DISRUPTING HARM IN KENYA

Evidence on online child sexual exploitation and abuse

Funded by End Violence Against Children

Implemented by ECPAT INTERPOL unicef Office of Research-Innocenti

Suggested citation:
ECPAT, INTERPOL and UNICEF. (October, 2021). *Disrupting Harm in Kenya: Evidence on online child sexual exploitation and abuse*. Global Partnership to End Violence against Children.

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

CONTENTS

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 General Comment No. 25 adopted in 2021. The General Comment also stresses the fact that spending time online inevitably brings unacceptable risks and threats of harm, some of which children also encounter in other settings and some of which are unique to the online context.

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

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

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

Disrupting Harm represents the most comprehensive and large-scale research project ever undertaken on online child sexual exploitation and abuse at a national level and has resulted in 13 country reports and 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 we can do to prevent them.

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

Disrupting harm to children is everyone's responsibility.

Dr Howard Taylor
Executive Director
End Violence Partnership

EXECUTIVE SUMMARY

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

Perceptions of online risks

The great majority of caregivers in Kenya are highly concerned that their children will talk to people online whom they have never met in person, or encounter sexual images on the internet. Caregivers generally use the internet less than their children, and their ability to guide them may be limited.

Meanwhile, two-thirds of internet-using children have not been taught about how to stay safe online. Their awareness of the risks varies. In the *Disrupting Harm* Kenya household survey of 1,014 internet-using children age 12-17 and their caregivers, 14% of the children had met someone face-to-face after first encountering them online in the past year. According to children, many of these encounters did not result in immediate harm and most respondents described being pleased about the outcome. Although these encounters tended to be positive for children in our survey, this remains a risky activity, the outcome of which can be highly variable. Children should therefore not meet with online contacts in person without taking some safety precautions like informing a trusted adult, only meeting in public places, and never meeting the person alone. Six per cent (60 children) had shared naked images or videos of themselves with other internet users in the past year. While such images are most frequently shared voluntarily among peers and close friends, seven children had shared naked images as a result of threats and six said they were pressured by their friends.

> Children are subjected to these potential and actual instances of sexual exploitation and abuse both online and offline. In Kenya, most children who have been exposed to any manifestation of OCSEA have also been subjected to physical, sexual or emotional violence in person.

Potential and actual instances of sexual exploitation and abuse

As part of the household survey, children were asked whether they had been subjected to a range of potential and actual instances of online sexual exploitation and abuse (OCSEA) within the past year. OCSEA refers to situations that involve digital or 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.

Potential instances of OCSEA included, for example, unwanted requests to talk about sex and unwanted requests for images showing their private parts. Actual instances of OCSEA included, for example, being offered gifts in return for sexual images and being threatened or blackmailed online to engage in sexual activities. The proportions of children who said that these things had happened to them varied between 5% and 13%, depending on the question. Most children who were subjected to possible grooming attempts refused to do as asked. However, a small proportion complied with unwanted requests to talk about sex or share sexual images. Seven percent of all children surveyed said sexual images of them had been shared without their permission in the past year.

Children are subjected to these potential and actual instances of sexual exploitation and abuse both online and offline. In Kenya, most children who have been exposed to any manifestation of OCSEA have also been subjected to physical, sexual or emotional violence in person.

Consistent with the evidence about violence against children offline, persons already known to the child were responsible for most of the potential and actual instances of OCSEA disclosed by respondents of the household survey. In many cases, these persons were other children. Even so, there were many instances where the offenders were adults. These instances could be evidence of grooming of children with a view to sexually abusing and exploiting them in person and/or for the creation of child sexual abuse material (CSAM). People unknown to the child were involved in about one incident in four. This has significant implications for prevention and awareness raising, as many awareness efforts focus primarily on the threat from strangers rather than people the child already knows. This should also be a consideration for response systems, as it could be much more difficult for victims to seek help if they are emotionally and/or economically dependent on abusers.

Disclosure of online sexual exploitation and abuse

Many incidents of OCSEA go undisclosed and formally unreported. Approximately one-third of the children surveyed who had been subjected to OCSEA had told nobody, and those who did tell someone, confided mainly in their friends. Only a minority had told their caregivers or other adults and very few went to the police or spoke to a social worker or helpline. The main reasons given for not disclosing were a lack of awareness about where to go or whom to tell, feeling embarrassed or ashamed or that it would be emotionally too difficult to talk about it, and fear of getting in trouble. Frontline workers attributed this to strong taboos regarding sex in Kenya. As shown in the household survey with children, these feelings of shame and embarrassment affect both girls and boys. The criminalisation of homosexuality adds an additional layer of stigma that may contribute to silencing children who are abused by an offender of the same sex.

> Many children in Kenya did not tell anyone the last time they were subjected to OCSEA.

> Some people hold the belief that sexual abuse that only happens in the online environment is not ‘real’ abuse.

Interviews were conducted with nine Kenyan girls who had been sexually assaulted by offenders who got to know them online. These girls revealed that they were initially deceived by compliments, gifts and promises and did not realise they were being groomed into OCSEA. Later they were too ashamed and fearful of stigma or repercussions to tell anybody. Eventually they went to individuals or organisations outside the family for support, or were obliged to tell their stories because they had become pregnant.

While most caregivers say they would tell the police if their children were sexually abused, others said they would not report due to concern about negative consequences, fear of not being treated properly and/or a belief that reporting would have no effect. In our frontline workers’ survey, more than half of respondents said that cases of OCSEA are not being reported because services are not trusted. In addition, frontline workers said that many adults may not know that certain types of behaviour online are serious and punishable offences. Some people hold the belief that sexual abuse that happens in the online environment is not 'real' abuse.

