 80% of the caregivers had *never* used the internet. The *Disrupting Harm* household survey shows that caregivers generally use the internet much less frequently than their children, which indicates that their ability to guide their child's internet use and mitigate possible risks is limited. A third of caregivers say they would respond by restricting their children's internet access if their child were bothered or upset by something online.

^{1.} Internet users are defined as those who have used the internet in the past three months (n = 5, 938 children).

Two-thirds of internet-using children have not been taught anything about how to stay safe online. Nevertheless, a majority of the children did indicate awareness of risks associated with some online behaviours - they identified that things like sharing personal information and sending sexual images or videos to others, were risky. Yet a minority of these children reported that they had engaged in risky online behaviours during the past year; 14% said they met someone face-to-face after first encountering them online, and 6% had shared naked images or videos of themselves with others online. The most common reason stated by children for sharing naked images or videos was flirting or having fun (like amongst romantic partners). A minority of children had been coerced to share sexual content. Regardless of how sexual content is initially shared, the risk is it being shared further.

Awareness of online child sexual exploitation and abuse

Disrupting Harm engaged a wide range of stakeholders - including government stakeholders. frontline social service providers, law enforcement, and children and their caregivers - to understand the nature and scope of OCSEA in Ethiopia. Findings across all research activities point to quite limited awareness of OCSEA within the country. For example, all nine senior government officials interviewed in Ethiopia noted that while the topic had begun to receive attention, awareness of OCSEA among the public, policymakers, and frontline workers remains very low. The same sentiment was echoed in survey responses from frontline workers. However, government officials that were interviewed suggested possible avenues to improve both the government and the public's knowledge on OCSEA. These suggestions are highlighted throughout the report.

Children's experiences of online sexual exploitation and abuse

In the *Disrupting Harm* household survey, children were asked whether they had been subjected to different forms of online sexual exploitation and abuse within the past year. OCSEA refers to situations that involve digital or communication technologies at some point during the continuum of abuse

or exploitation. Data from the *Disrupting Harm* household survey revealed that in the past year alone, 10% of children internet-using children aged 12–17 in Ethiopia were victims of grave instances of online sexual exploitation and abuse. This includes blackmailing children to engage in sexual activities, sharing their sexual images without permission, or coercing them to engage in sexual activities through promises of money or gifts.

Consistent with the evidence about violence against children offline, people already known to the child were responsible for most instances of OCSEA. Unknown people were responsible for a smaller proportion of these instances (between 2–13% depending on the form of OCSEA in question). This finding has implications for prevention, as online safety activities tend to focus on the threat of harm from strangers rather than people the child already knows.

Disclosure and formal reporting of online sexual exploitation and abuse

The majority of OCSEA incidents go undisclosed and are not formally reported. Approximately 25% of the children who said they experienced an incident in the past year did not tell anyone what happened to them. Of those who did disclose or report what happened, 33% disclosed informally – such as to friends. Almost no one reported to the police or used other formal reporting mechanisms like helplines. Efforts to identify OCSEA cases in the formal justice mechanisms were unsuccessful, confirming that formal reports are not being made, or at least not being received. These findings indicate that these services might not be able to support children, or that children are unaware of their existence.

Indeed, the main barrier to disclosing OCSEA reported by the children in the household survey was a lack of awareness about where to report or whom to tell. Additionally, some children did not report due to feelings of embarrassment or shame, or because it would be emotionally too difficult to recount their experiences. In the frontline service providers survey, respondents unanimously said that OCSEA was not reported because response services, such as the police and hot- and helplines were not trusted.



Scaled to the population, this represents an estimated 300,000 children who were subjected to any of these harms in the span of just one year.



Law enforcement responses

Ethiopia has a police unit with 180 dedicated officers to investigate child sexual exploitation and abuse, but they have not received any specialised training about online forms of these crimes. In response to inquiries made as part of *Disrupting Harm*, Ethiopian law enforcement agencies reported that there were zero cases in police records indicating OCSEA during the 2017–2019 period. Law enforcement participants did provide general data about child sexual exploitation and abuse that it was indicated may include instances where digital, internet or communication technologies were involved – however records do not specifically classify this.

Data from the National Center for Missing and Exploited Children (NCMEC) related to Ethiopia did indicate evidence that OCSEA is a threat in Ethiopia. In fact, in 2019, NCMEC received more than 15,000 CyberTips for Ethiopia from U.S based technology companies. Nearly all of these involved possession, manufacture and distribution of child sexual abuse materials.

Access to Justice

Despite comprehensive efforts to identify a sample, the research team was not able to identify a single child who had accessed justice through the formal justice system for OCSEA-related crimes. Nor was the *Disrupting Harm* team able to identify justice professionals with direct experience working on OCSEA-related cases in the justice system. The consolidated *Disrupting Harm* research data indicates that while it is occurring, it is likely that children who have been subjected to OCSEA have not yet been able to access formal justice mechanisms.

Key insights

The *Disrupting Harm* report for Ethiopia concludes by highlighting four insights from the research:

- 1. In the past year alone, 10% of internet-users aged 12–17 in Ethiopia were victims of grave instances of online sexual exploitation and abuse. This includes blackmailing children to engage in sexual activities, sharing their sexual images without permission, or coercing them to engage in sexual activities through promises of money or gifts. Scaled to the population, this represents an estimated 300,000 children who were subjected to any of these harms in the span of just one year.
- 2. Of the children who were subjected to OCSEA in Ethiopia, very few turn to formal reporting mechanisms like helplines or the police.
- **3.** The justice system has not yet processed any OCSEA cases that could be determined. There is an urgent need for ground-breaking investment in knowledge, capacity and structures for law enforcement and judicial systems to better respond to OCSEA.
- **4.** Important OCSEA-related legislative reform is required to facilitate action.

Taken together, these findings point to a need for stronger institutional support for children who have been affected by OCSEA, as well as increased awareness of OCSEA to help children and families recognise it when it occurs.

The Disrupting Harm in Ethiopia report concludes with a series of detailed set of recommended actions for government, law enforcement, justice, social services, as well as for caregivers, teachers, communities, digital platforms and Internet service providers. These can be found on page 68 of this report.

DISRUPTING HARM METHODS

As with all the settings in which children live and grow, 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 Global Threat Assessment² and a desire to understand and deepen the impact of its existing investments, the <u>Global Partnership to End Violence against Children</u>, through its Safe Online initiative, decided to invest in research to strengthen the evidence base - with a particular focus on 13 countries across Eastern and Southern Africa and Southeast Asia.

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.

Extensive data collection for nine unique research activities took place from early 2020 through to early 2021 and focused on the three-year period of 2017–2019. During an extensive analysis phase, the data from all the research activities were triangulated and a series of 13 country reports were developed. Analysis for Ethiopia was finalised in July 2021. Using the same methods in all 13 countries also allows for cross-country comparisons, which will be presented in the two regional reports in the series.

The desired outcome of this report is to provide a baseline and evidence for Ethiopian policy makers to tackle OCSEA and strengthen victim support. In addition, the findings and recommended actions are expected to have relevance for a broader global audience. The recommendations made in the report are aligned with the WeProtect Model National Response³ and contribute to the 2030 Agenda for Sustainable Development.⁴

Summary of methods used by ECPAT in Ethiopia

Government duty-bearer interviews

Nine interviews with senior national duty-bearers,⁵ whose mandates included OCSEA at a national level, were conducted between July 2020 and September 2020. Due to the COVID-19 pandemic, the interviews were conducted virtually. Contacting the intended sample of 10–12 participants was quite difficult, with some departments non-responsive despite repeated contacts. More information on the method for this activity can be found here, while the preliminary report of the data can be found here. Attributions to data from these respondents have ID numbers beginning with RA1 throughout the report.⁶

Non-law enforcement data collection

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

^{2.} WeProtect Global Alliance. (2018). Global Threat Assessment 2018: Working together to end the sexual exploitation of children online. London: WeProtect Global Alliance.

^{3.} WeProtect Global Alliance. (2016). <u>Preventing and Tackling Child Sexual Exploitation and Abuse: A model national response</u>. London: WeProtect

^{4.} United Nations. (n.d.) <u>Sustainable Development Goals.</u> See: Goals 5.2, 8.7 and 16.2.

^{5.} In this instance, duty-bearers are defined as those who hold specific responsibilities for responding to the risks of OCSEA at a national level. Participants represented: Ministry of Women, Children and Youth, UNICEF Ethiopia, Ministry of Innovation and Technology, Ministry of Education, Federal Attorney General's Office, Federal Supreme court- Child Justice Project Office, Ministry of Culture and Tourism, Cybercrime Unit, UNODC 6. The format RA1-ET-01-A is used for IDs. 'RA1' indicates the research activity, 'ET' denotes Ethiopia, '01' is the participant number and 'A' indicates the participant when interviews included more than one person.

Frontline social service providers' survey

A non-probability convenience sample - obtained by reaching out to a set of NGOs - of 50 clientfacing frontline workers in Ethiopia such as outreach workers, social workers, case managers, psychologists, and some health and legal professionals directly working with children's cases⁷ participated in a survey, administered online between July and October 2020. 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 it and respond to it. While 50 participants were surveyed, the dataset indicated some anomalies at the data cleaning stage, leading to the ultimate exclusion of 17 surveys from the analysis. A total of 33 responses were analysed. The anomalies can possibly be attributed to a lack of understanding of OCSEA and very few reported experiences of supporting OCSEA victims. Additionally, survey administrators suggested that despite being reassured about the anonymity of their responses, participants may have remained concerned about possible surveillance and due to the fear of their answers being linked to them, did not provide detailed responses.8 More information on the method for this activity can be found here, while the preliminary report of the data can be found here. Attributions to data from these respondents have ID numbers beginning with RA3 throughout the report.

Access to Justice and Legal Remedies - interviews with OCSEA victims and their caregivers

This research activity aimed to provide a better understanding of how and to what extent child victims of OCSEA can access justice and remedies in Ethiopia. Ten interviews with 15-18-year-old children and their caregivers were supposed to be conducted. However, despite extensive efforts, the Disrupting Harm study in Ethiopia could not identify any OCSEA victims who had been through the legal system. Efforts to identify a sample included discussions with over 20 national and international civil society organisations, contact with justice professionals and law enforcement officers working with child victims of trafficking and sexual abuse and exploitation. The most likely explanation is that no OCSEA victims have been able to successfully report their experiences. Therefore, data on access to justice for OCSEA victims

is not presented in this report. This limits the ability to triangulate other data points in analysis. However, the inability to identify children who have accessed justice is also a finding in itself, as it displays lack of disclosure by victims and indicates that cases are not recognised as such within the formal justice system.

Access to Justice and Legal Remedies - interviews with justice professionals

Eleven semi-structured interviews with 10 criminal justice professionals were also supposed to be conducted in Ethiopia. The sample was to include State and non-State respondents who had experience with OCSEA criminal cases. As above, despite extensive efforts to identify criminal justice professionals who had experience working with OCSEA cases, the *Disrupting Harm* team could not find any individuals meeting the inclusion criteria. Of the 20 justice professionals contacted, all indicated they had no experience with handling OCSEA cases. Again, the most likely explanation is that OCSEA cases are not yet entering the justice mechanisms in Ethiopia. As mentioned above, the inability to identify participants is a finding in itself.

Literature review and legal analysis

A literature review was undertaken to inform the research teams prior to undertaking the primary data collection. It found that very little published literature existed in Ethiopia that addressed, or even touched on OCSEA. Documents are noted where relevant throughout the report but are particularly sparse – further confirming OCSEA is not yet on the agenda in the country. Comprehensive analysis of the legislation, policy and systems addressing OCSEA in Ethiopia was conducted and finalised in June 2020. More information on the method for this activity can be found here, while the full 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 of the *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). Participants were aged between 16 and 24 but had all been subjected to OCSEA as children.

^{7.} Such as outreach youth workers, social workers, case managers, psychologists, and some health and legal professionals directly working with children's cases.

^{8.} Personal communication with the field team in Ethiopia.

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 method for this activity can be found here. The report presenting the analysis of the 33 survivor conversations will be released separately. Attributions to data from these respondents have ID numbers beginning with RA5 throughout this report and are depicted in separate boxes.

Summary of methods used by INTERPOL in Ethiopia

Quantitative case data analysis

Data was sought on cases related to OCSEA from law enforcement authorities via the INTERPOL National Central Bureau in Addis Ababa. Data was also obtained from the mandated reports of U.S.-based technology companies to NCMEC, and from a number of other foreign law enforcement agencies, with a view to deepening the understanding of relevant offences committed in Ethiopia, offender and victim behaviour, crime enablers and vulnerabilities. Crime data was analysed for the three years from 2017 to 2019. More information on the method for this activity can be found here.

Qualitative capacity assessments

In addition to seeking data on OCSEA-related criminal cases, INTERPOL requested data on the capacity of the national law enforcement authorities to respond to this type of crime and interviewed serving officers. Particular emphasis was placed on human resources, access to specialist equipment and training, investigative procedures, the use of tools for international cooperation, achievements and challenges. Attributions to data from these respondents have ID numbers beginning with RA8 throughout the report. More information on the method for this activity can be found here.

Summary of methods used by UNICEF Office of Research - Innocenti in Ethiopia

To understand children's use of the internet, the risks and opportunities they face online and their specific experiences of OCSEA, a nationally representative household survey was conducted. The target population for the survey was children aged 12–17 who had used the internet in the previous three months. Additionally, one parent or caregiver of each child was interviewed. The term 'household survey' is used throughout the report to indicate findings that come from this specific research activity. The survey

sample was composed of 361 girls (36%) and 638 boys (64%). The age breakdown is as follows: 124 (12%) 12–13-year-olds, 267 (27%) 14–15-year-olds and 610 (61%) 16–17-year-olds were surveyed.

To achieve a nationally representative sample, the household survey used random probability sampling with national coverage. In Ethiopia, fieldwork coverage was 82%. Coverage is defined as the proportion of the total population that had a chance of being included in the survey sample, i.e., the fieldwork would cover the area where they live if sampled. Due to inaccessibility to field teams, the region of Tigray was removed from the list of primary sampling units, along with selected zones within the following regions: Afar, Amhara, Dire Dawa, Oromia, and Somali.

The sampling followed a three-stage random probability clustered sample design. At the first stage, 100 primary sampling units were selected from a list provided by Ethiopia's Central Statistics Agency. At the second stage, 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. At the third stage, individuals (children and caregivers) were selected within each eligible household using random methods.

Interviewers contacted sufficient addresses in each primary sampling unit to achieve ten interviewed households. Each interviewed household consisted of one interview with a randomly selected internet user aged 12–17 and a second interview with their caregiver; delivering a total sample of 1,000 children and 1,000 caregivers. In every household visited (n = 5,928) an attempt was made to collect data on the number of 12–17-year-old children in the household, their gender, and whether they used the internet in the past three months; this allowed for an estimation of internet penetration rates for all 12–17-year-old children in Ethiopia.

Fieldwork took place from 21 December 2020 until 19 January 2021. Data collection was carried out by TRIBOND Research and Consulting PLC, and coordinated by Ipsos MORI on behalf of UNICEF Office of Research – Innocenti. A more detailed explanation of the methodological approach and specific methods used for the analysis of the household survey data can be found here.

Ethical Approval

UNICEF's research protocol was reviewed and approved by the Ethiopian Society of Sociologists, Social Workers and Anthropologists. ECPAT's research protocol was reviewed and approved by the National Research Ethics Review Committee within the Ministry of Science and Higher Education. Additionally, both protocols were reviewed and approved by the HML Institutional Review Board.

INTERPOL assessed the threat of OCSEA and the capacity of law enforcement authorities for responding to this threat. Both assessments entailed interviews with law enforcement officials in relevant

units dealing with OCSEA. The team of interviewers took an online course on <u>Responsible Conduct</u> of Research from the Collaborative Institutional <u>training Initiative</u> and followed the <u>INTERPOL Code</u> of Conduct.

National Consultation

A national consultation took place on 30 September 2021. Government, law enforcement, and nongovernmental organisations were presented with the main findings of this report and asked to comment on the *Disrupting Harm* recommended actions. The objective was to ensure that the recommendations were relevant and feasible for the Ethiopian context.

Figure 1: Disrupting Harm methods in Ethiopia.



ABOUT ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE

Child sexual abuse refers to various sexual activities perpetrated against 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.⁹

Child sexual exploitation involves the same abusive actions. However, an additional element of a threat or of exchange for something (e.g., money, shelter, material goods, immaterial things like protection or a relationship), or even the mere promise of such, must also be present.¹⁰

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 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 technology 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 blurred¹¹ 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.¹²

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.¹³
- 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. While international legal instruments¹⁴ criminalising

^{9.} Interagency Working Group on Sexual Exploitation of Children. (2016). <u>Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse</u>. Bangkok: ECPAT International. 18.

^{10.} Interagency Working Group on Sexual Exploitation of Children. (2016). <u>Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse</u>. Bangkok: ECPAT International. 24.

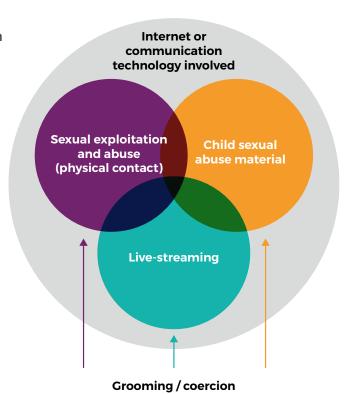
^{11.} May-Chahal, C., & Palmer, C. (2018). Rapid Evidence Assessment: Characteristics and vulnerabilities of victims of online-facilitated child sexual abuse and exploitation. Independent Inquiry into Child Sexual Abuse. UK: Lancaster University.

^{12.} Stoilova, M., Livingstone, S., Khazbak, R. (2021). <u>Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the evidence on children's internet use and outcomes.</u> Innocenti Discussion Papers no. 2021-01, Florence: UNICEF Office of Research - Innocenti.

13. Interagency Working Group on Sexual Exploitation of Children. (2016). <u>Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse</u>. Bangkok: ECPAT International. 40.

^{14.} 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. Section 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. Section 6.

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



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.

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 children¹⁵ 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 children¹⁶ 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 child¹⁷ and unwanted exposure of a child to sexual content¹⁸ are other phenomena which *can* represent 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 purposes 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 used in the *Disrupting Harm* study.

^{15.} 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, vol. 55, 706-716.

^{16.} Interagency Working Group on Sexual Exploitation of Children. (2016). <u>Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse</u>. Bangkok: ECPAT International. 52.

^{17.} Interagency Working Group on Sexual Exploitation of Children. (2016). <u>Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse</u>. Bangkok: ECPAT International. 21.

^{18.} Interagency Working Group on Sexual Exploitation of Children. (2016). <u>Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse</u>. Bangkok: ECPAT International. 44.

ABOUT ETHIOPIA - 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 internet technologies, particularly in low- and middle-income countries. The infographic below summarises the latest data on internet access and social media use in Ethiopia, some of which was gathered directly through the *Disrupting Harm* nationally representative household survey of internet-using 12–17-year-olds.

The data below provide an important backdrop for understanding the various facets of children's internet use. However, methodological limitations affecting data quality for some secondary sources should be kept in mind. Relying on purposive or other non-probability sampling techniques means that the data cannot be considered representative of the population in question. In other cases, variations in data collection methods and definitions of internet use pose a challenge for cross-country comparisons.



POPULATION TOTAL 2019

UN data

112,079,000¹⁸ (2018: 109,224,000)²⁰



FEMALE POPULATION 2019

I INI data

56,010,000²¹ (2018: 54.589.000)²²



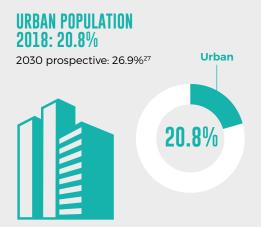
MALE POPULATION 2019

UN data

56,069,000²³ (2018: 54.635.000)²⁴

ETHIOPIA HAS THE 14TH LARGEST POPULATION IN THE WORLD AND IS THE SECOND MOST POPULOUS COUNTRY IN THE AFRICAN CONTINENT, AFTER NIGERIA.²⁵

POPULATION UNDER 18 2018 UN data: 52,244 48%



MEDIAN AGE 2020 **19.5**²⁸



- 19. United Nations Population Division. (2019). World Population Prospects 2019.
- 20. United Nations Population Division. (2019). World Population Prospects 2019.
- 21. United Nations Population Division. (2019). World Population Prospects 2019.
- 22. United Nations Population Division. (2019). World Population Prospects 2019.
- United Nations Population Division. (2019). World Population Prospects 2019.
 United Nations Population Division. (2019). World Population Prospects 2019.
- 25. World Population Review. (2019). Ethiopia Country Profile.
- 26. UNICEF. (2019). The State of the World's Children 2019. Children, Food and Nutrition: Growing well in a changing world. UNICEF, New York.
- 27. 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.
- 28. United Nations Population Division. (2019). <u>World Population Prospects 2019 File POP/5: Median age by region, subregion and country.</u> 1950-2100 (years).