Law enforcement data

The numbers of OCSEA cases handled by the Kenyan police were not provided on a national level but rather from the specialised unit. The Anti Human Trafficking and Child Protection Unit (AHTCPU) of the Directorate of Criminal Investigations alone handled 3,160 OCSEA cases in 2018 and 4,133 in 2019. These are the reported numbers and do not provide a complete picture of OCSEA prevalence. Frontline workers surveyed indicated that the offenders are most commonly adult members of the community in which the child lives. Some limited evidence was discovered of links between OCSEA and travel and tourism.

Between 2017 and 2019, the Kenyan law enforcement authorities received an average of 13,572 CyberTips per year from globally popular online platforms based largely in the United States via the U.S. National Center for Missing and Exploited Children (NCMEC). In 2020, the number was 14,434. Almost all of these reports concerned apparent cases of the possession, manufacture and distribution of CSAM in Kenya. While Facebook submitted 93% of the reports, numerous other electronic service providers also submitted reports, suggesting the misuse of a range of platforms by OCSEA offenders. Research using Google Trends points to interest in CSAM in Kenya including image and video content depicting sexual activity with and between teenagers, with children, and with babies.

Investigating cases and treatment of victims in the justice system

Findings from the capacity assessments of law enforcement and access to justice interviews revealed that often the police and prosecutors have difficulty knowing how to recognise, investigate and prosecute OCSEA cases. This reflects both gaps in legislation and a lack of access to training on these issues. The Computer Misuse and Cybercrimes Act defines CSAM and criminalises acts associated with it quite explicitly, while the Sexual Offences Act sets the age of sexual consent at 18. However, no specific references are made in either law to live-streaming, online grooming for sexual purposes or sexual extortion in the online environment. These potential loopholes may be plugged when the upcoming Children Bill 2021, currently before Parliament, is enacted.

Among the young people who were interviewed about their experiences in accessing justice after being victims of OCSEA, some had positive experiences with the police but most were disappointed. For example, some children were not informed about their rights or questioned sensitively. Some complained of officers expressing harsh opinions and judging them. Most children and caregivers did not sense a determination to bring the offenders to justice. Some caregivers felt that they were left out of the process. Only a minority of regular police stations have child protection units and these may not be able to retain trained staff. The vast majority of the frontline workers we spoke to rated the law enforcement officers' awareness and response to OCSEA as 'poor' or 'fair'.

Children, justice and social services

Similarly, most children and caregivers who had experiences of going through the formal justice system for an OCSEA case found it discomforting. Not all cases can be heard in a Children's Court, where child-friendly procedures are favoured. The Victim Protection Act envisages that the dignity of victims be preserved, and that each victim should be treated in accordance with his or her age and be protected from secondary victimisation. However, there are no specific operating procedures for how to implement this in practice. Knowledge of OCSEA among justice professionals is limited. Despite the efforts made to put children at ease, several children we spoke to still had to give evidence repeatedly and faced stigma and victim-blaming. Victim impact assessments were not always carried out. Although children are entitled to free legal aid and counselling, these services were not provided to most of the child survivors we spoke to. Where provided, they are not always free.

Investigations and trials of OCSEA cases are often drawn out, which delays justice and prevents child victims from moving on. Besides pressure on the courts and lack of expertise, another reason for this is the difficulty of obtaining evidence from internet service providers, either because they respond late to court orders or because they do not store data for a sufficiently long period. Safaricom, the largest mobile telecommunications operator in Kenya, has reportedly taken steps to expedite its response to requests for evidence.

The Victim Protection Act provides victims of crimes, including OCSEA, with free access to counselling, shelter and reintegration services. The Department of Children's Services under the Ministry of Labour and Social Protection seeks to provide these services to OCSEA victims with the support of civil society organisations. However, duty-bearers interviewed indicated that the Department itself is understaffed and the availability of services is limited, especially in rural areas. More than half of the frontline workers we surveyed rated the availability and quality of psychological services as either 'poor' or 'fair'.

The Anti-Human Trafficking & Child Protection Unit (AHTCPU)

The establishment of the AHTCPU under the Directorate of Criminal Investigations, first in Nairobi and more recently in Mombasa, is a good step towards improving responses to OCSEA. The Unit investigates cases of OCSEA which are reported to it in various ways or referred to it by regular police stations. The Unit staff are specialised in such cases and have close links with the Department of Children's Services.

The Unit can also advise regular police stations, take over cases from them and provide training to other professionals on handling cases of OCSEA. However, it has a very limited staff: there are currently just five officers dedicated to the investigation of OCSEA cases.

International cooperation and civil society

Both the AHTCPU and the National Kenyan Computer Incident Response Team cooperate with INTERPOL and other international partners to prevent and respond to OCSEA. There are working arrangements between the Kenyan law enforcement authorities and companies like Facebook and Google for obtaining information during investigations. Several international organisations have supported Kenya with mentorship, training, and equipment in areas related to OCSEA.

International and domestic civil society organisations play a major part in responding to OCSEA in Kenya. They refer cases to the police and the courts and cooperate with the Department of Children's Services in the provision of services like shelter, counselling and legal aid. They are also involved in awareness raising activities and in training the child protection workforce. However, these efforts are not sufficient to address these crimes fully.