ABOUT ETHIOPIA - DEMOGRAPHICS AND INTERNET USAGE

GDP PER CAPITA 2019 (US\$)

\$855.8°

ETHIOPIA IS ONE THE POOREST COUNTRIES IN THE REGION, BUT AT THE SAME TIME THE FASTEST **GROWING ECONOMY.**30

POVERTY RATES 2015: 23.5%³¹





LANGUAGES

AMHARIC ENGLISH

AMHARIC IS THE WORKING LANGUAGE IN ETHIOPIA.32 BOTH **ENGLISH AND AMHARIC ARE TAUGHT** IN SCHOOLS ACROSS THE COUNTRY.33 INTERNET PENETRATION RATE 2017: 18₋6%³⁴





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



INTERNET USE AMONG CAREGIVERS

16%



n = 1,000 caregivers of internet-using children.

......

Total 12-13 Years 14-15 Years **19**% 16-17 Years 46% **Girls** 21% **Boys 28**% **Rural** 21% Urban

MOST POPULAR DEVICE TO ACCESS THE INTERNET Source: Disrupting Harm data

AMONG 12-17-YEAR-OLDS*

Tablet

Computer





n = 1,000 internet-using children.

*Multiple choice question

n = 5,928 12-17-year-olds in Ethiopia.

16

^{29.} The World Bank. (n.d.). GDP per capita (current US\$) - Ethiopia.

^{30.} World Bank. (2019). Ethiopia Country Profile.

^{31.} The World Bank. (n.d.). Poverty headcount ratio at national poverty lines (% of population) - Ethiopia.

^{32.} Federal Democratic Republic of Ethiopia. (1994). Constitution of the Federal Democratic Republic of Ethiopia.

^{33.} UNICEF. (2016). Ethiopia. The impact of language policy and practice on children's learning: Evidence from Eastern and Southern Africa.

^{34.} International Telecommunications Union. (n.d.). Statistics.

IT ETHIOPIA – DEMOGRAPHICS AND INTERNET USAGE

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

Source: Disrupting Harm data

Mall

Internet café

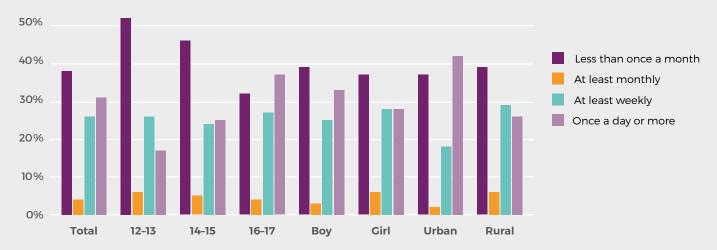




n = 1,000 internet-using children. *Multiple choice question

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

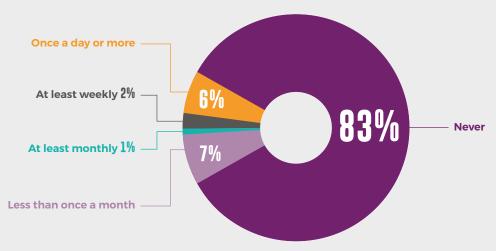
Source: Disrupting Harm data



Base: Internet-using children aged 12-17 in Ethiopia from the Disrupting Harm study. n = 1,000 internet-using children.

FREQUENCY OF INTERNET USE AMONG CAREGIVERS OF INTERNET-USING CHILDREN

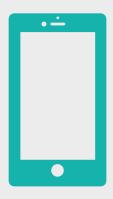
Source: Disrupting Harm data



n = 1,000 caregivers of internet-using children.

ABOUT ETHIOPIA - DEMOGRAPHICS AND INTERNET USAGE

MARKET SHARES IN MOBILE SUBSCRIPTIONS



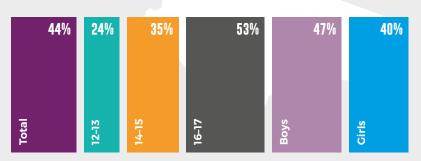
"... ETHIOPIA IS ONE OF THE LAST COUNTRIES IN THE WORLD TO HAVE RETAINED A STATE-OWNED MONOPOLY PROVIDER (ETHIO TELECOM) OF TELECOM NETWORK AND SERVICES." 35

ON 2 APRIL 2021, ETHIOPIA'S FINANCE MINISTRY ANNOUNCED IT HAD RECEIVED TWO BIDS, FOR NEW TELECOMS OPERATING LICENCES.³⁶

ON 2 MAY 2021, THE ETHIOPIAN GOVERNMENT AWARDED A TELECOM SERVICE LICENCE TO THE GLOBAL PARTNERSHIP FOR ETHIOPIA, WHICH IS A CONSORTIUM OF TELECOM COMPANIES.

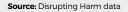
THE COUNTRY'S COUNCIL OF MINISTERS ALSO UNANIMOUSLY DECIDED TO EXPEDITE TASKS THAT WOULD ENABLE THE ISSUANCE OF THE SECOND TELECOM LICENSE THROUGH THE ETHIOPIAN COMMUNICATION AUTHORITY.37

CHILDREN WHO USE SOCIAL MEDIA ON A WEEKLY BASIS

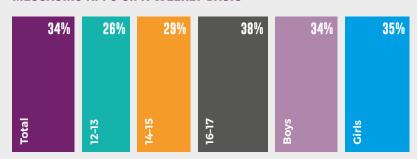


n = 1,000 internet-using children.

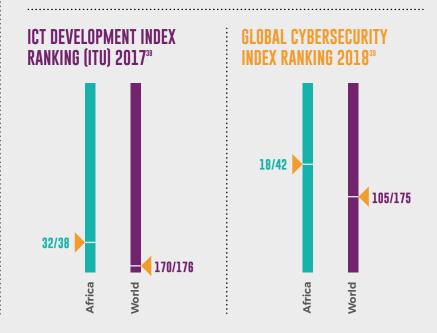
CHILDREN WHO USE INSTANT MESSAGING APPS ON A WEEKLY BASIS



Source: Disrupting Harm data



n = 1,000 internet-using children.



^{35.} Dione, O. (2021, March 21). Why Ethiopia Needs to Open its Telecom Market. World Bank Blogs.

^{36.} Reuters. (2021, April 27). Ethiopia Receives Two Bids for Two Telecoms Operating Licences. Reuters.

^{37.} Getachew, A. (2021, May 22). Global Consortium Wins Ethiopia's Telecom License for \$850M. Anadolu Agency.

^{38.} The ICT Development Index is a composite index that combines 11 indicators into one benchmark measure. It is used to monitor and compare developments in information and communication technology (ICT) between countries and over time.

^{39.} The <u>Global Cybersecurity Index (GCI)</u> is a trusted reference that measures the commitment of countries to cybersecurity at a global level – to raise awareness of the importance and different dimensions of the issue. As cybersecurity has a broad field of application, cutting across many industries and various sectors, each country's level of development or engagement is assessed along five pillars – (i) Legal Measures, (ii) Technical Measures, (iii) Organisational Measures, (iv) Capacity Development, and (v) Cooperation – and then aggregated into an overall score.

OVERVIEW OF LEGISLATION AND POLICY

Overview of legislation and policy

The most relevant pieces of Ethiopian legislation currently in effect regarding sexual offences in general, which also encompass OCSEA-related crimes, are the Criminal Code (2005)⁴⁰ and the Computer Crime Proclamation (2016).⁴¹

Ethiopia's Criminal Code (2005) includes two articles that criminalise a range of conduct related to materials deemed as "obscene or grossly indecent."42 This vague definition is open to interpretation, which might result in the impunity of those responsible for crimes against children. Moreover, the penalty associated with this crime is a simple imprisonment of up to three years. According to the Ethiopian Criminal Code (2005), this type of penalty is applicable to "crimes of a not very serious nature committed by persons who are not a serious danger to society."43 This approach does not take into account the grave nature of crimes related to CSAM. Finally, it is worth noting that by criminalising obscene material in general, the provisions of Ethiopia's Criminal Code (2005) do not only apply to CSAM but also have a much wider applicability to pornographic material depicting adults.

The Computer Crime Proclamation (2016) criminalises a series of acts associated with visual materials depicting minors - or persons appearing to be minors - engaged in sexually explicit conduct.44 The Proclamation partially criminalises online grooming, which it defines as enticing or soliciting minors for sexually explicit conduct by sending them erotic pictures, text messages or videos through computer systems;⁴⁵ and punishes these offences with imprisonment of five to ten years.46 While this covers grooming through explicit sexual communication and potentially also online sexual harassment, the provision does not cover online grooming intended as the establishment of a relationship with a child aimed at enabling sexual abuse online or the organisation of a meeting for sexual purposes.

Crucially, neither the Criminal Code (2005) nor the Computer Crime Proclamation (2016) criminalises online sexual extortion, online sexual harassment or the live-streaming of child sexual abuse. The Criminal Code does contain a provision on the organisation of "obscene or indecent performances in theatres or cinemas, by projection or by radio or television broadcast, by video, or in any other way," 47 but no definition is provided for what constitutes an obscene or indecent performance.

Though there are currently no plans for new laws or amendments that address OCSEA-related crimes, a respondent from the Federal Attorney General's Office shared that there are intentions to assess the legal gaps and challenges in addressing violence against children and women. This assessment will hopefully identify the legal gaps in addressing OCSEA, which would eventually lead to either a new law or a revision of existing laws. The assessment, noted the respondent from the Federal Attorney General's Office (RA1-ET-05-A), would be undertaken in the 2014 (Ethiopian calendar year). The *Disrupting Harm* analysis could provide helpful guidance regarding this assessment and future amendments to Ethiopian legislation.

A number of government agencies were identified during duty-bearer interviews as having responsibilities relevant to OCSEA though none are explicitly mandated to address OCSEA. Relevant agencies included the Ministry of Women, Children and Youth, the Federal Attorney General's Office, the Child Justice Project Office under the Federal Supreme Court, the Federal Police Commission, the Information Network Security Agency, the Ministry of Innovation and Technology, and the Ministry of Education.

Currently, Ethiopia's national budget does not have a line allocated to specifically addressing OCSEA-related crimes. A respondent from the Ministry of Women, Children and Youth indicated that there was budget allocated by the government for child abuse and exploitation in general, however the respondent from this ministry indicated that this budget is

^{40.} Government of Ethiopia. (2005). Criminal Code.

^{41.} Government of Ethiopia. (2016). Computer Crime Proclamation No. 958/2016.

^{42.} Government of Ethiopia. (2005). <u>Criminal Code</u>, Article 640 and 641.

^{43.} Government of Ethiopia. (2005). Criminal Code, Article 106.

^{44.} Government of Ethiopia. (2016). Computer Crime Proclamation No. 958/2016, Article 12.

^{45.} Government of Ethiopia. (2016). Computer Crime Proclamation No. 958/2016, Article 12 (2).

^{46.} Government of Ethiopia. (2016). Computer Crime Proclamation No. 958/2016, Article 12 (2).

^{47.} Government of Ethiopia. (2005). Criminal Code, Article 641.

insufficient and has to be supplemented through fundraising at both federal and regional levels.⁴⁸ (RA1-ET-01-A)

While there are no national policies or plans in place specifically related to OCSEA, the government is reportedly forming a national multi-stakeholder task force on OCSEA. According to the Director of Child Rights Advocacy under the Ministry of Women Children and Youth (RA1-ET-01-A), the formation of this task force is an indication that Ethiopia recognises the need to take action in addressing OCSEA. It also demonstrates that the government is aware that responses to OCSEA require a coordinated multi-agency approach. The appointment of focal persons by three of the mandated agencies - the Ministry of Women, Children, and Youth, Federal Attorney General, and the Ministry of Innovation and Technology - also shows political will from these agencies to play their roles.

Despite these tentative first steps, OCSEA remains a nascent issue on the government's agenda. The government duty-bearers who were interviewed indicated that OCSEA is not yet visible in government discussions on child protection, nor in coordination forums on violence against children, such as the 'National Coordination Body' under the Federal Attorney General's Office. A representative from this office said that "OCSEA has never been part of the agenda of the coordination body. We have a strategy and action plan, and as far as I know, it does not incorporate the issues of online child sexual exploitation." (RA1-ET-O5-A)



The government duty-bearers who were interviewed indicated that OCSEA is not yet visible in government discussions on child protection, nor in coordination forums on violence against children.



In order to be properly prepared to tackle this issue, government duty-bearers require capacity building. Other than a sensitisation session⁴⁹ involving key government ministries carried out by the Ministry of Women, Children and Youth, and a series of regional meetings on OCSEA convened by the African Union in 2019, none of the government duty-bearer respondents were aware of any training for policymakers on identifying or responding to OCSEA.

At government level, there is a child protection workforce in place within the different administrative levels: federal, regional, Zonal and Woreda. ⁵⁰ At the Kebele ⁵¹ level, there is a shortage of child protection specialists, which hinders implementation of child protection measures. According to an interviewee from UNICEF Ethiopia: "UNICEF is supporting the government in creating some form of child protection system. There is a new case management framework for child protection just endorsed in 2019. But who will implement this framework? We don't have a workforce on the ground." (RA1-ET-O2-A)

This gap is partly filled by child protection specialists at the Woreda level, who work with community-based structures and associations to implement activities. Overall, there are between two to five child protection experts per Woreda.

^{48.} The respondent from the Ministry of Women Children and Youth explained that the government has come up with resource mobilisation assistance structures known as Community Care Coalition whose main objective is to mobilise community contributions either in kind or in cash to support vulnerable children within the community. At the national level, he explained that the government budget is supplemented with funds from UN agencies and International Civil Society Organisations.

^{49.} This was a short session that was provided within a workshop organised by Terre des Hommes Netherlands under the Girls Advocacy Alliance project. It was therefore not a specific workshop organised on OCSEA.

^{50.} Woreda are the third level of the administrative division of Ethiopia - after zones and the regional states.

^{51.} Kebele is the lowest administrative unit in Ethiopia.

Awareness of Online Child Sexual Exploitation and Abuse

The current legislative and policy environment in Ethiopia is indicative of limited awareness of OCSEA throughout the country. Low awareness was clearly evident in several *Disrupting Harm* research activities, including the frontline service providers survey in which nearly all respondents (97%, n = 32) described awareness of OCSEA by caregivers and the general public as being 'poor'.

Nine senior government officials interviewed by Disrupting Harm were all in agreement that awareness of OCSEA is very low among the public and also among Ethiopian policymakers and frontline workers. "There is no understanding of online sexual abuse; almost everybody is not aware of it," said one of the duty-bearers, the Director of the Directorate of Women, Children and Youth in the Ministry of Innovation and Technology. (RAI-ET-03-A) A representative of the Federal Attorney General's Office (RA1-ET-05-A) said that policy makers and practitioners working at a technical level are not aware of the types and trends of online abuse, and therefore OCSEA is not reflected in the mandates and programmes of the respective ministries in Ethiopia. The Director of Child Rights Advocacy at the Ministry of Women, Children and Youth (RA1-ET-01-A) stated, "We are not aware; even the responsible government agencies are not aware of this issue. I can say OCSEA is in its infancy stages because it is a recent agenda item for us."

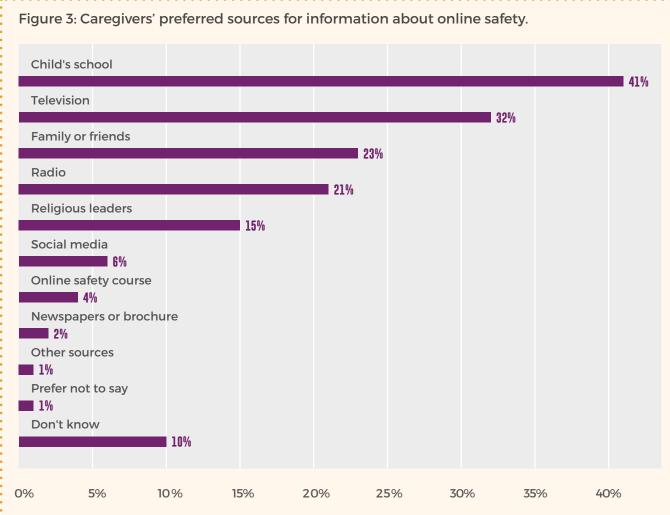
The only ongoing government initiative geared towards building public awareness on OCSEA is an outreach programme by the Ministry of Education on child online safety. Only two out of the nine government officials interviewed were aware of this outreach programme, which was launched about two years ago. A representative from the Ministry of Education indicated this outreach programme targets children and youth, but only those around cities, as they are considered more vulnerable to OCSEA due to higher internet use rates in urban parts of the country.

In the *Disrupting Harm* household survey, only 37% of children said they had *ever* received any

information on how to stay safe online, such as what to do if someone is bothering them online, what content not to share online, and how to change their privacy settings. Children from rural areas were less likely to have received this information than respondents in urban areas (32% rural; 47% urban). As internet connectivity advances across Ethiopia,⁵² the need for preventative outreach on OCSEA with all children – rural and urban – is becoming urgent. As one government official (RA1-ET-09-A) noted: "In future, when internet access will be booming, the problem of OCSEA may rise."

Caregivers can play an important role in keeping children safe both online and offline, but it is difficult to expect them to contribute to the efforts to prevent OCSEA without first building their awareness and understanding of OCSEA. Among caregivers of internet-using children, 22% said that they had *never* received any information or advice on how to help and support their child's internet use or how to keep them safe online. Evidence-based education around digital safety is required to ensure that children – and their caregivers – are equipped with the appropriate tools to benefit from their internet use and successfully manage online risks.

When caregivers who participated in the household survey were asked about their preferred source for information on how to keep their children safe online, 41% of the caregivers said schools should be providing guidance on online safety and 32% wanted to find this kind of information on television (see Figure 3). Based on these findings, the government should consider focusing their awareness raising efforts through these channels, including the expansion of the Ethiopian school curriculum to include online child protection as a pillar. As the interviewee from the General Directorate from the Ministry of Education (RA1-ET-04-A) said, "We have to work on the life skills of the children, on how they can safely use the internet... Within the curriculum, there should be some modification to include this."



Base: Caregivers of internet-using children aged 12-17 in Ethiopia. n = 1,000 caregivers.

The overall lack of awareness in Ethiopia around OCSEA was ascribed by one of the government officials to "the fact that the internet is not accessible everywhere and in every family, [so] OCSEA is therefore not seen as a big problem." (RA1-ET-O3-A) Another respondent, the Head of the Child Justice Project Office in the Federal Supreme Court (RA1-ET-O6-A), said, "most children are in rural areas and have no access to phones, let alone the internet." While internet access and OCSEA are obviously linked, it should be noted that a child does not have to be online in order

to be subjected to sexual exploitation and abuse involving digital, internet or communication technologies. For example, recording the sexual abuse of a child and sharing it online constitutes digitally facilitated abuse, as does live-streaming of abuse. So, while the currently low levels of internet access would imply that a smaller proportion of children in Ethiopia are exposed to abuse that occurs *directly* online (for example, being offered money through social media to engage in sexual acts), lack of internet access does not mean that children are not at risk of OCSEA.

1. CHILDREN ONLINE IN ETHIOPIA

The main focus of the *Disrupting Harm* report series is to present the perspectives of young people and duty-bearers about sexual exploitation and abuse of children that is facilitated or committed through digital technologies. To better understand OCSEA-related offenses in Ethiopia, it is vital to situate them within the wider context of children's internet use. Therefore, this first chapter presents a brief overview of children's internet access and online activities of 12–17-year-olds and then describes the occurrence of riskier online activities and the ways in which these risks are perceived by children and their caregivers.