Current initiatives for children

Interviews with government duty-bearers demonstrate that the Government of Kenya is aware of the threat of OCSEA and the need for cooperation and collaboration to counter it. It has established a National Technical Working Group on Child Online Protection which brings together mandated government agencies, civil society organisations, industry representatives and UN agencies. Government agencies have also conducted various awareness raising and training initiatives, albeit with limited reach so far.

Two national policies which touch on OCSEA are the National Plan of Action Against Sexual Exploitation of Children in Kenya, 2018-2022 and the National Information, Communications and Technology Policy (2019). However, neither policy has been widely disseminated publicly across all relevant stakeholders..

Two more specific policies are under development. One is the National Plan of Action on online child sexual exploitation and abuse, spearheaded by the Department of Children's Services. The National Plan of Action is in the final stages of development and is anchored in the WePROTECT Model National Response. The second is a National Strategy on Child Online Protection, which is led by the Communications Authority of Kenya and will embody the International Telecommunications Union Guidelines on Child Online Protection.

Key insights

The report for Kenya concludes by highlighting five key insights from the research:

1. Internet-using children in Kenya are subjected to OCSEA. According to children who were subjected to OCSEA and frontline workers, most offenders

are someone the child already knows. These crimes can happen while children spend time online or in person but involving technology.

2. Many children in Kenya did not tell anyone the last time they were subjected to OCSEA. Children tend to disclose to people they know rather than reporting to a helpline or the police.
3. Among children who were subjected to OCSEA through social media, Facebook and WhatsApp were the most common platforms where this occurred.
4. The law enforcement, justice and social support systems have inadequate awareness, capacity and resources to respond to cases of OCSEA.
5. Important OCSEA-related legislation, policies and standards are not yet enacted in Kenya.

The report ends with a detailed map for action to be taken by the government, by the law enforcement, justice and social services sectors and by those working within them, by communities, teachers and caregivers, and by digital platforms and service providers. These are too detailed to be recounted in the Executive Summary but can be found on page 92 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 for governments' approaches to prevention and response. Informed by the 2018 WeProtect Global Alliance Threat Assessment[1] the Global Partnership to End Violence against Children, 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 in Kenya 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 Kenya was finalised in May 2021. Using the same methodology 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 Kenyan policy makers to tackle online child sexual exploitation and abuse and strengthen victim support. In addition, the findings and advised next steps are expected to have relevance for a broader global audience. The recommendations made in the report are aligned with the WeProtect Model National Response[2] and contribute to the 2030 Agenda for Sustainable Development.[3]

Summary of methods used by ECPAT in Kenya

Government duty-bearer interviews

Twelve semi-structured interviews were conducted between May 2020 and July 2020 with a total of 16 senior national duty-bearers[4] with mandates that include OCSEA. Due to the COVID-19 pandemic, some interviews were conducted in person and some virtually. More information on the methodology can be found here, while the preliminary report of this data can be found here. Attributions to data from these respondents have ID numbers beginning with RA1 throughout the report.[5]

Analysis of non-law enforcement data and consultations

A range of non-law enforcement stakeholders have data and insight on the nature and scale of OCSEA. Data were obtained from INHOPE, the Internet Watch Foundation 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.

Frontline social service providers' survey

A convenience sample of 50 client-facing frontline workers in Kenya – such as outreach youth workers, social workers, case managers, psychologists, and some health and legal professionals directly working

[1] WeProtect Global Alliance (2018). Global Threat Assessment 2018: Global Threat Assessment 2018: Working together to end the sexual exploitation of children online. London: WeProtect Global Alliance.
[2] WeProtect Global Alliance (2016). Preventing and Tackling Child Sexual Exploitation and Abuse: A model national response.
[3] United Nations. (n.d.) Sustainable Development Goals. See: Goals 5.2, 8.7 and 16.2.
[4] 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: the Communications Authority of Kenya, the National Council of Children's Services, UNICEF Kenya Country Office, the NCAJ Special Task Force on Children Matters, the Kenya Film and Classification Board, the Office of the Director of Public Prosecutions, the Child Online Protection Unit, the Department of Children's Services, the Ministry of Labour and Social Protection, the Kenya Law Reform Commission, the Kenya Institute of Curriculum Development and the National KE-CIRT/CC.
[5] The format RA1-KY-01-A is used for IDs. 'RA1' indicates the research activity, 'KY' denotes Kenya, '01' is the participant number and 'A' indicates the participant when interviews included more than one person.

with children's cases – participated in a survey administered online during April and May of 2020. This research activity aimed to explore the scope and context of OCSEA as it is observed by those working the social support front line to prevent it and respond to it. More information on the methodology can be found here, while the preliminary summary report of this data can be found here. Attributions to data from these respondents have ID numbers beginning with RA3 throughout the report.

Access to Justice interviews with OCSEA victims and their caregivers

Ten interviews were conducted between June and August of 2020 with children (all girls) aged between 15 and 18 years who had accessed the legal system for OCSEA cases. The girls' caregivers were also interviewed. The children and caregivers decided themselves whether to be interviewed separately or jointly. Only one child chose to be interviewed in the presence of her caregiver. 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 Kenya. Despite deliberate efforts to identify males, the study in Kenya was unable to identify any male children who had been through the legal system. The female participants for this activity came from seven of the 47 counties in Kenya – namely Migori, Nairobi, Eldoret, Meru, Makueni, Nakuru and Mombasa. More information on the methodology can be found here, while the preliminary summary report of this data can be found here. Attributions to data from these respondents have ID numbers beginning with RA4 throughout the report. Note that the suffix 'child' or 'caregiver' is also included in the ID numbers to indicate interviews with children and caregivers.