1.1 INTERNET ACCESS AND BARRIERS

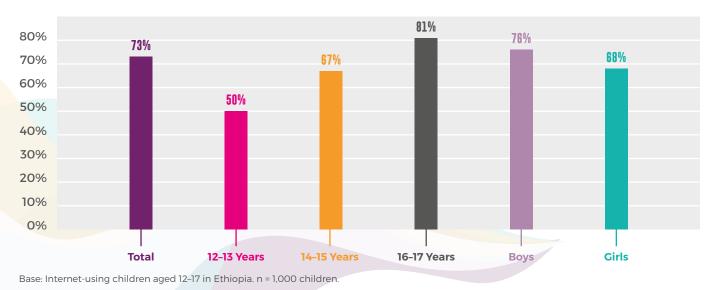
The International Telecommunications Union estimated that 25% of Ethiopians were using the internet in 2019, compared to about 1% in 2011.⁵³ Even after this spike in internet penetration, levels of internet access in Ethiopia are quite low and the country still has a largely unconnected rural population; only cities enjoy 3G access, and 4G is only available in the capital.⁵⁴

As of 2021, 25% of Ethiopian children aged 12–17 are internet users, meaning they have used the internet in the past three months, 55.56 according to the *Disrupting Harm* household survey. Children aged 12 and 13 were least likely to be internet users; only 8% of children in this age group used the internet in the past three months compared to 19% of 14–15-year-olds and 46% of 16–17-year-olds. There was no major difference between genders; 28% of boys were internet users compared to 21% of girls. The data does show a clear rural-urban divide; in rural areas only 21% of 12–17-year-old children accessed the internet, whereas in urban areas 45% of 12–17-year-olds did.

The remaining household survey data presented throughout this report comes from a sample of *internet-using* 12–17-years-olds. Forty percent of internet-using children were low frequency users, meaning they went online less than once a month. As in other countries,⁵⁷ older children – aged 16–17 – were more frequent users and were more likely to go online on a daily basis compared to younger children.⁵⁸ As might be expected, internet-using children in urban areas were more likely to go online *daily* (42%) compared to their peers in rural areas (26%).

More than 80% of the caregivers who participated in the household survey had *never* used the internet. Caregivers aged 29 years or younger were more likely than the oldest caregivers to use the internet on a daily basis (32% versus 3% respectively). As with children's internet use, there were no apparent gender differences in the frequency of use amongst caregivers. This generational gap in digital know-how was identified by the internet-using children; 73% of them said that they knew more about the internet than their caregivers (see Figure 4).

Figure 4: Children who say they knew more about the internet than their caregivers, by age and gender.



^{53.} International Telecommunications Union. (n.d.). Statistics.

^{54.} Bekele, D. (2020, March 4). The First Ethiopia Internet Development Conference: Meeting challenge and opportunity head on. Internet Society.

55. While conducting the random walk to identify eligible children to partake in the main survey, data was also collected 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 the estimation of internet penetration rates for all 12–17-year-old children in Ethiopia. n = 5,938 households.

^{56.} 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.

57. Global Kids Online. (n.d.). Global Kids Online.

^{58.}Global Kids Online. (n.d.). Global Kids Online.

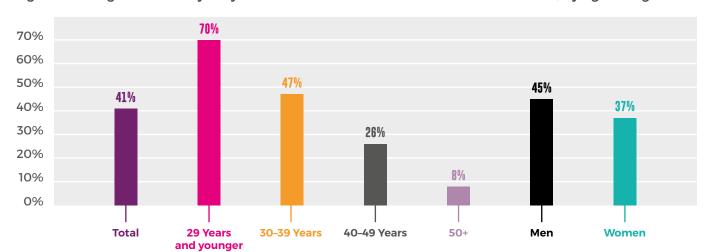


Figure 5: Caregivers who say they knew more about the internet than their child, by age and gender.

Base: Caregivers of internet-using children aged 12-17 in Ethiopia who use the internet. n = 156 caregivers.

As might be expected, older children were more likely to say this than younger respondents. In contrast, only 41% of caregivers said that they knew more about the internet than their children. Younger caregivers were much more likely to say this than older caregivers (see Figure 5). Given older caregivers' limited interaction with the digital environment, it is important to consider the kind of support they might need – from schools and other stakeholders – to effectively guide their children's internet use and help to mitigate risks.

Data collected through the *Disrupting Harm* household survey showed that in Ethiopia, as in most other countries, smartphones were by far the most popular device used by 12-17-year-old internet users (98%), likely due to their relatively lower cost and portability.⁵⁹ Use of other devices such as computers (5%) and tablets (2%) were far less common. There were no notable age or gender differences across all three types of devices. A large proportion of internetusing children in Ethiopia owned the devices that they used to go online, rather than sharing with others. Forty-five percent of children who owned a smartphone shared it with someone else. Younger children (aged 12-13) and girls were more likely to share their smartphone than older children

(aged 16-17) and boys. Rates of device sharing in Ethiopia are lower than those seen in other countries in the region. One reason could be that due to relatively low internet penetration in Ethiopia and the wide disparities in access, the surveyed sample of internet-using children possibly reflected children from families with higher incomes.

While the share of Ethiopians with a mobile subscription leaped from 2% in 2008 to 37% in 2017,60 there are still barriers that limit internet use for children in Ethiopia. Infrastructural obstacles, such as a slow connection or a poor signal, were cited by 40% of internet-using children as barriers that prevent them from going online when they want or need to. This was closely followed by high costs. Despite successive price cuts by Ethio telecom in 2019, findings from an Internet Society report reveal that internet access is still not affordable for the majority of Ethiopians.61

Compared to younger children, 16 and 17-year-olds were more likely to face most barriers to internet access, especially with respect to slow connections and high data costs. This could be because older children want to use the internet more frequently than younger children or engage in more activities online, therefore needing more data.

^{59.} Livingstone, S., Kardefelt Winther, D., & Saeed, M. (2019). Global Kids Online Comparative Report. Innocenti Research Report. UNICEF Office of Research - Innocenti. Florence.

^{60.} International Telecommunications Union. (n.d.). Country ICT data until 2018 - Mobile Cellular Subscriptions.

^{61.} Bekele, D. (2020, March 4). The First Ethiopia Internet Development Conference: Meeting challenge and opportunity head on. Internet Society.

However, younger children were more often restricted in their internet usage by their caregivers or teachers. Caregivers as a barrier to access was more commonly reported by girls (22%) than boys (10%), and the same pattern was repeated for teachers (boys 5%; girls 15%). This means that not only were girls less likely to access the internet in the first place, but those who did faced additional barriers to their active usage.



Infrastructural obstacles, such as a slow connection or a poor signal, were cited by 40% of internetusing children as barriers that prevent them from going online when they want or need to.



Is Restricting Children's Internet Access the Answer?

Many caregivers restrict their children's internet use in a bid to protect them from online risks. In Ethiopia, such restrictive practices appear to be quite common; 32% of internet-using children in the survey reported that they are not allowed to use social media, 37% reported not being allowed to watch videos online, and 15% said that their caregivers often limit the time they can go online. Among the caregivers, 16% said that they would restrict their child's internet access if their child was bothered by something online, and 20% said that they would punish their child.

The restrictive approach might reduce children's immediate exposure to online risks, but it also reduces their digital skills and familiarity with the

online environment. On the other hand, *supportive engagement* by adults of children's online activities has been associated with positive skills development for children in other countries.⁶²

Supportive engagement, which can be practiced also by caregivers who use the internet less frequently than their children, could include doing online activities together, talking to children about their internet use, and educating them about the risks that exist online and how best to mitigate them. In these ways, we allow children to benefit from the many positives that the internet has to offer, while providing guidance and support that can help them navigate online risks to prevent them experiencing harms.

^{62.} Livingstone, S., Kardefelt Winther, D., & Saeed, M. (2019). Global Kids Online Comparative Report. Innocenti Research Report. Florence: UNICEF Office of Research - Innocenti.

1.2 CHILDREN'S ACTIVITIES ONLINE

To learn more about digital experiences, children were asked about the kinds of activities they like to engage in (see Figure 6). Social activities such as using social media, instant messaging and speaking to family and friends were the most popular among internet-using children in Ethiopia. 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 school work. Nonetheless, Figure 6 below provides a greater understanding of how 12-17-year-olds in Ethiopia use the internet and the activities they enjoy. Notably online gaming is relatively rare. Common barriers to internet use, such as high data costs or slow connections could explain why children do not engage in this potentially bandwidth-heavy activity. Another explanation could be that 50% of children said that their caregivers do not allow them to play games with other people online.

There were not many differences in the types of online activities that children engaged in across age groups, except for using social media and instant messaging apps, which were more popular among older children. This is again a departure from findings in other countries, where older children are more likely to engage in a wider range of online activities than younger children.

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

Online activities	Total	12-13	14-15	16-17	Boy	Girl
Used social media	44%	24%	35%	53%	47%	40%
Used instant messaging	34%	26%	29%	38%	34%	35%
Talked to family or friends who live further away	27%	25%	21%	30%	25%	30%
Watched videos	26%	33%	21%	26%	28%	22%
Searched for new information	24%	11%	20%	28%	25%	21%
School work	20%	10%	18%	24%	21%	19%
Looked for news	20%	19%	13%	23%	23%	14%
Participated in a site where people share their interests	20%	13%	15%	23%	21%	18%
Followed celebrities and public figures on social media	18%	15%	18%	19%	20%	15%
Looked for health information	16%	13%	17%	17%	17%	14%
Looked for information about work or study opportunities	15%	9%	13%	17%	15%	14%
Looked for information or events in local neighbourhood	14%	7 %	14%	15%	17%	9%
Sought emotional support		11%	12%	15%	14%	12%
Watched a live-stream	13%	7 %	12%	14%	13%	12%
Played online games	10%	16%	12%	9%	11%	8%
Discussed political or social problems		6%	7 %	10%	9%	8%
Created a blog or website	6%	4%	5%	6%	6%	4%
Created their own video or music	5%	5%	6%	5%	5%	4%

Base: Internet-using children aged 12–17 in Ethiopia. n = 1,000 children.

^{63.} Livingstone, S., Kardefelt Winther, D., & Saeed, M. (2019). <u>Growing up in a Connected World</u>. Innocenti Research Report. Florence: UNICEF Office of Research – Innocenti.

1.3 PERCEPTIONS AND EXPERIENCES OF RISKY ONLINE ACTIVITIES

Discussion of online risks often hinges upon adult-centric perceptions. To ensure we also 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

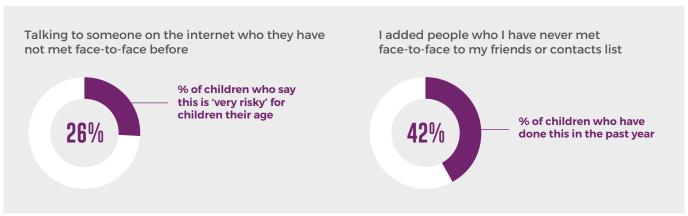
A common concern noted by the internet-using children and their caregivers is exposure of children to unknown people online. When asked to rate the level of risk related to several online behaviours, 52% of caregivers and 26% of children said that talking to people online whom they had never met in person was 'very risky' for children. In contrast, 34% of children said that this was not risky at all, while 16% were not sure if this was a risky behaviour.

Similarly, 69% of caregivers and 39% of internetusing children agreed that children sending personal information – such as full name, address or phone number – to someone they had never met in person was 'very risky', but nearly 25% of children said that sharing personal information was not risky at all, and 12% were unsure if this carried a risk. Younger children were more likely than older children to describe this activity as not risky at all. An in-person meeting with someone unknown whom they first met online was perceived as 'very risky' for 57% of caregivers and 30% of internet-using children. However, another 28% of the children judged this as 'not risky at all'. These numbers may suggest the need for awareness raising about these potentially risky behaviours in order to mitigate these becoming experiences of harm.

How do children's perceptions match their behaviours? In the past year, 42% of children added people they had never met before to their contact lists; and 25% of children shared their personal information with someone they had never met face-to-face.

Furthermore, internet-using children were asked, "in the past year, have you ever met anyone face-to-face that you first got to know on the internet?"⁶⁴ Eighteen percent (n = 183) said that they had met someone in person whom they had first got to know online.

Figure 7: Children's assessment of risk in speaking to unknown people versus children who added strangers to their contacts in the past year.



Base: Internet-using children aged 12–17 in Ethiopia. n = 1,000

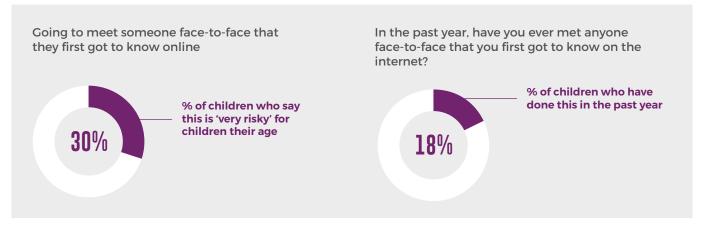
^{64.} This question could capture a range of scenarios - from offline meetings with distant relatives or friends of friends whom the child first met online, to meeting an adult in person as part of the grooming process.

Figure 8: Children's risk assessment of sharing their personal information with unknown people versus children who have engaged in this behaviour in the past year.



Base: Internet-using children aged 12-17 in Ethiopia. n = 1,000

Figure 9: Children's assessment of risk in meeting people in person that they first got to know online versus children who had engaged in this behaviour in the past year.



Base: Internet-using children aged 12-17 in Ethiopia. n = 1,000



Internet-using children were asked, "in the past year, have you ever met anyone face-to-face that you first got to know on the internet?" Eighteen percent (n = 183) said that they had met someone in person whom they had first got to know online.



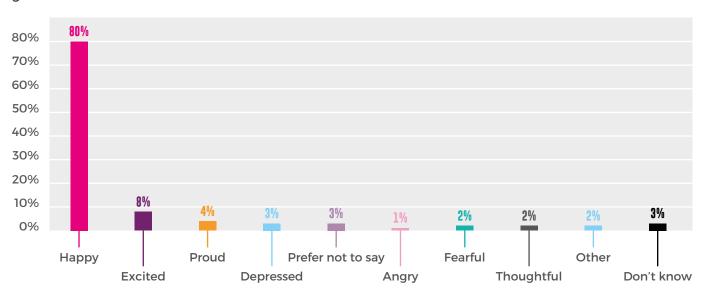


Figure 10: How children felt the last time they met someone face-to-face whom they had first got to know on the internet.

Base: Internet-using children who met someone face-to-face that they first got to know online in the past year. n = 183 children.

Among these 183 children, the vast majority characterised the experiences as positive indicating that the risk of harm from meeting someone they did not first know was relatively low. A large majority (over 80% or 146 children) reported feeling happy about the encounter, and 14% were excited (see Figure 10). Girls were less likely than boys to engage in this behaviour. Research done across more than 30 countries around the world has produced similar findings.^{65,66} However, it must be noted that if harm occurs in these circumstances, it can be very severe. There are many different types of such encounters, like connecting with new children in the community or going to group events with caregivers. But these meetings could also be with ill-intentioned offenders. Educating children and their caregivers of these risks is essential.

1.3.2 Seeing sexual content online

In the household survey, 58% of children and 81% of caregivers said that seeing sexual images or videos on the internet was very risky for children. Similarly,

when frontline workers in Ethiopia were asked to select risk factors of OCSEA, all 33 respondents agreed that access and exposure to pornography increased children's vulnerability to OCSEA.

A third of children in Ethiopia saw sexual content online at least once in the past year, according to the household survey. One in five children reported actively looking for sexual images or videos online, and 27% said they saw this type of content online by accident. Among the children who saw sexual content by accident, more than one third said that they came across this content on social media (35%), 17% were sent it via direct messages, 18% saw them in online advertisements, and 13% encountered it when conducting online searches. Older children were more likely than younger children to have seen sexual content in advertisements. Girls were more likely than boys to say they saw sexual content online by accident (29% girls, 23% boys). On the other hand, boys were more likely than girls to report purposely seeking sexual content online (22% boys; 16% girls).

^{65.} Livingstone, S., Kardefelt Winther, D., & Saeed, M. (2019). Global Kids Online Comparative Report. Innocenti Research Report. Florence: UNICEF Office of Research - Innocenti.

^{66.} Smahel, D., Machackova, H., et al. (2020). EU Kids Online 2020: Survey results from 19 countries. Florence: UNICEF Office of Research - Innocenti.

Figure 11: Children's risk assessment of seeing sexual content online versus children who have actively looked for this type of content in the past year.



Base: Internet-using children aged 12-17 in Ethiopia. n = 1,000

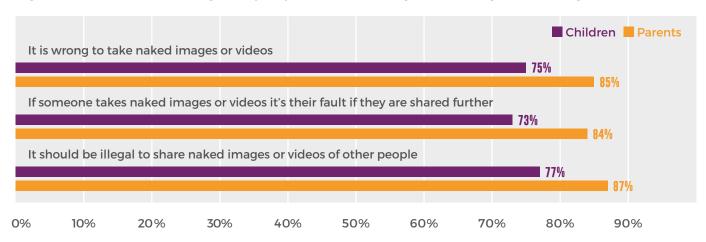
1.3.3 Making and sharing self-generated sexual content

Most of the children and caregivers surveyed said that they believed "it is wrong for a person to take naked images or videos of themselves." In addition, 81% of caregivers and 60% of children thought it was 'very risky' for children to share a sexual image or video with someone online. As shown in Figure 12, most said that they believed that it should be illegal to share someone's naked images or videos with others; and the Ethiopian Criminal Code does in fact does criminalise the distribution and circulation of any type of obscene materials, which based on judicial interpretation might include any type of sexual images.

Around 8% of internet-using children in Ethiopia reported taking naked pictures or videos of themselves during the past year. This figure could also be under-reported due to fear of stigma or common discomfort to discuss sex and producing sexual content.

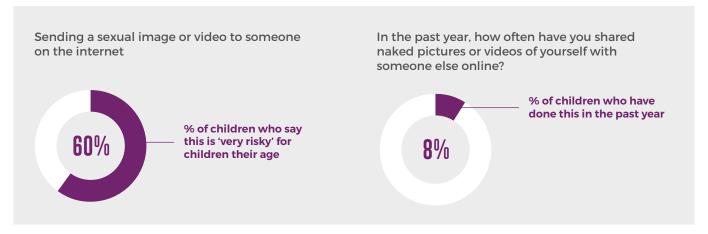
Boys and younger children were slightly more likely than girls and older children to take naked pictures or videos of themselves in the past year. Relatedly, 6% of children reported allowing someone else to take naked pictures or videos of them during the past year. While this is concerning and could be an indication of abuse or exploitation, these instances could also have occurred between trusted peers (though even in these circumstances the risk of unwilling on-sharing remains).

Figure 12: Children and caregivers' perspectives on taking and sharing naked images or videos.



 $Base: Internet-using\ children\ |\ Caregivers\ of\ internet-using\ children.\ n=1,000\ children\ |\ 1,000\ caregivers.\ n=1,000\ children\ |\ 1,000\ caregivers\ children\ children\$

Figure 13: Children's assessment of risk in sharing sexual content online versus children who have engaged in this behaviour in the past year.



Base: Internet-using children aged 12-17 in Ethiopia. n = 1,000

The research data also showed that concerningly, 11% of children pressured someone their age to send them sexual pictures or videos in the past year. This suggests an urgent need to teach children about consent. Forty-eight percent of children surveyed said that they had received sex education. As might be expected, the oldest children were most likely to have received this. Beyond teaching children how to be assertive and say no if they do not want to engage in sexual activities, these sex education classes were most likely to cover topics such as sexually transmitted diseases, morality (what is right or wrong for the child in relation to sex) and contraception.

Within this subsample of 75 children, the motivations to share sexual images of themselves included being in love (n = 18), flirting and having fun (n = 18), or trusting the other person (n = 11). However, a few children revealed some concerning reasons for sharing this kind of content. For instance, five children did so because they were threatened, and three children did so because their friends were pressuring them.



The research data also showed that concerningly, 11% of children pressured someone their age to send them sexual pictures or videos in the past year.



Within the subsample of 75 children, 30 children (40%) shared naked images or videos of themselves with a current or former romantic partner. Fifteen children (20%) shared with someone they first met online who had some other connection with their life (e.g., was a contact of a family member or friend). Fifteen percent, or 11 children, shared self-generated sexual images with a friend or someone they knew in person, and three children (4%) shared naked images or videos of themselves with an unknown person who had no other connection to their life.

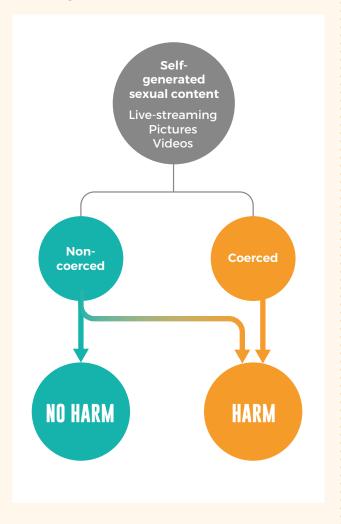
The Rise in Self-Generated Sexual Content Involving Young People

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. Forms of behaviour that are increasingly normative to young people can be bewildering for adults who grew up in a different time. For instance, chatting and video live-streaming is common, whether among small private groups of friends or large, anonymous public audiences. While much of this is harmless, producing and sharing self-generated sexual content using these tools is also increasing and bringing significant risks.⁶⁷

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. Such exchanges are increasingly becoming part of young people's sexual experiences. However, the data also show that the creation and sharing of self-generated sexual content can be coerced through threats or peer pressure (see <u>chapter 2.2</u>).