Access to Justice interviews with justice professionals

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

Literature review and legal analysis

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

Conversations with OCSEA survivors

Unstructured, one-on-one conversations led by trauma-informed expert practitioners were arranged with 33 young survivors of OCSEA in five 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. The survivor conversations were analysed collectively for all countries and lessons are weaved through all the national reports. The Kenya report presents data from the nine Kenyan female survivors. More information on the methodology can be found here. The report presenting the analysis of all 33 survivor conversations will be released separately in late 2021. Attributions to data from these respondents have ID numbers beginning with RA5.

Summary of methods used in Kenya by INTERPOL

Quantitative case data analysis

Data was sought on cases related to OCSEA from law enforcement authorities via the INTERPOL National Central Bureau in each country. Data were also obtained from the mandated reports of U.S. based technology companies to the National Center for Missing and Exploited Children (NCMEC) and from a number of other partner organisations with a view to deepening the understanding of relevant offences committed in the country, offender and victim behaviour, crime enablers and vulnerabilities. Crime data was analysed for the three years from 2017 to 2019.

[6] The interviewees comprised one lawyer, one prosecutor, one magistrate, one representative from the Department of Children's Services, three police officers (two representing the AHTCPU and one who was a former investigator with the Cybercrime Unit), three counsellors (one from the International Justice Mission, one formerly with Childline Kenya and the other formerly with CRADLE), and two child rights advocates involved in outreach activities on child online protection – one from Watoto Watch Network and the other from Mtoto News.

Qualitative capacity assessments

In addition to seeking data on OCSEA cases, INTERPOL requested data on the capacity of 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 this activity have ID numbers beginning with RA8 throughout the report.

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

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

Household survey of internet-using children and their caregivers

In order to understand children's use of the internet, the risks and opportunities they face online, specifically OCSEA, a nationally representative household survey was conducted with 1,014 internet-using children. The target population for the survey was children aged 12-17 in Kenya who have used the internet in the three months before the interview. Additionally, one parent or caregiver of each child was interviewed. The interviews were conducted in person.

To achieve a nationally representative random sample, the survey used random probability sampling with national coverage. In Kenya, fieldwork coverage was 100%. Coverage is defined as the proportion of the total population that had a chance of being included in the survey sample – meaning that the fieldwork would cover the area where they live if sampled. This means that all eight provinces of Kenya (Central, Coast, Eastern, Nairobi, North Eastern, Nyanza, Rift Valley and Western) were represented in our sample. Although in recent years counties have been used in preference to provinces in official classifications, provinces were used to determine the proportional allocation of PSUs (stratification) in Kenya given the number of counties was too many for this purpose. However, all counties had an equal chance of selection into the sample and the population is representative at the national level.

The sampling followed a three-stage random probability clustered sample design. At the first stage, 100 primary sampling units (PSUs) were selected. The PSU list was provided by the Kenya National Bureau of Statistics (KNBS). At the second stage, interviewers randomly 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.

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

The fieldwork took place between 21 December 2020 and 19 January 2021. Data collection was carried out by IPSOS MORI on behalf of UNICEF Office of Research – Innocenti.

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

Ethical Approval

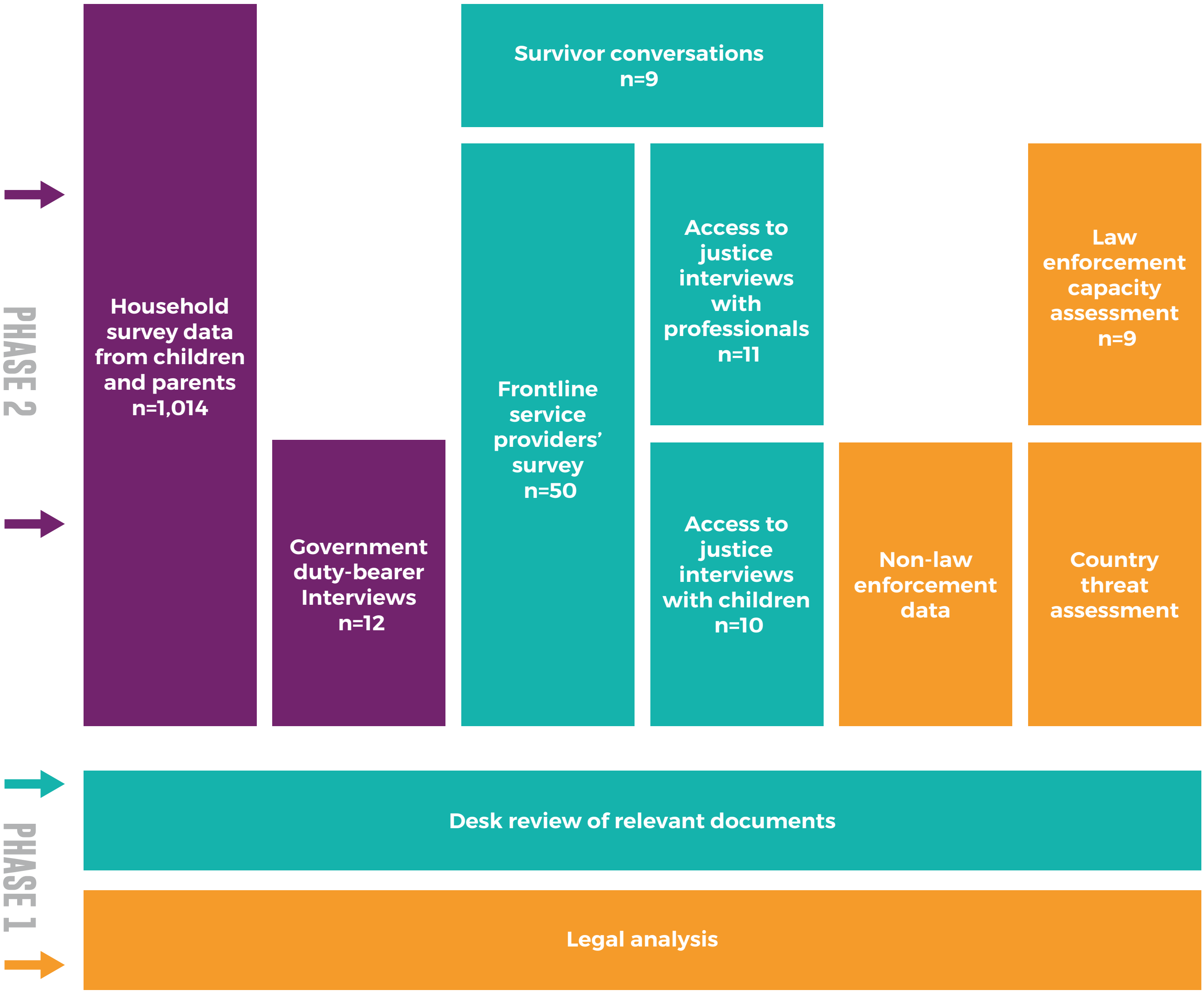
The ECPAT and UNICEF research components were reviewed and approved by AMREF Health Africa – Science and Ethical Review Committee. UNICEF also obtained required research approval for the household survey from the National Commission for Science, Technology and Innovation (NACOSTI). ECPAT and UNICEF's protocols were also reviewed and approved by HML Institutional Review Board.