While coercion can clearly be seen as a crime and leads directly to harm, 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 risk remains 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 circulated by offenders perpetually (see Figure 14).^{68,69}

Figure 14: Mapping the consequences of sharing self-generated sexual content involving children.



2. ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE IN ETHIOPIA

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 Ethiopia. The chapter draws on a variety of sources – including law enforcement data, mandated reports from U.S.-based technology companies to NCMEC related to Ethiopia, surveys with frontline workers and conversations with children themselves, as well as the household survey – in order to create a well-rounded presentation of the nature of these crimes against children.



This chapter presents national law enforcement data related to OCSEA (chapter 2.1), followed by estimates of the occurrence of certain instances of OCSEA based on children's self-reported experiences (chapter 2.2 and 2.3). The purpose of these estimates is not to provide a conclusive picture of the prevalence of OCSEA. There are several reasons for this. Firstly, the existing administrative data accessed, such as that kept by law enforcement authorities, rarely delineates or classifies OCSEA elements. Secondly, with respect to the household survey, one would expect a degree of under-reporting due to privacy concerns, hesitation to discuss sex and sexuality as well as fear of legal self-incrimination as some practices are criminalised. Furthermore, in households where sexual abuse occurs, it is less likely to be given permission to talk to the children in such a survey. Finally, many estimates are based on analysis of sub-samples of the household survey data, which are small because OCSEA is still a rarely reported phenomenon. These smaller sub-samples result in a larger margin of error.

While the *Disrupting Harm* team is confident in the data and the quality of the sample obtained, the challenges of researching these specific and sensitive phenomena, particularly with children, means 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 incidence of certain crimes against children related to OCSEA in Ethiopia and the extent to which internet-using 12–17-year-old children in Ethiopia are subjected to OCSEA.



Ethiopian law enforcement sources reported that zero OCSEA-related cases were recorded in 2017, 2018 and 2019.



2.1 LAW ENFORCEMENT DATA

The analysis in this chapter draws on qualitative and quantitative data from law enforcement authorities and several partner organisations, with a view to understanding relevant offences, offender and victim behaviours, crime enablers and vulnerabilities.

2.1.1 Recorded OCSEA-related offences

Ethiopian law enforcement sources reported that zero OCSEA-related cases were recorded in 2017, 2018 and 2019. Analysis in this chapter is therefore reliant on complementary data sources, including law enforcement statistics for the more general category of CSEA offences. Between 2017 and 2019, there was a 283% increase in CSEA cases. Data supplied by law enforcement sources did not distinguish between different types of CSEA offences.

2.1.2 International OCSEA detections and referrals

On behalf of Ethiopian law enforcement, data was requested for *Disrupting Harm* from NCMEC on CyberTips concerning suspected child sexual exploitation in Ethiopia.⁷⁰

After a year-on-year increase of 234% in 2018, CyberTips for Ethiopia declined by 54% in 2019. While a percentage increase in 2018 of 53% is not dissimilar to the global increase of CyberTips worldwide (66%), the sharp reduction in Ethiopia in 2019 was more marked than the global average (8%).⁷¹ Inclusion of public data for 2020 indicates that numbers for 2018 may have been something of an anomaly. Ethiopia's proportion of the global total number of CyberTips has been consistently low (average of 0.12%) and lower than might be expected, given that Ethiopia accounted for 1.45% of the world's population, and 0.53% of the world's internet-using population according to International Telecommunications Union estimates.⁷²

Figure 15: Number of CSEA/OCSEA cases recorded by law enforcement in Ethiopia.

Department of Special Investigations (DSI)	2017	2018	2019
Number of CSEA cases	147	186	563
Number of OCSEA cases	0	0	0

Base: Data provided by INTERPOL National Central Bureau Addis Ababa.

Figure 16: CyberTips concerning suspected child sexual exploitation in Ethiopia.

	2017	2018	2019	2020	% CHANGE 2017 to 2018	% CHANGE 2018 to 2019	% CHANGE 2017 to 2019	% CHANGE 2019 to 2020
Ethiopia	9,838	32,824	15,054	17,451	234%	-54%	53%	16%
Global Total	10,214,753	18,462,424	16,987,361	21,751,085	81%	-8%	66%	28%
Ethiopia % of Global Total	0.10%	0.18%	0.09%	0.08%				

Base: CyberTip data supplied by NCMEC.

70. U.S. federal law requires that U.S.-based Electronic Service Providers report instances of suspected child exploitation to the CyberTipline of NCMEC. 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 prevalence of OCSEA on a number of platforms popular in the focus countries.

^{71.} The reduction in reports in 2019 was observed in many countries and is to a large extent explained by improvements to electronic service providers' reporting procedures, including the ability to attach multiple files to a single report.

^{72.} International Telecommunications Union. (n.d.). <u>Statistics.</u>

Ethiopian law enforcement received CyberTips through the INTERPOL National Central Bureau in Addis Ababa. The data above stand in contrast to the zero OCSEA cases recorded by Ethiopian law enforcement, raising possible questions over how CyberTips from NCMEC are processed in Ethiopia.

Analysis of the types of incidents captured by CyberTips reveals that the possession, manufacture and distribution of CSAM (referred to in U.S. legislation as "child pornography") accounts for almost all of the CyberTips for Ethiopia in the reporting period.

Figure 17: CyberTips concerning suspected child sexual exploitation in Ethiopia, by incident type.

Incident Type	2017	2018	2019
CSAM, including possession, manufacture and distribution (NCMEC classification: child pornography) ^{73,74}	9,838	32,821	15,052
Travelling child sex offences (NCMEC classification: child sex tourism) ⁷⁵	0	0	2
Child sexual molestation	0	1	0
Misleading words or digital images on the internet	0	2	0
Ethiopia Total	9,838	32,824	15,054

Base: CyberTip data provided by NCMEC.

Figure 18: CyberTips concerning suspected child sexual exploitation in Ethiopia, by reporting electronic service provider.

Reporting Electronic Service Provider	2017	2018	2019	% of 2019 Total
Facebook	9,817	32,756	14,829	98.51%
Google	8	32	133	0.88%
Instagram, Inc.	8	30	79	0.52%
WhatsApp Inc.	_	2	4	
SmugMug-Flickr	_	_	3	
Hacker Factor	_	_	2	
Tagged.com	-	-	2	
Tumblr	_	-	2	
4chan community support LLC	_	1	_	
Chatstep	2	-	_	
Yahoo! Inc.	3	-	_	

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

^{73.} The terminology used in this column reflects classification by NCMEC in line with U.S. legislation. *Disrupting Harm* advocates use of the term child sexual abuse material, in line with the <u>Luxembourg Guidelines</u>.

^{74.} 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.

^{75.} The terminology used in this column reflects classification by NCMEC in line with U.S. legislation. *Disrupting Harm* advocates use of the term travelling child sex offences, in line with the <u>Luxembourg Guidelines</u>.

CyberTips classified as relating to CSAM increased in 2018 and declined in 2019. The overall increase between 2017 and 2019 was 53%. In terms of priority level, NCMEC tagged zero reports for Ethiopia as Priority 1, the level that indicates a child is in imminent danger.

All but three of the CyberTips for Ethiopia in the period of 2017 to 2019 had electronic service providers as their source. A total of 11 electronic service providers submitted at least one CyberTip of suspected child exploitation for Ethiopia in the reporting period. This would indicate less diversity in the platforms misused by OCSEA offenders compared to some other *Disrupting Harm* countries, and perhaps also in usage by the general population.

While Facebook accounts for the same proportion of CyberTips for Ethiopia in 2019 as in the reporting period as a whole (99%), the number of CyberTips submitted by Facebook in 2019 were less than half than the previous year. Smaller but persistent increases are observable in CyberTips from Google and Instagram. The two CyberTips from Tagged. com speak to the misuse of adult dating sites for suspected distribution of CSAM. Appearance in the data of the anonymous image-based bulletin board 4chan, and the digital forensics research company Hacker Factor indicates that, while the number of these CyberTips is small in comparison to those from social media and search providers, there are some OCSEA offenders in Ethiopia with a level of technical sophistication and specialist interest.

Telegram

The data from both interviews with government officials interviews and the household survey confirmed that Telegram is particularly popular in Ethiopia in comparison to other messaging apps like WhatsApp, which are more popular in other African countries. As detailed in chapter 2.2.1, a high proportion of Ethiopian children say that they received requests to talk about sex or send sexual content via Telegram; this was not the case in other *Disrupting Harm* target countries.

Of note is that Telegram does not report to NCMEC - as it is not a U.S.-based electronic service provider, it is not required to.

The popularity of Telegram in Ethiopia could explain the app's prominence in Ethiopian children's experiences of OCSEA. Additional information from law enforcement and other frontline workers is needed.

CyberTips for Ethiopia also permit analysis of headline statistics for unique Internet Protocol (IP) addresses used to engage in suspected child sexual exploitation.

Figure 19: CyberTips concerning suspected child sexual exploitation in Ethiopia, number of unique upload IP addresses by year.⁷⁶

	2017	2018	2019	% Change 2017-2019	% Change 2018-2019
Ethiopia Unique Upload IP Addresses	1,815	3,664	3,527	94%	-4%
Total Ethiopia Reports	9,838	32,824	15,054	53%	-54%
Reports per Unique IP Address	5.42	8.96	4.27	-21%	-52%

Base: CyberTip data provided by NCMEC.

^{76.} Please note: the same IP address may be counted in more than one year, and a report can contain more than one unique IP address. Technical measures by Internet service providers including the dynamic assignment of IP addresses and the sharing of IP version 4 addresses across a large number of devices can also have an impact on the number of unique IP addresses logged.

An IP address is assigned to each individual device on a specific network at a specific time. Multiple reports per IP address can indicate that suspects (or at least their devices) are engaged in multiple offences of CSAM distribution during the same online session. Ethiopia registers comparatively high average numbers of IP addresses per report, which suggests a tendency of offenders to upload multiple items of CSAM in a detected session, indicating a more deliberate style of offending.

Finally, one foreign law enforcement agency reported sending two referrals to Ethiopia related to online child sexual exploitation offences in the period 2017–2019.⁷⁷ Referrals from foreign law enforcement agencies are most often made when an ongoing investigation is found to involve an offender or victim in the second country, or when a domestic service provider makes a report to the national law enforcement authority that is indicative of OCSEA in the second country. Since the data requirement for this project did not include systematic collection of data concerning OCSEA referrals from all law enforcement agencies outside Ethiopia, it is possible that there have been additional international referrals in the reporting period from other foreign law enforcement agencies.

2.1.3 Evidence of CSAM from other sources

Hosting: Ethiopia has not been identified as a hosting country for images and videos assessed as illegal by INHOPE member hotlines contributing to the ICCAM platform. Moreover, the Internet Watch Foundation actioned zero reports concerning confirmed CSAM hosting in Ethiopia in the calendar years 2017, 2018, and 2019. 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 evidence of an absence of CSAM hosting in the country.

Distribution on peer-to-peer networks: The Child Rescue Coalition operates the Child Protection System for detecting distribution of CSAM on peer-to-peer file sharing networks. Data supplied for the time

period 9 June 2019 to 8 June 2020 reveals that seven Ethiopian IP addresses were identified as engaged in peer-to-peer distribution or downloading (see figure 20). Since the Child Protection System does not monitor all file sharing networks, this should not be taken to be representative of the sum total of CSAM offending on such platforms. Representation of data for Ethiopia alongside that for other *Disrupting Harm* study countries in Africa allows for comparison:

Figure 20: CSAM distribution and downloading from *Disrupting Harm* focus countries, observed on peer-to-peer file sharing networks by the Child Rescue Coalition.

	IP Addresses	Globally Unique Identifiers (GUIDs)
Ethiopia	7	4
Kenya	76	24
Mozambique	6	10
Namibia	94	117
South Africa	2,413	842
Tanzania	47	5
Uganda	4	4

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

CSAM distribution on the monitored peer-to-peer networks would appear to be much less popular in Ethiopia than in several other *Disrupting Harm* study countries. In as much as data supplied by NCMEC indicates several thousand instances of suspected CSAM possession, manufacture and distribution in Ethiopia in 2017, 2018 and 2019, it would appear that Ethiopian CSAM offenders may prefer globally popular U.S.-based platforms to peer-to-peer (P2P) file-sharing networks.

Web Searches for CSAM: Research was conducted on Google Trends⁷⁹ with a view to identifying levels of interest in CSAM in Ethiopia. In the first instance, a sample of 20 terms selected by the INTERPOL

^{77.} INTERPOL requested data and qualitative insights from a number of foreign law enforcement agencies with intelligence on or outreach activities in the focus countries. In line with intelligence handling protocols and data protection requirements, some of these sources have been anonymised.

^{78.} For more information on the ICCAM project, see: International Association of Internet Hotlines: What is ICCAM and Why is it Important?.
79. 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) for relative popularity based on the ratio of searches using the selected term or string to the total number of searches using all terms/strings within the geographical and time parameters set. For more information on data and scoring, see "FAQ about Google Trends data".

Crimes Against Children team served as keywords and phrases for specialist interest in CSAM. Queries for the time period 1 January 2017 to 31 December 2019 on searches in Ethiopia returned a result of 'not enough data' for each of these 20 terms.

Returns of 'not enough data' equate with a O relative popularity score, indicating a comparatively low level of interest in that term (as opposed to absolute O search volume) within the geographical and time limits set. When compared to global searches for the same terms and those from other countries in the same time frame, this suggests that specialist CSAM search terms may be used less in Ethiopia than they are 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 search is still used for CSAM discovery.

Less specialist, more 'entry level' searches related to CSEA were popular in Ethiopia in the reporting period, including English language searches for image and video content depicting sexual activity with and between teenagers, with children, and with babies. Related searches for particular formats such as 'high-definition video', 'amateur', self-produced material, and for material recording familial abuse appear to indicate that some web searchers in Ethiopia have specific requirements reflective of a more persistent and active interest in CSAM that has progressed beyond initial curiosity.

Because individuals in Ethiopia looking for CSAM may search in languages other than English, use of local language and slang search terms presents a key knowledge gap. There is therefore an opportunity for law enforcement to review OCSEA investigations in Ethiopia, with a view to identifying additional terms and search strings used by offenders. The results above nevertheless appear to demonstrate that there is demand for CSAM in Ethiopia, and the open web is used for its discovery.



Data supplied by NCMEC indicates several thousand instances of suspected CSAM possession, manufacture and distribution in Ethiopia in 2017, 2018 and 2019.



2.1.4 Links to travel and tourism

Data on travelling child sex offenders can provide an indication of OCSEA, as these offenders often record their sexual abuse or exploitation of children for their own use or for further distribution. Online facilitation of CSEA by travelling offenders has been observed through the use of communications technology to groom or procure children for offline abuse, or to maintain an online relationship with children whom the offender has already abused offline.

Convicted sex offenders in a number of countries are required to notify a central authority of overseas travel. Analysis of data supplied by one foreign law enforcement agency reveals that between 2015 and 2020 there were nine notifications to national sex offender registries concerning travel to Ethiopia, representing just 0.13% of total notifications in that period, and 14% of notifications in the *Disrupting Harm* focus countries in Africa.⁸⁰ A second agency reported that out of 283 notifications of convicted sex offender travel from May 2017 to June 2020, 0.5% were destined for Ethiopia.

The U.S. Homeland Security Investigations' Angel Watch Centre provides referrals to officials in destination countries on convicted U.S. child sex offenders who have confirmed scheduled travel. Those confirmed as not being admitted into the destination country are counted as 'denials'. In the fiscal years 2017 to 2020, it made five referrals concerning travellers to Ethiopia, representing 4% of the total number of referrals to *Disrupting Harm* focus countries in Africa in those years. However, the agency did not receive confirmation that any of these individuals were denied entry to the country.

80. INTERPOL requested data and qualitative insights from a number of foreign law enforcement agencies with intelligence on or outreach activities in the focus countries. In line with intelligence handling protocols and data protection requirements, some of these sources have been anonymised.

2.2 CHILDREN'S EXPERIENCES OF CHILD SEXUAL EXPLOITATION AND ABUSE IN ETHIOPIA

Under the *Disrupting Harm* project, OCSEA was defined specifically to include online grooming of children for sexual purposes, CSAM and the live-streaming of child sexual abuse. These concepts are used in this chapter to organise and present the research findings. At the same time, it must be recognised that the ways in which children are subjected to OCSEA are often far more complex and nuanced. The experiences or offences in question often occur in combination or in sequence. Moreover, 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.

2.2.1 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 occur either completely online or via a combination of online and in person.

Online grooming is a complex process which is often fluid and difficult to detect, especially where it involves a slow building 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 or appear 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 following section focuses primarily on children's experiences of various facets of online grooming as captured in the household survey of internet-using 12–17-year-olds. 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 add up to over 100%.

Legislation on grooming

The Ethiopian Computer Crime Proclamation criminalises the enticement or solicitation of minors for sexually explicit conduct by transmitting or sending erotic speeches, pictures, text messages or videos through computer systems; and punish these offences with rigorous imprisonment of five to ten years.^{81,82} This legislation covers "sexually explicit communication" online with a child for the purpose of enabling sexual abuse.

Potential grooming - children asked to talk about sex

In the past year alone, 12% of internet-using children participating in the household survey in Ethiopia were asked to talk about sex or sexual acts with someone when they did not want to; there were no notable differences by age or gender. Depending on the context, these experiences could mean varying levels of harm for a 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 indicate malicious instances of attempted grooming – thus why it is described as instances of potential (versus actual) grooming.

Online or offline? Of the 120 children in the household survey who had received unwanted requests to talk about sex within the past year, 59 said that this happened online. Only those 59 children who said that this happened online – on social media *or* in an online game – were included in the subsequent analysis, as these instances represent potential OCSEA cases.

Children who received unwanted requests for sexual talk on social media (n = 49) were most likely to be targeted through Facebook or Facebook Messenger and Telegram.

How children felt: Seventy-one percent of the children who received unwanted requests to talk about sex or sexual acts through online channels disclosed feeling negatively about the experience. In comparison, 28% said this did not affect them at all. Younger children were much less likely to be affected by such encounters compared to older children (67% 12-13 vs. 27% 16-17).

^{81.} Government of Ethiopia. (2016). Computer Crime Proclamation No. 958/2016, Section 3, Article 12 (2).

^{82.} There are two types of imprisonment in Ethiopia: simple and rigorous. The rigorous imprisonment is applicable only to crimes of a very grave nature committed by criminals who are particularly dangerous to society. Besides providing for the punishment and for the rehabilitation of the criminal, this sentence is intended also to provide for strict confinement.

I HAVE BEEN ASKED TO TALK ABOUT



THE LAST TIME THIS HAPPENED ONLINE...



Whom did you tell?**

Friend

3%

Helpline

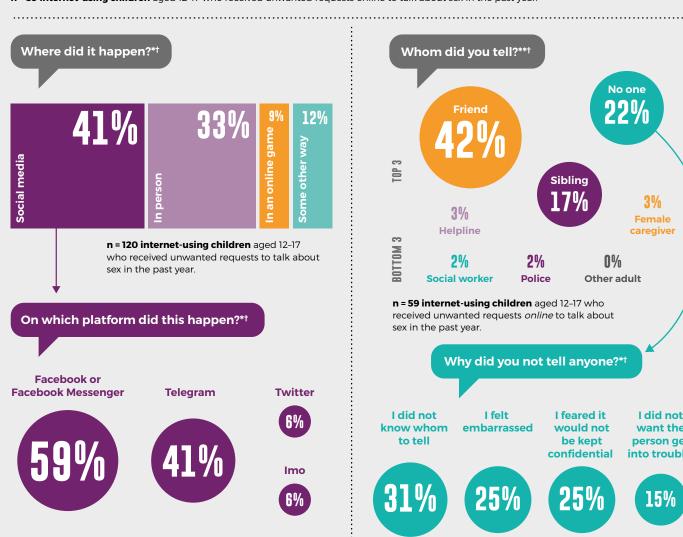
2%

Social worker

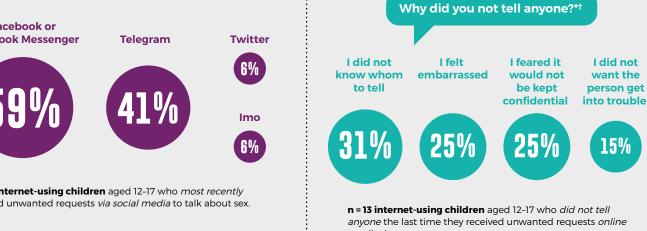
sex in the past year.