INTERPOL has assessed the threat and the capacity of law enforcement on countering the threat. Both assessments entailed interviews with law enforcement in relevant units and national agencies dealing with OCSEA. Similarly to UNICEF, INTERPOL obtained NACOSTI approval. The team has taken an online course on Responsible Conduct of Research from the Collaborative Institutional Training Initiative and followed the INTERPOL's Code of Conduct.

National Consultation

A national consultation took place on 8 June 2021. Government and non-governmental organisations were asked to comment on the *Disrupting Harm* recommendations with the objective to ensure that the recommendations were relevant for the Kenyan context.

Figure 1: *Disrupting Harm* methods in Kenya


PHASE 2
Household survey data from children and parents n=1,014
Government duty-bearer Interviews n=12
Survivor conversations n=9
Frontline service providers' survey n=50
Access to justice interviews with professionals n=11
Access to justice interviews with children n=10
Non-law enforcement data
Law enforcement capacity assessment n=9
Country threat assessment
PHASE 1
Desk review of relevant documents
Legal analysis

ABOUT ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE

***Child sexual abuse* refers to various sexual activities perpetrated on children (persons under 18), regardless of whether the children are aware that what is happening to them is neither normal nor acceptable. It can be committed by adults or peers and usually involves an individual or group taking advantage of an imbalance of power. It can be committed without explicit force, with offenders frequently using authority, power, manipulation or deception.[7]**

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

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

Differentiating between 'online' and 'offline' child sexual exploitation and abuse as two completely separate forms of violence does not help us to understand, prevent or respond to the issue, nor is it the intention of *Disrupting Harm* to make such a distinction. Children can be abused or exploited while they spend time in the digital environment, but equally, offenders can use digital technology to document and share images of in-person abuse and exploitation.

Disrupting Harm also focuses on how technology *facilitates* child sexual exploitation and abuse and contributes much-needed evidence to understand the role digital technology plays in perpetrating sexual violence against children.

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

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

- Production, possession or sharing of **child sexual abuse material (CSAM):** Photos, videos, audios or other recordings, or any other representation of real or digitally generated child sexual abuse or sexual parts of a child for primarily sexual purposes.[11]
- **Live-streaming of child sexual abuse:** Child sexual abuse that is perpetrated and viewed simultaneously in real-time via communication tools, video conferencing tools and/or chat applications. In most cases, the offender requesting the abuse in exchange for payment or other material benefits is physically in a different location from the child(ren) and the facilitators of the abuse.
- **Online grooming of children for sexual purposes:** Engagement with a child via technology with the intent of sexually abusing or exploiting the child. While international legal instruments[12] criminalising grooming indicate that this must take place with intent to meet the child in person, it has become

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

[8] *Ibid.*, 24.

[9] 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.