TOP 3

n = 59 internet-using children aged 12-17 who received unwanted requests online to talk about sex in the past year.



n = 49 internet-using children aged 12-17 who most recently received unwanted requests via social media to talk about sex.



to talk about sex.

22%

0%

Other adult

3%

Female

caregiver

Sibling

2%

Police

n = 59 internet-using children aged 12-17 who received unwanted requests online to talk about How children responded: Of the 59 children in the sample who were asked *online* to talk about sex when they did not want to, over half refused to comply. Some of the most common responses were pro-active, for example, blocking the person or asking the other person to leave them alone. Other common responses were avoidance-based; such as ignoring the problem and hoping it would go away, avoiding using the internet for a while (7%), and deleting any messages from the other person (2%). However, a small proportion of children (9%) did as they were asked even though the request was unwanted.

Who made the requests: Children were most likely to be targeted with unwanted online requests to talk about sex by someone they already know; most often a current or former romantic partner, followed by a friend or acquaintance who is 18 years or above, family members, and a friend or acquaintance under 18 years of age. Around 38% of children said they received these requests from an unknown person,⁸³ while 7% of children did not want to answer this question.

Whom children tell about it - if anyone: When considering how to tackle and respond to OCSEA, formal reporting mechanisms - covered in chapter 3 of this report - are key issues. The data collected by Disrupting Harm in Ethiopia indicate that 57% of the full sample of internet-using children did not know where to get help if they or a friend were subjected to sexual assault or sexual harassment. Indeed, the experiences of children subjected to sexual violence in the past year reveal that they rarely report their experiences through official mechanisms.

Among the subsample of children who had received unwanted online requests to talk about sex in the past year, only one child used online mechanisms to report what had happened, while two children reached out to a hotline and one child reported to the police. Twenty-two percent of children in this subsample did not talk to anyone about what had happened. Among the 31 children who did not tell anyone the last time this happened, their main reasons were a lack of awareness of whom to tell and feeling embarrassed or ashamed.

Five of these children did not think what happened to them was serious enough to report, and five were concerned their story would not be kept confidential.

When children disclosed to someone about being targeted with unwanted online requests to talk about sex, it was most likely be with friends or siblings, and less likely to be with adults (see page 42). On the occasions that they did disclose to adults, the most likely confidants were male caregivers (14%), then teachers (12%). While boys and girls in the sample were equally likely to be asked to talk about sex, it was more likely that children (both girls and boys) shared their experience with their father or other male caregivers (14%) compared to mothers or female caregivers (3%).

Only 36% of children were confident that they knew how to report harmful content on social media. This finding, which was quite consistent across age and gender groups, is concerning considering that many internet-using children use social media (44%) or instant messaging (34%) apps on at least a weekly basis where they may encounter this risk.

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 they also intend to meet the child in person or not. Global action to address online grooming of children with the sole intent of getting them to send sexual images or videos of themselves (and not meet) has been slow.84 In 2015, amid concern about this issue, the 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."85

^{83.} This figure combines two mutually-exclusive responses selected by respondent: 'Someone I didn't know before this happened' and 'I don't know who the person was.'

^{84.} Interagency Working Group on Sexual Exploitation of Children. (2016). <u>Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse</u>. Bangkok: ECPAT International. 50.

^{85.} Council of Europe's Lanzarote Committee. (2015). Opinion on Article 23 of the Lanzarote Convention and its explanatory note. Para 20.

The children who took part in the household survey were asked if, in the past year, they received a request "for a photo or video showing their private parts when they did not want to." While these data could capture relatively harmless sharing of such images among peers, it could also point to attempts to manipulate children into self-generating and sharing sexual images or videos through digital technologies. Within the past year, 8% of the internet-using children (84 children) surveyed in Ethiopia had received unwanted requests for a photo or video showing their private parts.

How children felt: Similar to children who were asked to *talk* about sex, children who were asked to send sexual images when they did not want to, were most likely to feel embarrassed or not affected at all. Referring to their last experience being asked for sexual images, children also expressed feeling angry (11%), guilty (10%), and distressed (10%).

Interviews with survivors of OCSEA in other Disrupting Harm countries illustrated that confusion was a common response to unwanted requests online. One survivor from Cambodia recalled not being sure if what was being asked was acceptable or not: "We did talk to each other and brought up why he took photos like that. But we didn't know. We didn't know why he took photos or understand. Sometimes my friend said, 'he took photos with half my body pointed upwards,' like that, and we didn't really care, and another thing, we didn't know that taking photos like that made us... made us... sometimes we thought a lot, is it wrong or right?" (RA5-CA-02) Another survivor experienced a gradual realisation that what was happening was wrong: "I got to think of that how he was ruining me especially after I realised that what he was doing was wrong, I didn't realise that before then." (RA5-NA-02-A)

How children responded: Of the 84 children who received unwanted requests to send sexual images or videos, 45% refused, 10% ignored the problem, 10% tried to get the other person to leave them alone, and 7% stopped using the internet for some time. This aligns with how children responded to unwanted requests to talk about sex. The similarities in responses could be because children were asked to talk about sex *and* to send sexual images in the same encounter. Fourteen percent (n = 12) of the children who received these requests complied.

Who made the requests: Children were most likely to receive unwanted requests for sexual content of themselves from a romantic partner, followed by a family member, friends or acquaintance 18 years or above, and a friend younger than 18 (12%). Eighteen percent of children said they received the request from someone unknown to the child, while 14% did not want to answer this question. Overall, children are more likely to receive unwanted requests – to share sexual content of themselves or talk about sex – from people they already know, rather than by someone unknown to the child.

Online or offline? Children who were asked to send sexual content were more likely to be targeted with these requests online – through social media and/ or online games – than in person. The most common social media platforms through which requests for sexual images or videos occurred were Facebook or Facebook Messenger and Telegram; other platforms mentioned by children included Twitter (12%), Imo (12%) and YouTube (12%).

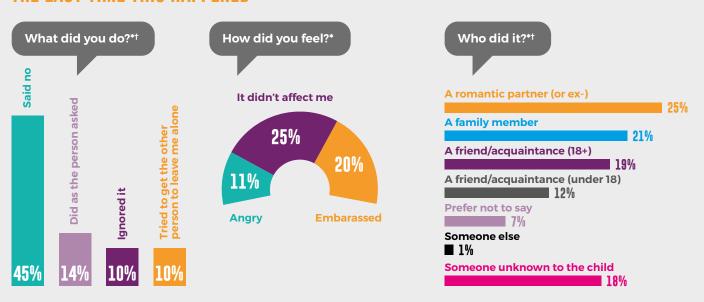
Whom children tell about it - if anyone: One in three children spoke to a friend the last time they were asked for sexual *images or videos* and very few told an adult about their experience; 27% did not share their experience with anyone (n = 23). This data reveals a concerning pattern where children are relying on themselves or children their age to understand how to navigate these situations and cope with the negative consequences that might arise from complying with these requests. For the 23 children who were asked to send sexual images when they did not want to and did not disclose this request to anyone, the main barrier was by far a lack of awareness around where to go or whom to tell, while some kept this experience to themselves because they felt they had done something wrong.

I WAS ASKED FOR A PHOTO OR VIDEO SHOWING MY PRIVATE PARTS WHEN

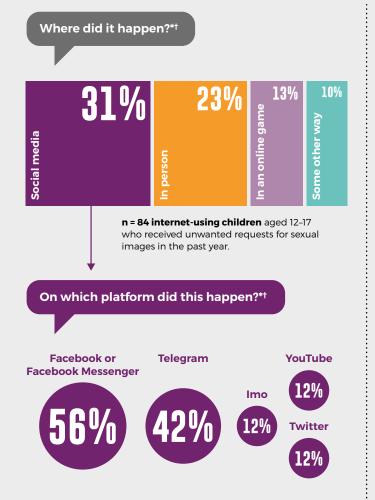


.....

THE LAST TIME THIS HAPPENED



n = 84 internet-using children aged 12-17 who received unwanted requests for sexual images in the past year.



n = 26 internet-using children aged 12–17 who *most recently* received unwanted requests for sexual images via social media.



[&]quot;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



n = 23 internet-using children aged 12-17 who did not tell anyone the last time they received unwanted requests for sexual images.

Based on children's testimonies it is clear that unwanted requests are a problem that exists for some internet-using children in Ethiopia. Taken together with the lack of reporting, this suggests that children may not be adequately equipped with the knowledge needed to recognise some risky scenarios and know what to do if they are being harmed.

Building awareness among children and equipping them with the knowledge and skills to avoid or navigate such situations is a multi-sectorial effort and a joint responsibility. One possible avenue to address this problem is to develop school curricula that cover OCSEA and how it manifests, as well as digital skills and reactive measures such as blocking contacts or reporting inappropriate behaviour online.

When teaching children about the diverse risks that exist online, highlighting the importance of consent and the possible risks that can arise – particularly from sending sexual images of themselves or others – is vital. Furthermore, given that most of these requests were sent on a social media platform, there is a clear need for those platforms to detail – in child-friendly terms – what children should do when subjected to any form of harm or sexual abuse online, such as how to report or disclose to a trusted adult. These platforms have a duty to respond rapidly when receiving reports about possible child sexual exploitation and abuse, which should possibly be mandated by law.

A survivor from Malaysia emphasised the need for a more open conversation between adults and children about sexual experiences: "I just feel people should talk about it more, and caregivers should have these conversations with their kids from a younger age; like [saying] 'When a guy starts doing, acting like this to you, it's not because they are being nice to you, it's not because they care. It's because they are trying to take advantage of you' – and things like that ... I think the next generation [of parents must] do a better job at raising kids and having these conversations with them." (RA5-MY-01-A)

Offering children money or gifts for sexual images or videos

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. A total of 74 children – 7% of internet-using children surveyed in Ethiopia – said that during the past year they were offered money or gifts if they provided sexual images or videos of themselves. There were no notable age or gender differences among this group of children.

Who made the offers: According to the children who were subjected to this during the past year, these offers were most likely to come from people in their immediate circle; for more than 25% of children who had been offered money in exchange for sexual images or videos the offender was a family member, followed closely by romantic partners, friends or acquaintances 18 years or older, and friends or acquaintances under 18 years of age. Twenty-two percent of children said that an unknown person offered them money or gifts for sexual images or videos.

Online or offline? As with other forms of OCSEA covered in this chapter, the unwanted requests were most commonly delivered to children through online channels However, 22% of children said this happened to them in person and 16% said they received requests through another type of medium. Given the sensitivity of the topic at hand it is understandable that this question had a relatively high non-response rate (27%). The 15 children whose most recent experience being offered money for sexual images or videos happened via social media said that these encounters occurred on Facebook or Facebook Messenger, Telegram, Twitter, Imo and Line (7%).

Whom children tell about it - if anyone: Among the 74 children, 33% told a friend about their experience the most recent time this happened and 6% told a sibling. In comparison, 16% confided in a parent or caregiver (father 11%; mother 5%) and 9% turned to a teacher for help.

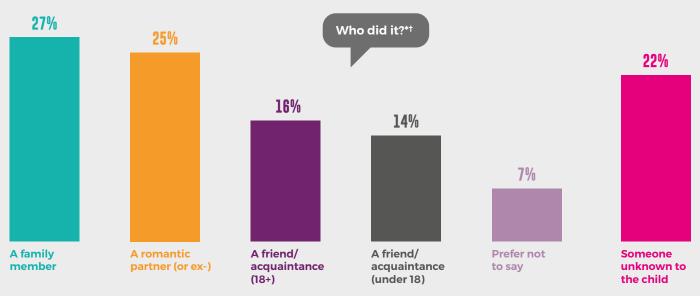
Nearly 25% of the children who were offered money or gifts in return for sexual images or videos did not disclose to anyone; the main barriers to reporting mentioned by these 17 children were lack of awareness around where to go or whom to tell and feeling embarrassed. Almost no children reported the incident to helplines (n = 1), social workers (n = 1),

IN THE PAST YEAR

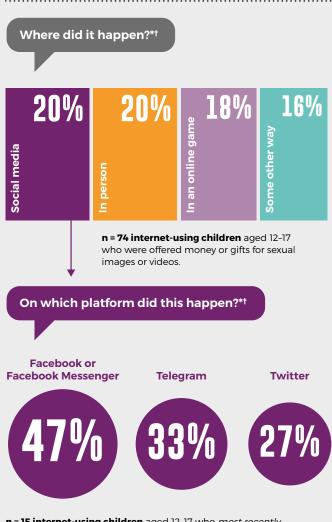
I WAS OFFERED MONEY OR GIFTS IN RETURN FOR SEXUAL IMAGES OR VIDEOS



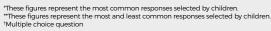
THE LAST TIME THIS HAPPENED...

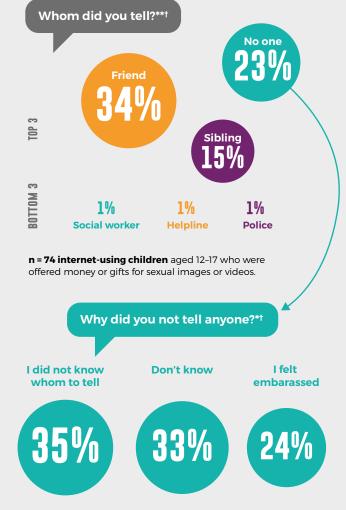


n = 74 internet-using children aged 12-17 who were offered money or gifts for sexual images or videos.









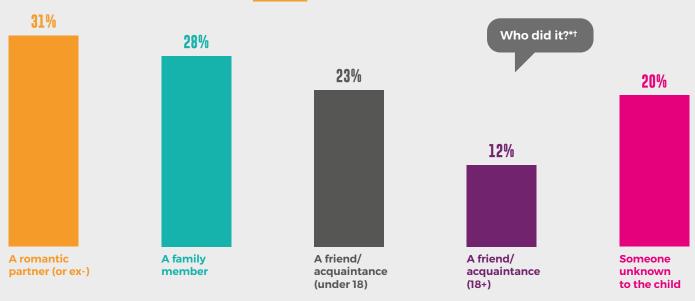
n = 17 internet-using children aged 12-17 who did not tell anyone the last time they were offered money or gifts for sexual images or videos.

IN THE PAST YEAR

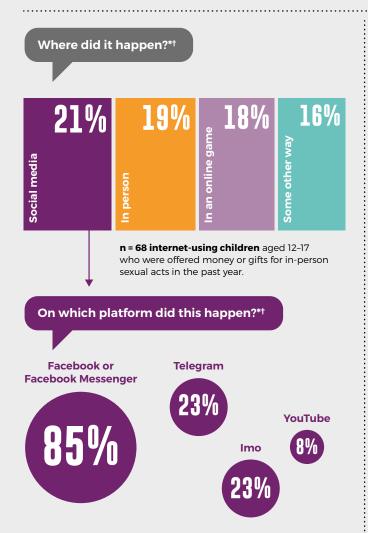
I WAS OFFERED MONEY OR GIFTS TO MEET IN PERSON TO DO SOMETHING SEXUAL



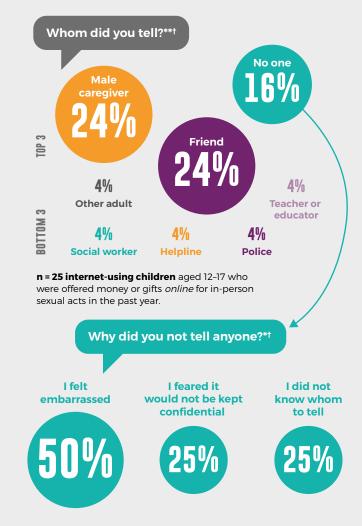
THE LAST TIME THIS HAPPENED ONLINE...



n = 25 internet-using children aged 12-17 who were offered money or gifts online for in-person sexual acts in the past year.



n = 14 internet-using children aged 12–17 who *most recently* received offers of money or gifts for in-person sexual acts via social media.



n = 4 internet-using children aged 12–17 who did not tell anyone the last time they were offered money or gifts online for in-person sexual acts.

[&]quot;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

or the police (n = 1). Overall, as with other reported occurrences of OCSEA, the children who were offered money in exchange for sexual content were very unlikely to engage with the formal reporting mechanisms available in Ethiopia and tended to rely more heavily on other children their age when facing very serious and potentially traumatic experiences, instead of adults. This puts a heavy burden on young people to know how to guide their peers and advise them on how best to respond to these undesired requests. This pattern is particularly concerning given that public awareness of OCSEA in Ethiopia seems quite low among the general public, including children (see page 41).

Offering children money or gifts for sexual acts in person

In Ethiopia, 7% of children who participated in the household survey said they were offered money or gifts to meet someone in person to do something sexual in the past year. As with many of these figures, these numbers can be expected to be underreported as children may not feel comfortable or safe enough to disclose their experiences of abuse and exploitation.

Online or offline? Since offering a child money or gifts to engage in sexual acts in person can happen entirely 'offline' without involvement of technology, children were asked if the most recent request they received to talk about sex happened in person, on social media, in an online game, or in some other way. Of the 68 children who said they were offered, during the past year, money or gifts to meet in person and engage in sexual activities, 19% received such requests during an in-person interaction. Respondents were more likely to receive these requests online; 21% on social media, and 18% through an online game. Ten children said this happened through some other medium and 25% did not answer this question, perhaps due to a reluctance to divulge too many details of the incident. For those children who had this experience through social media, the most common platforms where this last occurred were Facebook or Facebook Messenger, Telegram, and Imo.

Who made the offers: Individuals that are already known to children were much more likely to be committing these acts than people unknown to the child. Children's responses revealed that current or former romantic partners and family members were the most likely to offer children money or gifts online to meet in person for sexual acts. Only five cases included an individual unknown to the child.

Whom children tell about it - if anyone: Once again, children were very unlikely to use formal reporting channels and instead tended to confide in those they had a personal relationship with (see infographic on page 48). Children were equally likely to tell a friend or a male caregiver. Of the 20 children who were offered money or gifts online to meet in person and engage in sexual activities, four did not tell anyone. For those four children, the barriers to disclosing included not knowing where to go or whom to tell, feeling embarrassed or ashamed, and concerns that their story would not be kept confidential.

Sexual extortion

Sexual extortion is sometimes used in the grooming process. Often the offenders have already obtained sexual images of the children and threaten to publicly publish or share these with their friends or family members as a way of coercing children into sharing more images or engaging in other kinds of sexual activities. Such threats can also be used to extort money. Despite evidence showing children being threatened or blackmailed through online means, there is no law in Ethiopia criminalising sexual extortion committed online.

In the *Disrupting Harm* household survey in Ethiopia, 5% of internet-using children (n = 55) said they were threatened or blackmailed to engage in sexual activities at least once in the past year. This figure may be under-reported as some children might not feel comfortable answering the question (as seen in the high non-response rates to some questions in this section of the survey).

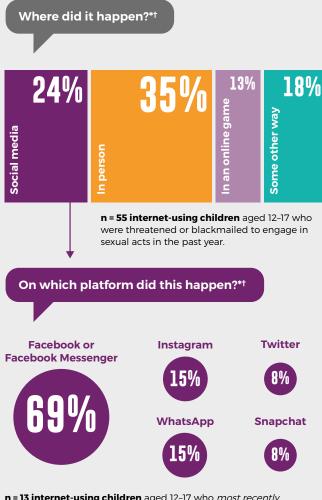
SOMEONE THREATENED OR BLACKMAILED ME TO ENGAGE IN SEXUAL ACTIVITIES

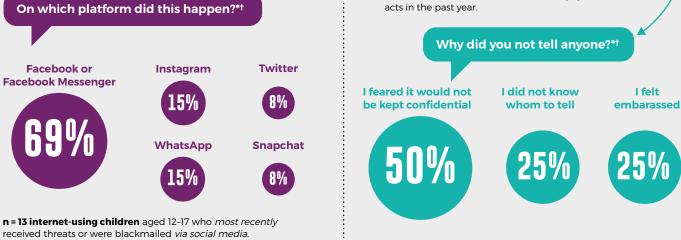


THE LAST TIME THIS HAPPENED ONLINE...



n = 20 internet-using children aged 12-17 who were threatened or blackmailed online to engage in sexual acts in the past year.





[&]quot;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

Whom did you tell?**†

Friend

Female caregiver

Sibling

Male caregiver

n = 20 internet-using children aged 12-17 who were threatened or blackmailed online to engage in sexual

Other adult

Source: Disrupting Harm data

n = 4 internet-using children aged 12–17 who did not tell anyone the last time they were threatened or blackmailed online to engage in sexual activities.

Interviews conducted in other Disrupting Harm countries with survivors of online sexual extortion detailed how the extortion evolved: "He required photos of me; I said I wouldn't send any. No, no way. That's when he started to use threats. He screenshot my whole friends list. He said if I don't send photos to him, all the friends on my list would get all the photos he had received." (RA5-CA-07-A) The threat to share images was mentioned repeatedly across survivor accounts: "He started threatening me - saying, 'If you not going to, I will post those nude pictures you sent me; I will post them all on Instagram and on Facebook and on Tik Tok, and I will also share them on my WhatsApp.' I begged him, I said 'Please don't do that to me, don't do it, don't put my photos on social media.' Then he was like, 'No, it's too late." (RA5-NA-03-A)

Children were as likely to be extorted for sexual acts online – through social media and online games – as they were to receive these threats in person. This is the first form of abuse explored in the household survey where the abuse was equally likely to occur online or offline. Perhaps this is rooted in the fact that the offenders tend to be individuals in the child's immediate circle, who have access to the child and are able to make these threats face-to-face. Only children who said that this most recently happened to them via social media or in an online game (n = 20) were included in the subsequent analysis.

For the 20 children subjected to sexual extortion online, the offenders were most commonly current or former partners, followed closely by friends or other acquaintances under 18 years. There were three cases in which the offenders were unknown to the victims. While taking protective measures against 'stranger danger' is necessary, the disproportionate focus on strangers – rather than on people already in children's lives – in the discourse around sexual violence against children online might be counterproductive given these clear patterns in the data. Another consideration for response systems is that it could be much more difficult to seek help for victims from offenders they know, if they are emotionally and/or economically dependent on abusers.

Children who had been subjected to sexual extortion online were most likely to tell a friend and/ or a sibling. Only one child reported to the police and two reported to a helpline, while four of these 20 children did not tell anyone.

2.2.2 CSAM and live-streaming of child sexual abuse

Ethiopian legislation does not comprehensively define and criminalise CSAM. The only relevant provisions are included in the Criminal Code, which makes illegal conduct related to publications that are "obscene or grossly indecent" 86 (qualifiers not defined by the law and therefore open to judicial interpretation) and the Computer Crime Proclamation, which criminalises a series of acts associated with visual materials depicting minors engaged in sexually explicit conduct or persons appearing to be a minor engaged in sexually explicit conduct.87 This provision fails to include depictions of the sexual parts of a child's body for primarily sexual purposes, non-visual materials, or digitally generated child sexual abuse material, including realistic images of non-existing children. Moreover, it does not relate to knowingly obtaining access to CSAM as a criminalised conduct.

Live-streaming of child sexual abuse is currently not criminalised by the Ethiopian legislation. However, the Criminal Code contains a provision on the organisation of "obscene or indecent performances in theatres or cinemas, by projection or by radio or television broadcast, by video, or in any other way." However, once again no definition is provided for what constitutes an obscene or indecent performance. Moreover, under Ethiopian legislation, recruiting, causing or coercing a child into participating in pornographic performances and knowingly attending pornographic performances that involve children are not criminalised.

While CSAM and live-streaming of child sexual abuse are currently considered separate concepts in law, in reality it is artificial to break them up as live-streaming sexual violence against children is just one modality through which CSAM can be produced, disseminated and consumed.

^{86.} Government of Ethiopia. (2005). Criminal Code, Article 640.

^{87.} Government of Ethiopia. (2016). Computer Crime Proclamation No. 958/2016, Article 12.

^{88.} Government of Ethiopia. (2005). Criminal Code, Article 641.

How Technological Development Has Influenced Online Child Sexual Exploitation and Abuse

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 we engage with each other, particularly for young people. While this is often harmless and has many benefits, the misuse of such tools is creating new ways of perpetrating OCSEA.

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 create any records, because video is not downloaded or retained by default, although

metadata is. This means when the streaming stops the CSAM vanishes, unless the offender deliberately records it. This creates specific challenges for investigators, prosecutors and courts, especially as the existing legal definitions of CSAM and methods of investigation and prosecution are not always up to date.

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

Children's experiences sharing of sexual images without permission

CyberTip data presented in chapter 2.1 showed that CSAM is a real and existing threat to the safety and wellbeing of children in Ethiopia. The possession, manufacture and distribution of CSAM accounted for almost all of Ethiopia's CyberTips between 2017 and 2019. Moreover, the Disrupting Harm household survey found that 5% (n = 50) of internet-using children aged 12-17 in Ethiopia said that someone had shared sexual images of them without their permission. This is an alarming number considering the implications of such an experience. The children in the sample ages 16 and 17 were most likely to have their images shared without permission (34 out of 50 children). Boys were also more likely than girls to experience this harm in the past year (boys: n = 37; girls: n = 13).

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 capture instances of severe sexual abuse, the trauma associated with those in-person experiences can also be repeatedly reactivated by the sharing

of the content. However, *Disrupting Harm* did not seek to obtain specific data from children pertaining to severe sexual abuse, mainly because our ethical and methodological approach required us only to capture what children shared on their own terms, rather than seeking out and delving into specific forms of abuse. This is not to say that victims of such acts were not part of our samples but instead, that this was not disclosed.

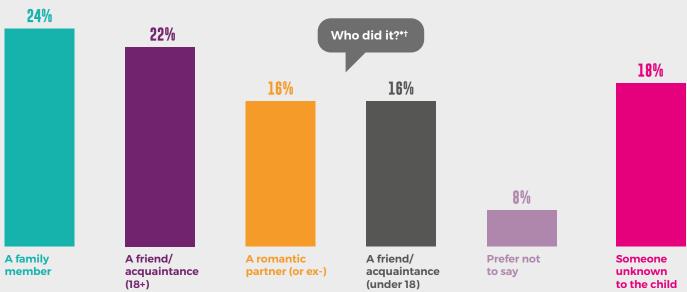
The majority (73%) of surveyed children in Ethiopia said that if a person takes naked images or videos of themselves, it is their fault if those materials are shared with other people; this perception is also shared by 84% of caregivers who said the same. Such victim-blaming may explain the low levels of reporting seen throughout the data from children who have been subjected to OCSEA. To illustrate, among the 50 children in the sample whose sexual images were shared without their permission, a fifth - 10 children - did not tell anyone at all. If children did disclose their experiences, they were most likely to tell a friend, followed by caregivers and siblings. Very few children told a teacher or a social worker and only four children turned to a helpline or the police (see infographic on page 53).

IN THE PAST YEAR

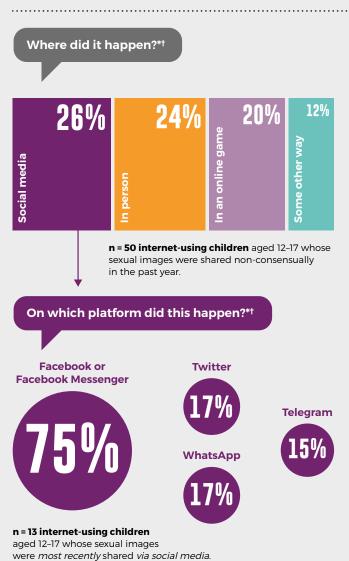
SOMEONE SHARED SEXUAL IMAGES ME WITHOUT MY CONSENT

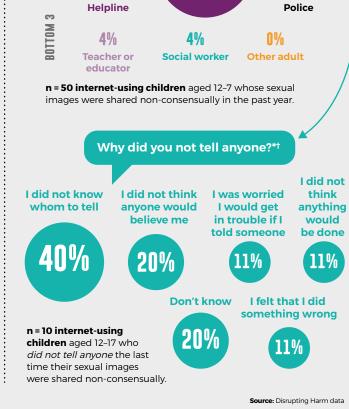






n = 50 internet-using children aged 12-17 whose sexual images were shared non-consensually in the past year.





8%

Whom did you tell?**[†]

Female

caregiver

16%

8%

급

[&]quot;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

Who shared the images: Individuals known to the child such as family members and adult friends or acquaintances were the most likely offenders (n = 12 and 11, respectively). As shown in the infographic, this was followed by friends or acquaintances younger than 18, and romantic partners. Notably, nine children said their images were shared by someone unknown, indicating that these children were possibly tricked or threatened into sharing naked images or had them stolen. Understanding the context around these cases is an area for further research, possibly through qualitative methods to get more granular detail.

Online or offline? Out of the 50 children whose images were shared without permission during the past year, 13 said that this happened via social media and 10 in an online game. For children whose images were shared on social media, this was most likely to have happened most recently on Facebook, Twitter, WhatsApp and/or Telegram. Twelve children said this happened to them in person, which means that someone might have shared images while they were present or taken images of the child without their permission. Six children said their images were shared non-consensually in some other way.



Individuals known to the child such as family members and adult friends or acquaintances were the most likely offenders (n = 12 and 11, respectively).



Accepting money or gifts in exchange for sexual images or videos

When children create sexual content in exchange for something, this constitutes child sexual exploitation, irrespective of whether they are coerced or actively engage in this activity.89 This section of the report considers instances when money or gifts were exchanged for sexual content, regardless of how the process was initiated.

While the practice of accepting money in exchange for sexual activities is not new,90 the use of digital technologies to do so is. This practice is particularly risky for children because of the risk of on-sharing. Data from the Internet Watch Foundation and Microsoft revealed that it is very common for selfgenerated sexual content involving children to be shared further; 90% of 'youth generated' sexual images and videos that were assessed in the Internet Watch Foundation and Microsoft study were 'harvested' from the original upload location and redistributed on third party websites.91

Given the sensitivity of this topic, only 15-17-year-old respondents in the Disrupting Harm survey sample were asked whether they had accepted money or gifts in exchange for sexual content. Among the 751 respondents who were asked this question, four percent (31 children) responded affirmatively. It is expected that children may be hesitant to reveal that they engaged in these kinds of practices, even in an anonymised survey, so this is likely underreported.

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.

^{89.} ECPAT International. (2020). Summary Paper on Sexual Exploitation of Children in Prostitution. Bangkok: ECPAT International. 90. Peebles, G. (2012, March28). Stolen Childhoods: Child Prostitution And Trafficking In Ethiopia. Eurasia Review

2.3 OTHER EXPERIENCES OF CHILDREN THAT MAY BE LINKED TO OCSEA

Additional 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.

2.3.1 Sexual Harassment

The household survey data showed that in the past year around one in five internet-using children in Ethiopia (19%) received sexual comments online that made them feel uncomfortable. These kinds of comments included jokes, stories or comments about the child's body, appearance or sexual activities. Among the 191 children who were harassed in this way, this was more likely to happen online than in person. The most common platforms where this happened to children were Facebook, and instant messaging apps Telegram and Imo.

Sexual harassment of children was most likely to be committed by an unknown person (26%), followed by a romantic partner (21%), someone in their family (19%), closely followed by a friend older than 18 (18%) and a friend younger than 18 (8%). This shows that it is more common by far for children to be sexually harassed by people they already know, compared to by strangers online.

As with severe forms of sexual violence, children were most likely to either tell a friend or not tell anyone at all, the last time they were sexually harassed online. Only 15% of children told their caregivers. Not knowing where to go or whom to tell, not thinking it was serious enough to report and feeling embarrassed, were the most common barriers for children who did not disclose their experience to anyone.

Online sexual harassment of children is currently not criminalised by Ethiopia's Criminal Code or by the Computer Crime Proclamation. However, as mentioned above, the Computer Crime Proclamation does criminalise the enticement or solicitation of minors for sexually explicit conduct by sending erotic material through computer systems, 92 which could potentially cover the sexual harassment of a child.



One in five internet-using children in Ethiopia (19%) received sexual comments online that made them feel uncomfortable.



2.3.2 Receiving unwanted sexual images

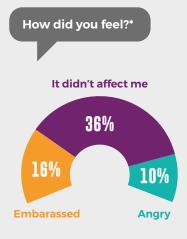
Nineteen percent of children in the sample said that someone had sent them unwanted sexual images in the past year. These experiences may be accidental or unintended, but they could also be indications of attempted grooming. The most common platforms where this last occurred were Facebook, Telegram and Imo; and breaking with trends for other experiences reported so far, these were most likely to come from someone unknown to the child (40%). This was followed by a family member (16%), a romantic partner (15%) and a friend younger than 18 years (12%).

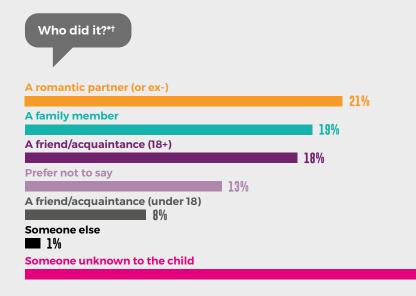
Thirty-five percent of the children that received unwanted sexual images online did not tell anyone, while another 35% told a friend. Only around 10% of these children told their caregivers, while almost no one told a teacher or social worker or reported to the police or a helpline. For children who did not tell anyone about what happened, the main reason was that they did not know where to go or whom to tell, that they felt embarrassed, ashamed, or that they didn't think it was serious enough to report.

Feelings of embarrassment and shame were common barriers to reporting among 12-17-year-olds who were subjected to the various forms of OCSEA described throughout <u>chapter 2.2</u> and <u>2.3</u>.

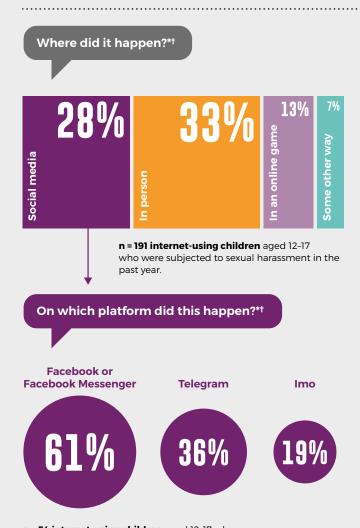
SOMEONE MADE SEXUAL COMMENTS ABOUT THAT MADE ME FEEL UNCOMFORTABLE

THE LAST TIME THIS HAPPENED...

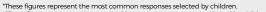




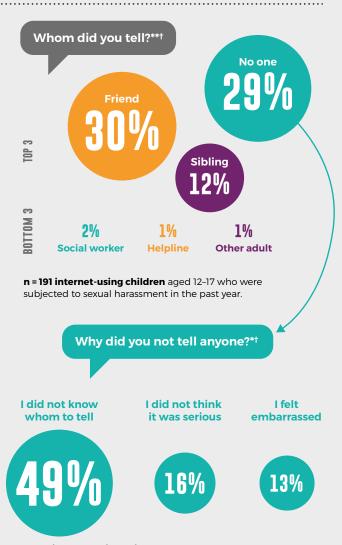
n = 191 internet-using children aged 12-17 who were subjected to sexual harassment in the past year.







"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



n = 55 internet-using children aged 12-17 who did not tell anyone the last time they were subjected to sexual harassment.

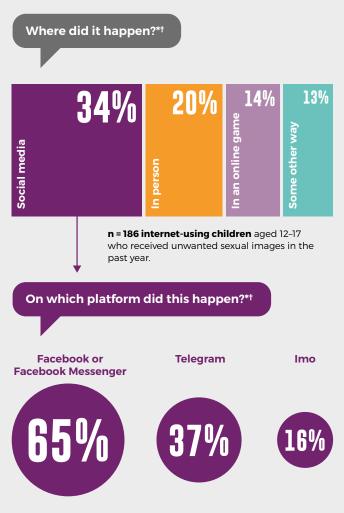
26%

THE LAST TIME THIS HAPPENED...





n = 186 internet-using children aged 12-17 who received unwanted sexual images in the past year.





Whom did you tell?**† **Friend Sibling** Male 급 caregiver BOTTOM 3 1% 1% 1% Helpline Social worker Police n = 186 internet-using children aged 12-17 who received unwanted sexual images in the past year. Why did you not tell anyone?*1 I did not know I felt Don't know whom to tell embarassed **15**%

n = 65 internet-using children aged 12-17 who did not tell anyone the last time they received unwanted sexual images.

40%

[&]quot;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

2.4 INSIGHTS ABOUT VICTIMS AND OFFENDERS FROM KNOWN OCSEA AND CSEA CASES

2.4.1 Victims

Beyond the household survey data, which gives an indication of who the victims of OCSEA are, the *Disrupting Harm* team identified very little further data. As already reported, there was no data available from law enforcement sources about OCSEA victims or offenders in Ethiopia.

While child sexual exploitation and abuse (CSEA) that does not explicitly involve digital, internet or communication technology is not the focus of this

report, data on offline offending is included here as it is possible that these instances do involve technology, but it is not recorded. Furthermore, data about offline forms of offending may help us understand the context in which online offending may occur or may already be occurring.

According to national law enforcement, all recorded CSEA victims were Ethiopian nationals. Where victim gender was recorded, the vast majority (89%) were girls.

Figure 21: Victims of CSEA in Ethiopia, by year and recorded age group.93

Victim Age Group	2017	2018	2019	% Change 2017- 2019	Total 2017-2019	% of Total
0-3 years	14	26	17	21%	57	6.4%
4–6 years	17	40	52	206%	109	12.2%
7-9 years	16	29	49	206%	94	10.5%
10-12 years	29	61	43	48%	133	14.8%
13-15 years	43	84	83	93%	210	23.4%
16 and 17 years	116	68	49	-58%	233	26.0%

Base: Data provided by law enforcement sources to Disrupting Harm through a questionnaire.

Figure 22: Victims of CSEA in Ethiopia, by year and gender.

Victim Gender	2017	2018	2019	% Change 2017- 2019	Total 2017-2019	% of Total
Male	31	25	26	-16%	82	11%
Female	204	161	267	31%	632	89%

Base: Data provided by law enforcement sources to Disrupting Harm through a questionnaire.

2.4.2 Offender

Ethiopian law enforcement reported that all recorded CSEA offenders in 2017, 2018, and 2019 were male Ethiopian nationals.

To expand on the current understanding of the context in which OCSEA happens in Ethiopia, the frontline service providers survey sought to explore the typical relationships that were observed by frontline workers between offenders and child survivors when they reported having worked with

OCSEA cases. In line with what Ethiopian law enforcement reported, most respondents (30 out of 33) had not managed any OCSEA cases in the past 12 months. Only three respondents reported working on OCSEA⁹⁴ cases and of those, two described the offenders to be a 'community member over 18' and one as a 'relative under 18'. When asked about the facilitators,⁹⁵ only two respondents reported working on OCSEA cases that involved a facilitator. One described the facilitator as a 'community member over 18' and one as a 'community member under 18'.

Figure 23: CSEA offenders in Ethiopia, by year and recorded age group.96

Offender Age Group	2017	2018	2019	% Change 2017- 2019	Total 2017-2019	% of Total
Under 18	106	36	69	-34.9%	211	28.0%
18-29	27	105	204	655.6%	336	44.6%
30-39	0	29	88	-	117	15.5%
40-49	5	11	38	660.0%	54	7.2%
50-59	7	0	7	0.0%	14	1.9%
60-69	0	3	9	-	12	1.6%
70-79	2	2	3	50.0%	7	0.9%
80 and above	0	0	2	-	2	0.3%

 ${\tt Base: Data\ provided\ by\ law\ enforcement\ sources\ to\ \textit{Disrupting\ Harm}\ through\ question naires.}}$



According to national law enforcement, all recorded CSEA victims were Ethiopian nationals. Where victim gender was recorded, the vast majority (89%) were girls.



^{94.} These cases were identified by the frontline workers as OCSEA cases but did not go through the formal justice system as such and therefore did not match the sample subject criteria for the Access to Justice interviews.

^{95.} 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')." 96. NB: A discrepancy has been identified between 2019 totals for offenders by age group (n = 420) and gender (n = 563).

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

This chapter presents evidence about current response mechanisms to OCSEA in Ethiopia. This includes formal reporting options, and responses by police and the court system. It considers the contributions which government, civil society and the internet and technology industry make to combating OCSEA in Ethiopia. Much of the data in this chapter is drawn from qualitative interviews and responses may not reflect the full range of experiences of those accessing the response mechanisms to OCSEA in Ethiopia.