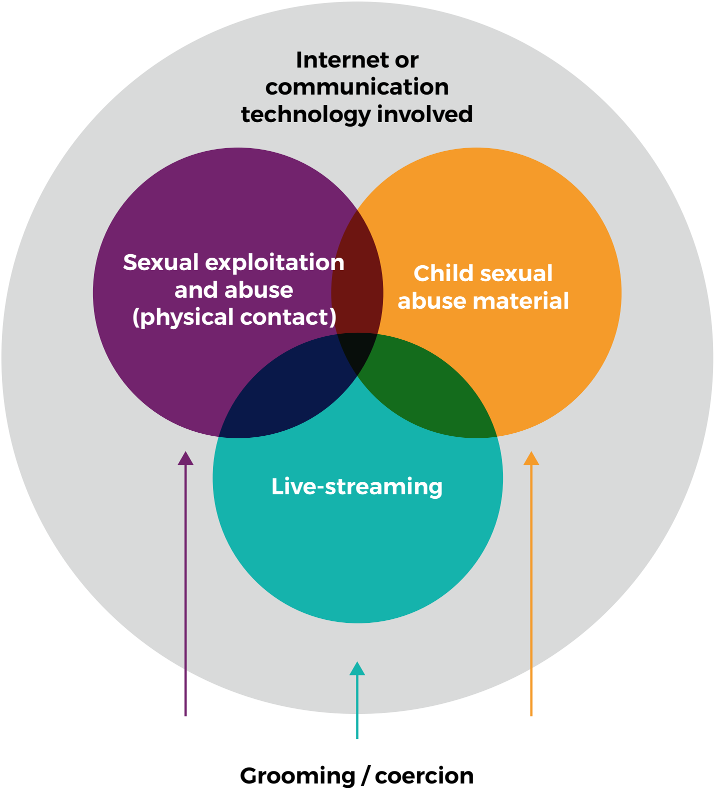
[10] Stoilova, M., Livingstone, S., Khazbak, R. (2021). Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the evidence on children's internet use and outcomes. Innocenti Discussion Papers no. 2021-01, Florence: UNICEF Office of Research – Innocenti.

[11] Interagency Working Group on Sexual Exploitation of Children. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Bangkok: ECPAT International. 40.

[12] The only two legally binding international instruments containing an obligation to criminalise the grooming of children for sexual purposes are: Council of Europe. (2007). Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. Council of Europe Treaty Series – No. 201. Article 23; and European Parliament and Council. (2011). Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. Article 6.

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.

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


Internet or communication technology involved
Sexual exploitation and abuse (physical contact)
Child sexual abuse material
Live-streaming
Grooming / coercion

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

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

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

Sexual harassment of a child[15] and **unwanted exposure of a child to sexual content**[16] are other phenomena which can impact and 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 program 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.

[13] Cooper, K., Quayle, E., Jonsson, L. & Svedin, C.G. (2016). Adolescents and self-taken sexual images: A review of the literature. Computers in Human Behavior, vol. 55, 706-716.
[14] Interagency Working Group on Sexual Exploitation of Children. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Bangkok: ECPAT International. 52.
[15] *Ibid.*, 21.
[16] *Ibid.*, 44.

ABOUT KENYA – DEMOGRAPHICS AND INTERNET USAGE

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

The available data presented here 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:

52,574,000[17]

(2018: 51,393,000)[18]

Census data:

47,564,000[19]

FEMALE POPULATION 2019

UN data:

26,452,000[20]

(2018: 25,859,000)[21]

Census data:

24,015,000[22]

MALE POPULATION 2019

UN data:

26,122,000[23]

(2018: 25,534,000)[24]

Census data:

23,548,000[25]

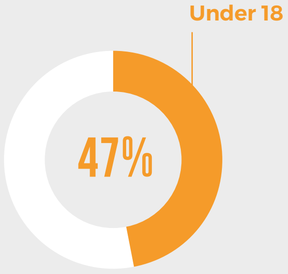
POPULATION UNDER 18 2018

UN data:

23,965,000[26]

Census data:

NO DATA

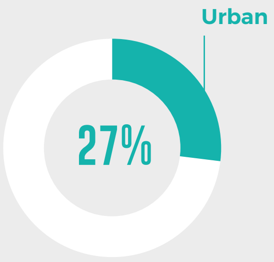


MEDIAN AGE 2020[27]

20.1

URBAN POPULATION 2018: 27%[28]

2030 prospect: 33.4%[29]



CHILDREN IN RURAL AREAS IN KENYA CONTINUE TO HAVE MUCH LESS ACCESS TO HEALTH, SECURITY & EDUCATION THAN THOSE LIVING IN URBAN AREAS.[30]

[17] United Nations Population Division. (n.d.). World Population Prospects 2019.
[18] *Ibid.*
[19] Republic of Kenya. (2019). 2019 Kenya Population and Housing Census. Volume I: Population by County and Subcounty.
[20] United Nations Population Division. (n.d.). World Population Prospects 2019.
[21] *Ibid.*
[22] Republic of Kenya. (2019). 2019 Kenya Population and Housing Census. Volume I: Population by County and Subcounty.
[23] United Nations Population Division. (n.d.). World Population Prospects 2019.
[24] *Ibid.*
[25] Republic of Kenya. (2019). 2019 Kenya Population and Housing Census. Volume I: Population by County and Subcounty.
[26] UNICEF. (2019). The State of the World's Children 2019. UNICEF, New York.
[27] United Nations Population Division. (n.d.). World Population Prospects 2019.
[28] United Nations Population Division. (n.d.). World Urbanization Prospects: The 2018 Revision.
[29] United Nations Population Division. (n.d.). World Population Prospects 2019.
[30] UNICEF. (2018). Country Office Annual Report 2018 – Kenya.

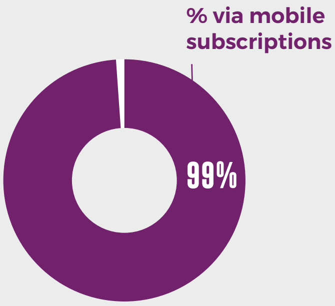
ABOUT KENYA – DEMOGRAPHICS AND INTERNET USAGE

TOTAL INTERNET SUBSCRIPTIONS[31]

Oct –Dec 2020:

44,391,490[32]

For comparison, in Oct-Dec 2019 the number of subscriptions stood at 39,657,090 – also 99% mobile[33]



INTERNET USE AMONG CAREGIVERS OF INTERNET-USING CHILDREN

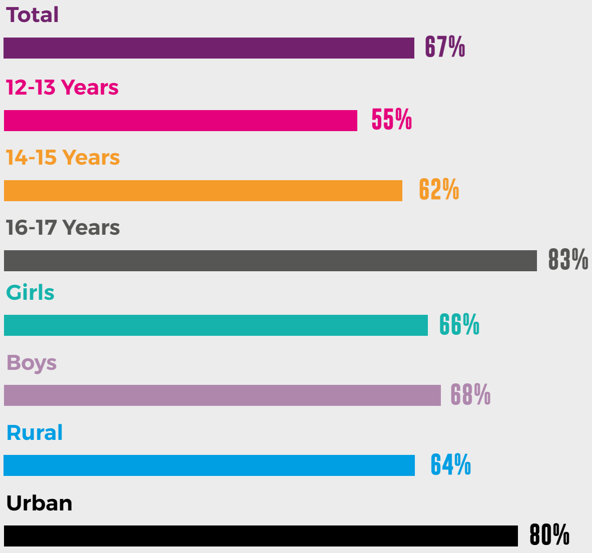
Source: Disrupting Harm data

51%

n = 1,014 caregivers of internet-using children.

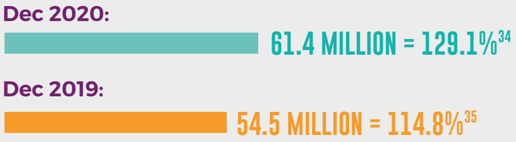
Source: Disrupting Harm data

2020 INTERNET PENETRATION RATES AMONG 12-17-YEAR-OLDS[33]



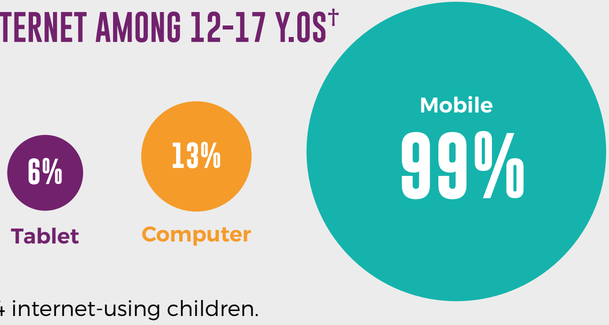
n = 1,879 households.

MOBILE (SIM) PENETRATION



MOST POPULAR DEVICE TO ACCESS THE INTERNET AMONG 12-17 Y.OS†

Source: Disrupting Harm data

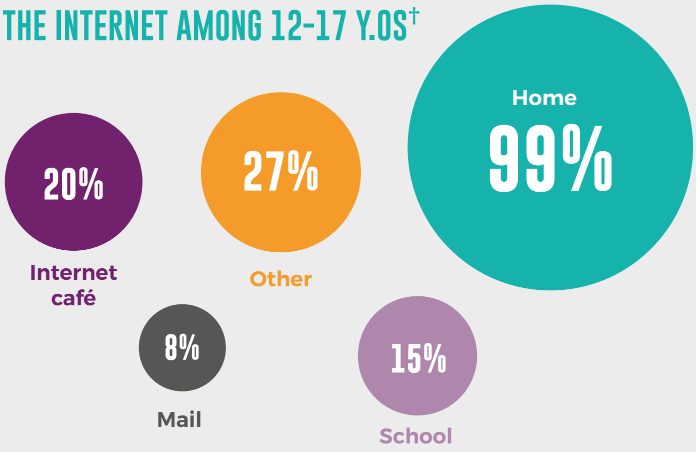


n = 1,014 internet-using children.

†Multiple choice question

MOST POPULAR PLACE TO ACCESS THE INTERNET AMONG 12-17 Y.OS†

Source: Disrupting Harm data



n = 1,014 internet-using children.

†Multiple choice question

GDP PER CAPITA 2019 (US$)

$1,816.5[36]

ONE OF THE FASTEST GROWING ECONOMIES IN SUB-SAHARAN AFRICA IN 2019[37]

[31] The number of subscriptions is not reflective of the number of unique users.

[32] Communications Authority of Kenya. (2020). Second Quarter Sector Statistics Report for the Financial Year 2020/2021 (October-December 2020).

[33] Communications Authority of Kenya. (2019). Second Quarter Sector Statistics Report for the Financial Year 2019/2020 (October-December 2019).

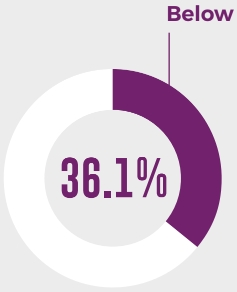
[34] Communications Authority of Kenya. (2020). Second Quarter Sector Statistics Report for the Financial Year 2020/2021 (October-December 2020).

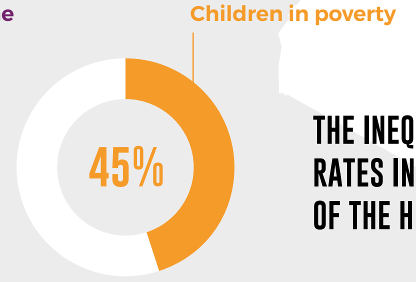
[35] *Ibid.*

[36] World Bank. (2020). GDP per capita (current US$) – Kenya.

[37] World Bank. (2021). Kenya Overview.