3.1 FORMAL REPORTING MECHANISMS

As evidenced in this report, internet-using children are already being subjected to OCSEA but awareness is still very low in Ethiopia. *Disrupting Harm* had limited success in identifying samples of any children who had accessed justice mechanisms. Duty-bearers interviewed acknowledged this lack of awareness and intervention and are keen to rapidly catch up.

3.1.1 Reporting mechanisms

As mentioned in <u>chapter 2</u>, children overwhelmingly did not report their experiences of sexual violence through formal reporting mechanisms, and instead were more likely to turn to interpersonal and informal disclosures. According to the household survey, almost no children reported OCSEA incidences to helplines, social workers, or the police, and many of the children never told anyone about potential or actual OCSEA they were subjected to.

This finding is in line with findings from the government interviews, where a respondent from UNICEF Ethiopia indicated that in an ongoing assessment on the 'Capacity of Child Protection Systems in Ethiopia', preliminary findings suggest that for incidents of violence against children there are low levels of disclosure and reporting to law enforcement agencies. (RA1-ET-02-A) This aligns with a qualitative study on violence affecting children and youth undertaken in 2019, which found that in Ethiopia, most cases of violence are unreported or dealt with through family, friends, community support, informal mechanisms or religious institutions. The study showed that in particular, vulnerable children and young people are unlikely to report cases of rape or sexual assault.97

There are several ways in which OCSEA-related crimes can be reported in Ethiopia. Within cities and towns, child protection units in police stations are the focal units for receiving cases of OCSEA. While in principle every police station should have a child protection unit, often that is not the case. Even when they exist, the police officers are overstretched according to the Head of the Child Justice Project Office of the Federal Supreme Court. (RA1-ET-06-A)

This lack of capacity is echoed in the survey of the frontline workers, where all the respondents rated law enforcement's awareness and response to OCSEA as poor (n = 33).

Beyond reporting to the police, duty-bearer interview responses indicated that – especially in rural settings – OCSEA-related complaints could be made through various other structures such as teachers or One-Stop Centers and hotlines. Though these structures are mentioned, the team was not able to find any information about them and therefore could not evaluate how effective they are in dealing with OCSEA concerns.

Phone hotlines using the short code 919 are being operated in six out of Ethiopia's 12 regions, based within regional police offices. These hotlines, which are supported by the Ethiopian government in partnership with UNFPA and UN Women, are not specific for reporting OCSEA but one respondent said that hotlines can register cases of sexual exploitation though they may not have a specific category for online issues. (RA1-ET-O1-A)

Regardless, hotlines do not seem to be prominently known in Ethiopia, as the survey data from the frontline workers indicated that 91% of respondents indicated that 'No hotline/helpline' is one of the main barriers to reporting within the country. Taking this into consideration it is not surprising that one of the hotlines – ECFA Ethiopia – reported to Child Helpline International that they received only 70 contacts concerning OCSEA in 2017 and none in 2018 and 2019. These 70 contacts concerned offenses targeting girls, including online distribution of child sexual abuse material (CSAM) and grooming.

^{97.} Chuta, N., Morrow, V., Pankhurst, A., & Pells, K. (2019, August). <u>Understanding violence affecting children in Ethiopia: a qualitative study.</u>

^{98.} The hotlines are in the following locations: Addis Ababa city, Oromia region, Gambela region, Benishangul-Gumuz region, Harari region and Somali region. Hotlines do not cover the whole of Ethiopia, as there are 12 geographical regions, and hotlines only cover Addis city and five regions. Hotlines are government- supported and are based within the regional police offices. Though as part of the Governments Growth Plan II, the Ethiopian government planned the creation of three-digit telephone lines at federal level, these were not mentioned by any respondent as having been set-up.

Another indicator for the lack of reporting is the great difficulty the *Disrupting Harm* team faced in trying to find a sample of OCSEA victims who had accessed the formal justice system. Despite contacting more than 20 national and international civil society organisations, justice professionals and law enforcement officers working with child victims of trafficking and sexual abuse and exploitation, the *Disrupting Harm* team were not able to identify any OCSEA victims between 15–18 years old who had accessed the formal justice system.

3.1.2 Why children might not report?

The fact that a substantial proportion of children do not report OCSEA to anyone is concerning. Equally worrisome is that most participants in the duty-bearer interviews suggested that the lack of reporting is because no OCSEA is happening in Ethiopia. (RA1-ET-09-A, RA1-ET-03-A, RA1-ET-06-A) This contrasts with evidence reported by children in the household survey of both potential and actual instances of OCSEA, and suggests that the lack of reporting is influenced by the following factors: fear of shame; stigma and victim blaming; not knowing how or who or where to report incidents of attempted or actual OCSEA; lack of knowledge of OCSEA as a rights violation; and lack of confidence in the police and other support services.

Fear of shame, stigma and victim-blaming

Children often feel ashamed to talk to others about their experiences of OCSEA. In the survey of frontline workers, stigma from the community and discomfort around discussing sex were among the main reasons indicated as influencing reporting by OCSEA victims. A Child Protection Specialist noted in their interview that children worry they may get in trouble or feel that no one would believe them or understand their situation if they reported what happened to them, and added that "Sometimes it's family honour, so they don't want to disclose these issues." (RA1-ET-O2-A)

Ethiopian law criminalises same-sex sexual acts under the Criminal Code's section on "sexual deviations." Global evidence indicates that such laws may silence boys from reporting cases of sexual abuse committed by a same-sex offender, as they fear that they themselves might be criminalized despite being victims of a crime. In Ethiopia, although the legislation provides for the criminalisation of those who perform homosexual acts on minors, it may also deter children who were sexually abused or exploited by an offender of the same-sex from seeking help.¹⁰⁰

Not knowing where to go to report OCSEA

Fifty-seven percent of internet-using children said that they would not know where to seek help if they experienced sexual assault or harassment. According to children who were subjected to OCSEA in the past year, this was also one of the most common barriers preventing them from disclosing or reporting.

Children are not taught what OCSEA is and might not perceive OCSEA as wrong

As the Director of the Directorate of Women, Children, and Youth, Ministry of Innovation and Technology noted: "There is no understanding of online sexual abuse, almost everybody is not aware of it. Offline sexual exploitation of children, people are more aware." (RA1-ET-O3-A)

Lack of confidence in the police and other support services

Almost no children in the household survey indicated that they reported to police about the various forms of potential or actual OCSEA to which they were subjected to. In the frontline service providers survey, 94% of respondents said that cases of OCSEA are not reported by children because services cannot be trusted, and 82% said that poor quality of services was a main barrier to reporting. Duty-bearer interviews also indicated that sometimes little action is taken by the recipients of an OCSEA complaint, which further undermines confidence in the reporting mechanisms. (RA1-ET-02-A) This distrust in the reporting systems is further amplified by scepticism regarding the confidentiality of the available services. (79% of frontline workers reported concerns about confidentiality were a barrier to reporting.)

^{99.} Government of Ethiopia. (2005). <u>Criminal Code</u>, Article 629. 100. Josenhans, V., Kavenagh, M., Smith, S., & Wekerle, C. (2020). <u>Gender, rights and responsibilities: The need for a global analysis of the sexual exploitation of boys</u>. Child Abuse & Neglect, 110 (1), 6.

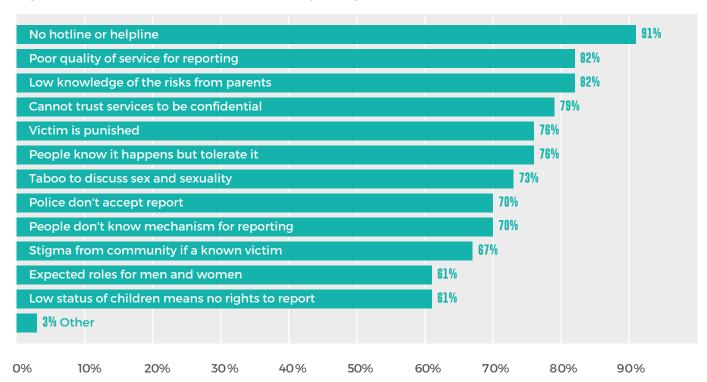


Figure 24: Social and cultural barriers to reporting OCSEA.

Base: n = 33.

Knowledge of frontline workers about OCSEA

The frontline service providers survey was administered *in person* (in the office of the ECPAT member in Addis Ababa) partly because many of the frontline workers social service providers are *not* regularly connected to the internet. This disconnection from the online world suggests that frontline workers have few chances to engage with – and learn about – the platforms that young people regularly use. Lack of familiarity with online settings may also lead to frontline workers having a weak understanding of OCSEA and its vulnerability factors, which poses an additional barrier for children seeking to disclose what they have experienced.

The results of the survey indicate some OCSEArelated areas are well understood by the frontline workers, and other areas where training is needed to ensure consistent knowledge. In the survey, the 33 frontline workers were presented with three scenarios depicting different modes of OCSEA and were asked to indicate the extent to which they agreed or disagreed that the child was a victim and that the perpetrator had committed an OCSEA-related offence. These questions were designed to elicit insights about how participants assessed different forms and situations of OCSEA. Responses are likely based on the participant's knowledge on the issue, which is influenced by social norms and beliefs and by how these issues may (or may not) be defined in national laws. The frontline workers overwhelmingly correctly identified the children as victims and the adults as perpetrators across the three scenarios. However, there was some divergence of views; for example, about whether an individual who watched online a video of a 16-year-old female undressing had committed an OCSEA-related crime.

3.2 LAW ENFORCEMENT RESPONSE

3.2.1 Limited recorded OCSEA-related cases

Ethiopian law enforcement reported zero OCSEArelated cases between 2017 and 2019. Interviews with law enforcement officials confirmed this finding. A respondent from the Cybercrime Unit - a dedicated unit that handles a broad range of online crimes - indicated that to date no OCSEA-related cases had been referred to them, except cases of sexual extortion of women that sometimes involve girls under 18. These cases could qualify as OCSEA-related cases if they involved technology at some point during the sexual extortion process. As a prosecutor from the Federal Attorney General's Office explained: "Sometimes we see a case of exposure of children to sexualised material, as well as sexting but not cases of online grooming, live-streaming, or child sexual abuse materials." (RA1-ET-05-A)

Consistent with the responses from the law enforcement sector, the Head of the Child Justice Project Office of the Federal Supreme Court noted that to date there are no specifically recorded OCSEA-related cases. "There is no tangible practical case of OCSEA that I can tell you." (RA1-ET-06-A) While the household survey data show that OCSEA is occurring in Ethiopia, these cases are not appearing in the justice system. It could be that some cases that include both online and offline elements of child sexual extortion or abuse are being addressed without being classified as an OCSEA-related case.

3.2.2 Technical capacity and training

All interviewed officials were in agreement that there is limited awareness and technical capacity of law enforcement actors to investigate, prosecute and successfully adjudicate OCSEA-related cases. While a dedicated Cybercrime Unit exists within the police, this unit handles a broad range of online crimes. The Cybercrime Unit does not necessarily specialise in the investigation of OCSEA, its officers are not trained on such investigation, and it does not have specific funding for investigation of OCSEA-related cases, according to the respondent from the Cybercrime Unit. (RA8-ET)

A representative from the Cybercrime Unit mentioned that coupled with the lack of technical expertise on OCSEA, the Cybercrime Unit currently lacks the required equipment (software and hardware) to effectively investigate OCSEA-related cases. He noted that the current software at the unit is outdated and needs to be updated: "My unit does the investigation related to phones, computers, as well as social media platforms e.g., Facebook. The challenge is however equipment, software and hardware and training. The software is outdated; its lifetime is three years or two years. We need to update, so this is very challenging." (RA1-ET-12-A) Additionally, no psychological supervision for those working with child sexual exploitation cases and material is available.

Ethiopia does not have any unit dedicated to investigation of OCSEA. According to law enforcement, there are 180 officers assigned to address all forms of child sexual exploitation and abuse, which could include OCSEA-related cases, but it is possible that none of these officers had undergone any training on OCSEA. (RA8-ET) Police officers and court judges are not provided with training on OCSEA, according to the Head of the Child Justice Project Office of the Federal Supreme Court: "What is happening on the ground is that we don't have police officers that are trained in the investigation of sexual violence." (RA1-ET-06-A)

Due to the limited technical expertise of Ethiopian law enforcement on OCSEA, the UNODC is focusing on building the necessary specialised capacity on OCSEA within the Federal Police Commission. Towards this goal, the UNODC facilitated an exposure visit of high-level police officers to the 'Anti Human Trafficking and Child Protection Unit' in Nairobi, Kenya.¹⁰¹ (RA1-ET-13-A) Additionally, the UNODC has also started mentoring investigators from the Cybercrime Unit on investigating OCSEA; approximately 19 investigators were mentored. The training of the 19 officers was done, not through workshops but by having an expert from UNODC sit with a few officers at a time to take them through the intricacies of investigating OCSEA and obtain evidence following accepted legal standards.

The same UNODC respondent also indicated that the organisation intends to support the Cybercrime Unit with all the equipment needed to make it operational and that discussions on this have been initiated with policy makers within the Federal Police Commission: "There is a Cybercrime Unit in Ethiopia... in that unit, we want to establish an online child sexual exploitation crime investigation centre. We want to have what we have in Nairobi in Ethiopia... We want to facilitate information that we get through INTERPOL and the National Center for Missing and Exploited Children – and to use this information to make sure perpetrators are apprehended. Most equipment is already bought and only waiting to be installed." (RA1-ET-13-A)

Throughout Ethiopia there is a lack of trained professionals at the community level that could support young people experiencing OCSEA. (RA1-ET-02-A) This gap was confirmed in the frontline service providers survey. When asked about support services, respondents were asked to evaluate the overall availability and quality of medical, psychological, legal and reintegration services for child victims of OCSEA in Ethiopia. These were rated by nearly all respondents as poor (97%–100%; n = 32–33 respectively). Interesting to note at this point that among the 33 surveyed frontline workers in Ethiopia, none reported having worked on an OCSEA case in the last 12 months.



Ethiopia does not have any unit dedicated to investigation of OCSEA. According to law enforcement, there are 180 officers assigned to address all forms of child sexual exploitation and abuse, which could include OCSEA-related cases, but it is possible that none of these officers had undergone any training on OCSEA.



3.3 ACCESS TO JUSTICE AND REMEDIES

Access to justice for victims of OCSEA cannot be assessed at present. Despite extensive searches, including consulting over 20 organisations between June 2010 and September 2020, Disrupting Harm was unable to identify criminal justice officials with experience handling OCSEA cases within the criminal justice system of Ethiopia. It was also impossible to identify victims of OCSEA who had attempted to secure access to justice.

The Ethiopian government has introduced a child-friendly approach to collecting testimonies from children - including the option of having an intermediary transmitting the questions from the courtroom to the child and vice versa. 102,103 However, the Disrupting Harm team has been unable to confirm how well this approach is implemented. Also noteworthy is that in 2018, a validation workshop was organised by the Federal Supreme Court of Ethiopia with a number of justice stakeholders to validate the Draft Child Justice Guidelines.¹⁰⁴ Four guidelines were discussed for validation. These related to establishment of a victim fund; provision of free legal aid to children; support to children and their caregivers with temporary shelter, counselling, transportation or house rent allowances; and psychological support services. 105 However, at the time of writing this report, it was unclear if these guidelines had been disseminated or implemented.

Compensation

Article 101 of the Criminal Code allows injured persons "to claim that the criminal be ordered to make good the damage or to make restitution or to pay damages by way of compensation." This means that, in theory at least, victims of OCSEA have the possibility to seek compensation from their perpetrators through a civil claim jointly lodged within a criminal suit 107 or separately, according to the general principle laid down on Article 2028 of the Civil Code. 108

The Criminal Code also contains a provision to enforce the payment of the compensation to the injured party of the proceeds of the sale of property, or the sum guaranteed as surety, or a part of the fine or of the yield of the conversion into work, or confiscated property. However, this provision does not establish the possibility to seek compensation through country-managed funds. None of the provisions that regulate access to compensation contain specific measures relating to victims of OCSEA offences. No information was found on cases of children successfully securing compensation or having access to effective remedies.

Finally, Proclamation No. 909/2015 on the Prevention and Suppression of Trafficking in Person and Smuggling of Migrants provides for the compensation of child victims of human trafficking, including child victims of sexual exploitation. Moreover, when victims cannot get compensation as established in Article 31 (1) and (2) and they are Ethiopian nationals, they can claim a reimbursement payment from the State, which will be paid from the Fund established according to Articles 32 to 38 of the Proclamation No. 909/2015. The applicability of this provision to child victims of OCSEA is unclear.

102. UNICEF Ethiopia. (2014, September 4). In Ethiopia, Danish diplomats observe progress in child protection. UNICEF Ethiopia blog. See also: UNICEF Ethiopia & Ministry of Finance. (2019, October). National Situation Analysis of Children and Women in Ethiopia.

103. UNICEF Ethiopia & Ministry of Finance. (2019). National Situation Analysis of Women and Children in Ethiopia.

^{104.} Justice for All-Prison Fellowship Ethiopia. (2018, October 8). Workshop on the validation of Draft Child Justice Guideline. Justice for All-Prision Fellowship.

^{105.} Justice for All-PPrison Fellowship Ethiopia. (2018, October 8). Workshop on the validation of Draft Child Justice Guideline. Justice for All-Prison Fellowship.

^{106.} Government of Ethiopia. (2005). Criminal Code, Article 101.

^{107.}Government of Ethiopia. (2005). <u>Criminal Code</u>, Article 101.

^{108.} Government of Ethiopia. (1960). Civil Code of the Empire of Ethiopia, Article 2028.

^{109.} Government of Ethiopia. (2005). <u>Criminal Code</u>, Article 102 (1).

3.4 COORDINATION AND COLLABORATION

A multi-stakeholder approach, where the government coordinates and regulates collaboration, is crucial to preventing and responding to OCSEA. Data collected in Ethiopia show that a coordinated response to OCSEA between government agencies, civil society and Internet service providers and platforms, is still at a nascent stage of implementation.

As presented in the Legal and Policy overview, there are currently no national policies and plans in place related to OCSEA, which shows a major gap in government response. This gap is consistent across other stakeholders whose involvement is crucial for a comprehensive response to OCSEA. For example, few civil society organisations in Ethiopia have responded to OCSEA, while in other countries the civil society sector plays an important role by referring cases to the police, supporting victims through the court process, raising awareness in schools and with children, and training frontline service providers and other professionals.

Regarding the collaboration of justice officials on OCSEA, one respondent from the Federal Attorney General's Office indicated the collaboration on violence against children in general is good because the different criminal justice sectors (police, prosecutor and the judiciary) have designated units within them that deal with cases of children. These, she explained, are the structures that collaborate closely on children's matters: "There is strong coordination among the justice actors. Each sector has its designated structure to deal with cases of children; police have child protection units at the national and lower levels, the prosecutor has special prosecution unit focusing on children and women, these two units work closely together, the courts have child-friendly benches. So, they all work together well." (RA1-ET-05-A)

At the same time, OCSEA is not in the strategy and action plan of the coordination mechanism that brings together relevant officials to discuss matters of child justice, according to the representative from the Federal Attorney General's office. (RA1-ET-05-A) In line with this, a respondent from the Cybercrime Unit said that there is a gap in the coordination of

OCSEA as there is no forum which brings together all the justice actors and other government ministries to plan and set in place mechanisms for responding and investigating OCSEA. He indicated that though the police have forums that bring together the different police units, these discuss crimes in general, so he recommended "that all the concerned bodies like the police, government, and non-government agencies should work in collaboration and there should be a forum for OCSEA." (RA1-ET-12-A)

Collaboration between law enforcement, justice actors and Internet service providers and platforms is essential to investigate crimes, convict offenders and prevent the dissemination of CSAM. The legal requirements and practical procedures differ depending on whether these operators are Ethiopian companies or global Internet service providers operating in Ethiopia. When law enforcement seeks to identify and locate a perpetrator – an IP address or a phone number provided by a domestic company – they may serve a domestic service provider with a legal request for subscriber information, which they can then use to apprehend the suspect and as evidence in court.¹¹⁰

However, it is often the case that a further step is required in data gathering processes – that is when there is a need to collect evidence from a global platform, such as Facebook. In 2017, 2018 and 2019, authorities in Ethiopia made a total of zero requests to the major social media platforms for content restriction or user data. This would indicate that, despite thousands of NCMEC CyberTips from global electronic service providers (mainly Facebook) concerning suspected OCSEA in Ethiopia, law enforcement officials in the country have had minimal contact with these providers on OCSEA matters.

^{110.} This explanation ignores challenges posed by carrier grade Network Address Translation, a process by which rapidly exhausting IPv4 addresses have been assigned by Internet service providers to multiple users at the same time, thereby precluding definitive identification of the device and user behind an IP address in certain cases.

4. HOW TO DISRUPT HARM IN ETHIOPIA

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

Detailed recommendations for action in Ethiopia are clustered under four key insights from the *Disrupting Harm* research and sign-posted for different stakeholder groups. However, all these recommended actions are interlinked and are most effective if implemented together.



INSIGHT 1

In the past year alone, 10% of internetusers aged 12-17 in Ethiopia were victims of grave instances of online sexual exploitation and abuse. This includes blackmailing children to engage in sexual activities, sharing their sexual images without permission, or coercing them to engage in sexual activities through promises of money or gifts. Scaled to the population, this represents an estimated 300,000 children who were subjected to any of these harms in the span of just one year.

Government

1.1 In advance of almost certain increases in internet connectivity in the coming years, especially among young people, take the opportunity to create awareness about child sexual exploitation and abuse, including how digital technology might play a role. These programmes must be evidence-based and not shy away from difficult and sensitive messages about OCSEA, including the finding that OCSEA perpetrators are often people known to the child. Adapting and contextualising existing evidence-based programmes should be prioritised and existing evidence-based materials considered as a starting point.

For awareness and education programmes in schools as well as reaching wider communities across the country, the Ministry of Education has a leading role to play. Liaising with the child rights clubs and peer mechanisms can also be important to create awareness about OCSEA (including awareness on reporting mechanisms – see insight 3). Information should be included in parenting education programmes.

Awareness and education programmes should be developed and tested through consultations with children and caregivers, to reflect their perspectives of online risks and the techniques they use to keep themselves safe. Key objectives should include:

- Equipping caregivers with the knowledge and skills to foster safe and ongoing communication with children about their lives online.
- Challenging social norms and taboos that limit discussion about sex and deter children and adults from seeking help about child sexual exploitation and abuse because of embarrassment and shame.
- Supporting caregivers, many of whom have never used the internet, in going online and becoming more familiar with the platforms that their children and adolescents are using.
- Strengthening children's digital literacy to provide them with the skills and understanding needed to avoid or navigate dangerous situations online. This could include lessons about how to block an individual and report inappropriate content or requests. Furthermore, establishing children's knowledge on the risks inherent to online interaction and the exchange of personal information, images, and videos.

1.2 When children do not receive age appropriate and culturally sensitive sex education including on OCSEA, perpetrators can take advantage.

We must ensure that knowledge reaches all children, and include information about 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. This will help children to identify risky or inappropriate interactions both online and in person. There are existing reports¹¹¹ and initiatives¹¹² that can serve as good starting points and best practice examples of age-appropriate resource material.¹¹³

1.3 Help adults who are in contact with children overcome discomfort in discussing sex and sexuality to encourage open dialogue about sexual abuse and exploitation online or in person. 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 for help when needed. To assist caregivers, provide evidence-based education and information to caregivers so that they can recognise exploitative or abusive behaviour from members of the community, both online and offline. This will also help them teach children how to recognise such behaviour and keep safe. Best practices already exist¹¹⁴ and can be used to build on and set in the local context.

1.4 Help children, caregivers, teachers and those working with children understand the full extent of the risks of sharing sexual content and how to engage in harm minimisation to limit possible negative repercussions. Most children who shared sexual content did so because they were in love or trusted the other person, but this behaviour can lead to serious harm, such as non-consensual sharing of the content with others and sexual extortion.

1.5 Education and awareness-raising approaches should reach all children, caregivers and teachers in Ethiopia. There is a sense that due to the relatively greater access to connectivity urban children are at greater risk of OCSEA than their rural peers. This is somewhat true, but not the whole picture. In fact, the distinction will rapidly become less relevant as connectivity improves throughout the country.

1.6 Education for all audiences (children, teachers, and adults) must come from people who understand the issues and solutions. Awareness and education programmes 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. Trainers must receive handson training and support to be able to share material that encompasses sex and technology – two complex areas. Ensure specific actions to include children that are often marginalised, such as children with a disability.

Caregivers, teachers, medical staff, and social support workers¹¹⁵

1.7 Caregivers and duty bearers should learn about what children are doing online and offline and be vigilant about the people with whom their children or the children in their community interact with. Consider whether these interactions seem appropriate for children. Only some threats come from strangers on the internet; many other risks emanate from peers, relatives and community members.

1.8 Improve understanding of digital platforms and technologies. Eighty percent of Ethiopian caregivers of internet-using children have never been online. Caregivers need to familiarise themselves with the internet and build their own digital skills. Simultaneously, they must start by asking children about what they like to do online and which platforms or websites they spend time on. Being involved and supportive of a child's internet use will help them understand the risk and benefits of being online and lead to more open dialogue between children and adults when children face dangers or harm online.

1.9 Inform children about their right to be protected from all forms of physical, sexual and emotional abuse, and on how to stay safe by setting boundaries, recognising appropriate and inappropriate behaviour from adults and those around them and how to say no to inappropriate behaviour.

Industry

1.10 Platforms should work proactively to prevent sexual content from appearing on children's feeds and where relevant adhere to government regulations on how to do so.

1.11 Internet service providers should comply with regulations to filter and remove child sexual abuse material. Enforcing this action is vital in keeping children safe online.

^{114.} 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.'

^{115.} Government, inter-governmental agencies, and civil society need to translate and convey these messages to reach caregivers, teachers, medical staff and social support workers.

Disrupting Harm alignment with the **Model National Response**

Many countries, companies and organisations have joined the WePROTECT Global Alliance to prevent and respond to online child sexual exploitation and abuse. As a member of the Global Alliance, Ethiopia can use the Model National Response to Preventing and Tackling Child Sexual Exploitation and Abuse to help organise its response to OCSEA. The 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 Ethiopia. The evidence from Ethiopia shows that even though few of the capabilities in the Model National Response exist, they are not functioning optimally.

The Disrupting Harm recommendations primarily address legislation,116 dedicated law enforcement,117 judiciary and prosecutors,118 and education programmes.¹¹⁹ All recommendations are practical, evidence-based and actionable. Disrupting Harm has also indicated to whom its various recommendations are addressed i.e., government duty-bearers, law enforcement authorities, justice professionals, the internet and technology industry, caregivers, the community and teachers.

INSIGHT 2

Of the children who were subjected to OCSEA in Ethiopia, very few turn to formal reporting mechanisms like helplines or the police.

Government

- 2.1 Ensure an effective national hotline equipped to deal with OCSEA. It should be connected to international networks (e.g., via the INHOPE network), and be empowered to serve take-down notices on domestic Internet service providers.
- 2.2 Ensure an effective national Helpline equipped to deal with OCSEA cases. Ensure the sustainability and their ability both to receive reports and to provide psychosocial support to children. Invest in training staff at helplines to increase capacity. Helplines should be adequately resourced and staffed and must provide good quality care and support to be considered useful channels for helpseeking children. Even if children are made aware of helplines, if initial responses to disclosure and helpseeking are poor, the child - and others observing the case - will be much less likely to seek help again.
- 2.3 Invest in improving the capacity of social service workforce. Improve capacity of frontline staff in contact with children to better identify children at risk or that have experienced OCSEA. This should include teachers, staff in schools as well as health workers, in addition to all those providing psychosocial support (see recommendation 2.11).
- 2.4 Increase awareness raising efforts about hotlines and helplines as reporting and help-seeking mechanisms for OCSEA. Awareness is currently very low in Ethiopia about these mechanisms for reporting on OCSEA - and indeed reporting on any form of violence, exploitation and abuse. An important prerequisite is that helplines should be adequately resourced and provide good quality care and support. Even if children are made aware of helplines, if initial responses to disclosure and helpseeking are poor, the child - and others observing the case - will be much less likely to seek help again.

^{116.} Model National Response #3.

^{117.} Model National Response #4.

^{118.} Model National Response #5.

^{119.} Model National Response #13.

Law enforcement

2.5 Establish a clear reporting process for cases of OCSEA and facilitate widespread training for all police to ensure full implementation. Reporting of OCSEA is currently extremely low; in fact, no cases have been identified. Training and monitoring to ensure police implement child-friendly procedures whenever children are involved as victims. Include the issue of OCSEA into existing child protection reporting mechanisms.

2.6 Create mechanisms for collaboration on OCSEA between civil society organisations and law enforcement. Build tools for sharing evidence, such as secure information exchange platforms.

Caregivers, teachers, medical staff, and social support workers¹²⁰

- **2.7 Foster safe and ongoing communication** between children and trusted adults about their lives online. Normalising communication about online activities will increase the likelihood that children will disclose any concerns, risks and harmful experiences they may face.
- 2.8 Responses to disclosures of OCSEA should always convey that it is never the child's fault, whatever choices they have made. It is always the fault of the adult abusing or exploiting the child. The research shows that children subjected to OCSEA often blame themselves and feel that they had let their caregivers and others down or were judged by the police. Responses should be without judgement or punishment. For example, see guidelines on first line response to child maltreatment.
- 2.9 Try not to restrict children's internet access as a response to potential harm. This is only likely to protect children temporarily and does not teach them how to navigate similar situations in the future. This response also tends to discourage children from confiding in adults about the problems they experience. Instead communicate and educate children and adolescents on safe internet use, including how to protect themselves against OCSEA.
- 2.10 Improve capacity of frontline staff in contact with children to better identify children at risk or that have experienced OCSEA. This should include teachers/staff in schools as well as health workers, additional to all those providing psychosocial support.

Industry

2.11 Make formal reporting mechanisms within platforms clear and accessible to children and outline in child-friendly terms what the process looks like after children submit a report. Platforms and service providers must respond rapidly to reports made by children and demonstrate transparency and accountability. Internet service providers should be legally obliged to filter and remove child sexual abuse material. Enforcing this action is vital in keeping children safe online.

INSIGHT 3

The justice system has not yet processed any OCSEA cases that could be determined. There is an urgent need for ground-breaking investment in knowledge, capacity and structures for law enforcement and judicial systems to better respond to OCSEA.

Law enforcement

- **3.1 Train all police officers and prosecutors**, especially at the Kebele and Woreda levels, about the linkages between online and in-person forms of child sexual exploitation and abuse. Inform them about the provisions of law that can be used to bring charges in cases of abuse in the online environment.
- **3.2 Establish more specialised child protection units** with trained female and male personnel capable of delivering child-friendly support, and the physical spaces and equipment needed to do so. Support for this might come from the Ministry of Peace, as the National Police Force falls under this ministry.
- **3.3 Develop guidelines for police officers on how to interview children.** This will prevent children from being interviewed repeatedly, which can feel like a form of secondary victimisation. Consider developing resources, such as information about rights shareable with children seeking assistance.
- 3.4 Improve relevant law enforcement Cybercrimes Unit ability to flag/refer cases of OCSEA to global tech platforms.

^{120.} Government, inter-governmental agencies, and civil society need to translate and convey these messages to reach caregivers, teachers, medical staff and social support workers.

3.5 Establish a connection to INTERPOL's International Child Sexual Exploitation (ICSE) database.¹²¹ The ICSE database is an intelligence and investigative tool, which allows specialised investigators to share data on cases of child sexual abuse. Establish a national child abuse material database on OCSEA.

3.6 Provide an effective mechanism and adequate resources to ensure that international OCSEA referrals, including NCMEC CyberTips, are subject to an appropriate level of investigation, with a view to minimising ongoing harm to children.

Court systems and justice professionals
3.7 Include OCSEA on the agenda of the existing
National Coordination Body under the Federal
Attorney General's Office and expand participation
to include the relevant agencies on OCSEA including
the Cybercrime Unit and the Information Network
Security Agency.

3.8 Train all justice officials, including prosecutors and judges, on how to handle OCSEA cases and deliver child-friendly justice.

3.9 Ensure that the arrangements for child-friendly justice in all cases of child sexual exploitation and abuse, including those with online elements, are implemented consistently. This will require financial resources, operating procedures and training. Develop and implement programmes preparing the child victim to engage with the court system and legal actors. Ensure that child victims do not have to face the perpetrator - for example, by employing videolink technology so that evidence may be given from another room. The court methods used in the Barnahus model¹²² may also be explored for adoption. If these options are unavailable, witness protection boxes can be used (although boxing the offender rather than the child is preferable). Request a victim impact statement for OCSEA cases. This will help create awareness of the impact of OCSEA and allow the victim to feel truly seen and heard in the court process.

3.10 Operationalise the four guidelines related to the establishment of a Victim Fund. These include provision of free legal aid to children; support to children and their caregivers with temporary shelter, counselling, transportation or house rent allowances; and psychological support services.

3.11 Establish access to legal aid, psychosocial and medical services for victims of child sexual abuse and exploitation.

Government

3.12 Urgently invest in the training of police officers, prosecutors, judges/magistrates, lawyers, courtroom staff, child protection officers and frontline workers on what OCSEA is and how to address it within their respective professions, especially at Woreda and Kebele Level. Address child protection issues including OCSEA in basic training and provide specialist training more widely. Provide both initial and ongoing refresher training in next five years.

3.13 Impose legal duties on Internet service providers to retain data for a set minimum period and to filter and/or block and/or take down child sexual abuse material as well as to comply with law enforcement requests for information in a prompt manner. This will assist investigations into crimes as well as aid in controlling the wide distribution of child sexual abuse material.

3.14 Provide dedicated funding for all relevant agencies to tackling OCSEA. Responsible ministries could be the Ministry of Women, Children and Youth; the Ministry of Culture and Tourism. To better achieve this funding goal UNICEF and NGOs that work on violence against children to support the government.

Industry

3.15 Prioritise responding to data requests from the courts in cases involving children to reduce duration of trials.

Social support sector

3.16 Train all staff on the frontline of social support services. to competently recognise the unique risks and harms of OCSEA and be able to provide effective, evidence-based responses.

3.17 Social support services need to find modern and innovative ways of being accessible to young people. Helplines are one way of achieving widespread access to a child population. These need substantial investment and resourcing: their mere existence is insufficient. Other social support services require online means of access, and support from young, trained staff that understand the way children engage in their online lives.

^{121.} More information on INTERPOL's International Child Sexual Exploitation (ICSE) database can be found here.

122. The Barnahus model is a standard practice for providing child victims and witnesses of violence rapid access to justice and care.

INSIGHT 4

Important OCSEA-related legislative reform is required to facilitate action.

Government

- 4.1 Amend and update legislation to bring it fully in line with the standards set by the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography. This Protocol is relevant to combating child sexual abuse material and other crimes related to the sexual exploitation of children.
- **4.2** Accede to the Convention on Cyber Security and Personal Data Protection adopted by the African Union in 2014. With respect to OCSEA, the Convention specifically includes child sexual abuse material.
- 4.3 Consider legal amendments to align with international conventions that offer excellent guidance for addressing this issue. For example, the Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) and the Convention on Cybercrime (Budapest Convention) adopted by the Council of Europe. Although these conventions are regional commitments for Member States of the Council of Europe, the guidance they provide on OCSEA is highly relevant. While it may not be required for States outside this region to comply with these conventions, they are a useful measure of national legal frameworks related to OCSEA and they are open for accession by States which are not members of the Council of Europe.
- 4.4 Amend legislation to more comprehensively criminalise conduct related to child sexual abuse material, and explicitly criminalise the livestreaming of child sexual abuse, and sexual extortion committed in the online environment, and online sexual harassment. While the Computer Crime Proclamation provides the procedural rules needed to assist law enforcement officers in the investigation of OCSEA cases, its provisions fail to include what constitutes child sexual abuse material, depictions of the sexual parts of a child's body for primarily sexual purposes, non-visual materials, or digitally generated child sexual abuse material including realistic images of non-existing children. Moreover, it does not include among the criminalised conduct, knowingly obtaining access to child sexual abuse material.
- **4.5** Amend legislation in such a way as to extend the crime of online grooming for sexual purposes to situations where the sexual abuse is not the result of a meeting in person but is committed online (e.g., when children are manipulated to produce child sexual abuse material and share it with the offender).¹²⁴

^{123.} OHCHR. (2000). Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.

124. The Lanzarote Committee recommend States Parties to the Convention to adopt this broader understanding of online grooming in its 2015 opinion on Article 23 of the Convention: Council of Europe's Lanzarote Committee. (2015). Opinion on Article 23 of the Lanzarote Convention and its explanatory note. Para 20.

ACKNOWLEDGEMENTS

ECPAT International, INTERPOL, and UNICEF Office of Research - Innocenti have greatly appreciated the unique opportunity to work shoulder-to-shoulder to generate evidence on the context, threats and children's perspective of OCSEA in Ethiopia. This comprehensive report is the result of a two-year collaborative effort to design, gather and analyse extraordinary evidence. These efforts would not have been successful without the engagement of so many Ethiopian people and partners.

The project partners would like to express their appreciation to everyone who engaged with *Disrupting Harm* by:

- Endorsing or contextualising the findings: African Union, Ministry of Science and Higher Education, Ministry of Women, Children and Youth.
- Supporting the data collection: Emmanuel Development Association (EDA), INTERPOL National Central Bureau-Addis Ababa, Ipsos MORI, TRIBOND Research and Consulting PLC, UNICEF Eastern and Southern Africa Regional Office, UNICEF Ethiopia Office.
- Sharing expertise and experiences through interviews and completing surveys: 06 Kebele CCC, 08 Kebele CCC, Alem children support organisation, African Humanitarian Action, African Network for the Prevention and Protection against Child Abuse and Neglect, Association for the Rehabilitation of Girls, Arat Kilo Child Care and Community Development, Beza Posterity Development Organization, Caring for Vulnerable Children Project, Child Aid and Development, Child Development Training and Research Center, Child Justice Project Office, Cybercrime Investigation Division, Cybercrime Unit, Dessie City Woreda Court, Dessie City Women, Youth and Children's Office, Ethiopian Women Lawyers Association, Federal Attorney General's Office, Federal Supreme Court, Freedom Fund, Forum on Sustainable Child Empowerment, Ministry of Culture and Tourism, Ministry of Education, Ministry of Innovation and Technology, Ministry of Women, Children and Youth, Mission for Child Development, Norwegian Refugee Council, Plan International, Professional Alliance for Development, Safe Migration Project, Terre des Hommes Ethiopia, UNICEF Ethiopia country office, and UNODC Programme Office in Ethiopia, Wollo University.

Without the collaborative effort of all staff, consultants, translators, and interns involved in the reports, this tremendous piece of research would not have come together. In particular, we would like to thank:

ECPAT International: Tiago Afonso,

Dr Victoria Baines, Alice Beaven, Will Beaven, Willy Buloso, Yermi Brenner, Dr Mark P. Capaldi, Narciso Cumbe, Dr Dorothea Czarnecki, Jarrett Davis, Rangsima Deesawade, Julia Durska, Sonia Espallargas Val, Anneka Farrington, Beatrice Gacengo, Thiyagu Ganesan, Dr. Susanna Greijer, Zipporah Goetze, Josefin Hagstrom, Alastair Hilton, Maria Ibañez Beltran, Worrawan Jirathanapiwat, Supriya Kasaju, Dr Mark Kavenagh, Bernard Kennedy, Dorine van der Keur, Susan Kreston, Marie Laure Lemineur, Raphaelle Lecler, Katrina Mariswamy, John McGill, Mark McKillop, Stella Motsi, Florence Mueni, Manida Naebklang, Cathrine Napier, Rumbidzai Ngindi, Freddie Nickolds, Megan Northey, Esther Obdam, Dr Nativity Petallar, Dr Kirsten Pontalti, Marie Joy Pring, Dr Ethel Quayle, Marita Rademeyer, Kieran Rumsby, Jennifer Schatz, Guncha Sharma, Nong Socheat, Chitrapon Vanaspong, Andrea Varrella, Kirsten Walkom, Timothy Williams.

UNICEF Office of Research - Innocenti:

Dr David Anthony, Dr Daniel Kardefelt-Winther, Marie Nodzenski, Marium Saeed, Rogers Twesigye.

INTERPOL's Crimes against Children Unit

The partners also acknowledge the guidance of the <u>Panel of Advisors</u> and the extraordinary financial investment in this project from the Global Partnership to End Violence against Children, through its Safe Online initiative. The <u>Disrupting Harm</u> partners are grateful to the Safe Online team for its conceptualisation of <u>Disrupting Harm</u>, its technical contributions, and its unwavering support.

Our biggest thanks go to the children who contributed – especially the young people who had experienced OCSEA and courageously spoke of it with the research teams. The experiences of children are key to understanding and guiding our way forward.