POVERTY RATES





THE INEQUALITY GAP (HIGHEST RATES IN RURAL AREAS) IS ONE OF THE HIGHEST IN AFRICA

2014

Approximately 8,300 people owned 62% of the country's wealth).[38]

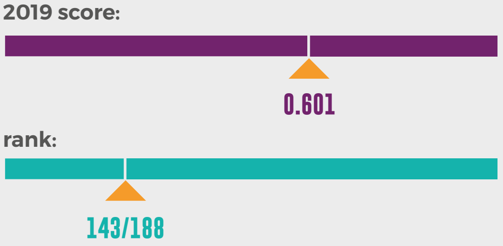
2015

36.1% of the population still lived below the national poverty line[39]

2017

According to the UNICEF Kenya 2017 Annual Report, 45% of children under 18 (9.5 million children) were experiencing poverty in Kenya (stark inequities – 85% in Turkana county compared to 7% in Nairobi)[40]

HUMAN DEVELOPMENT INDEX



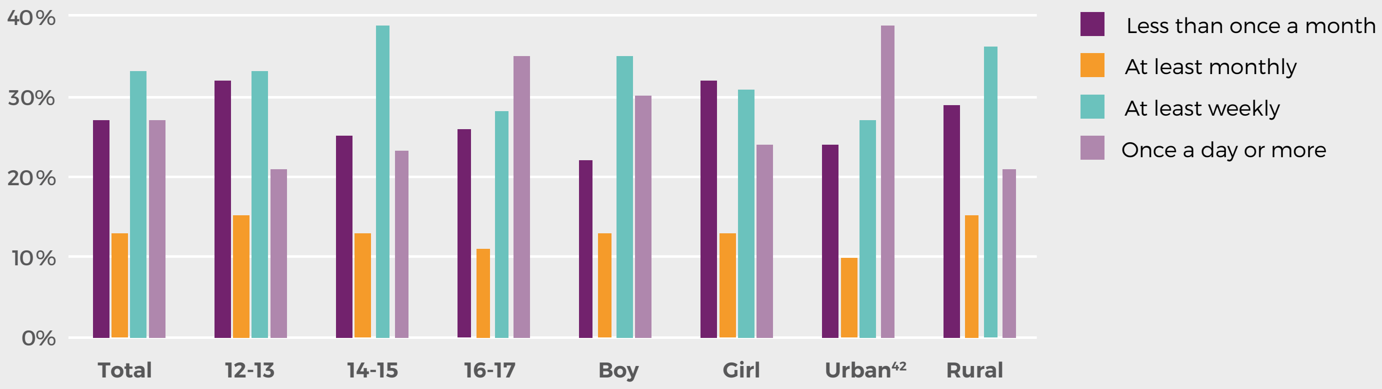
The Human Development Index (HDI) is a summary measure of average achievement in key dimensions of human development: a long and healthy life, being knowledgeable and having a decent standard of living. The HDI is the geometric mean of normalised indices for each of the three dimensions.

OFFICIAL LANGUAGES[41]

ENGLISH
SWAHILI

FREQUENCY OF INTERNET USE AMONG 12-17 YEAR OLDS

Source: Disrupting Harm data



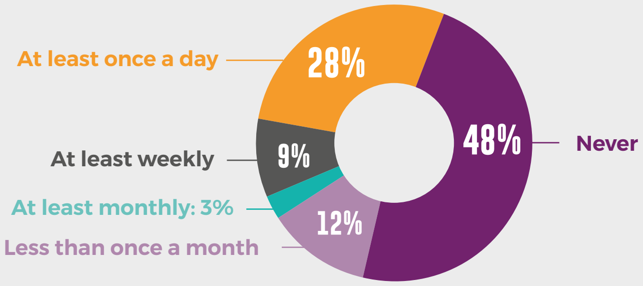
n = 1,014 internet-using children.

[38] Beegle, K., Christiaensen, L., Dabalen, A., and Gaddis, I. (2016). Poverty in a Rising Africa.
[39] World Bank. (n.d.). Poverty & Equity Data Portal.
[40] UNICEF. (2017). Country Office Annual Report 2017 – Kenya.
[41] Republic of Kenya. (2010). The Constitution of Kenya, Article 7.
[42] The urban category includes the urban and peri-urban areas of the sample.

ABOUT KENYA – DEMOGRAPHICS AND INTERNET USAGE

FREQUENCY OF INTERNET USE AMONG CAREGIVERS OF INTERNET-USING CHILDREN

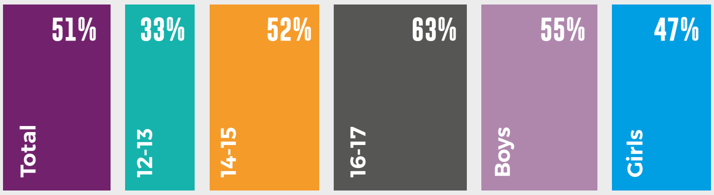
Source: Disrupting Harm data



n = 1,014 caregivers of internet-using children.

CHILDREN WHO USE SOCIAL MEDIA ON A WEEKLY BASIS

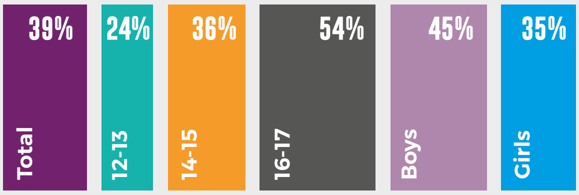
Source: Disrupting Harm data



n = 1,014 internet-using children.

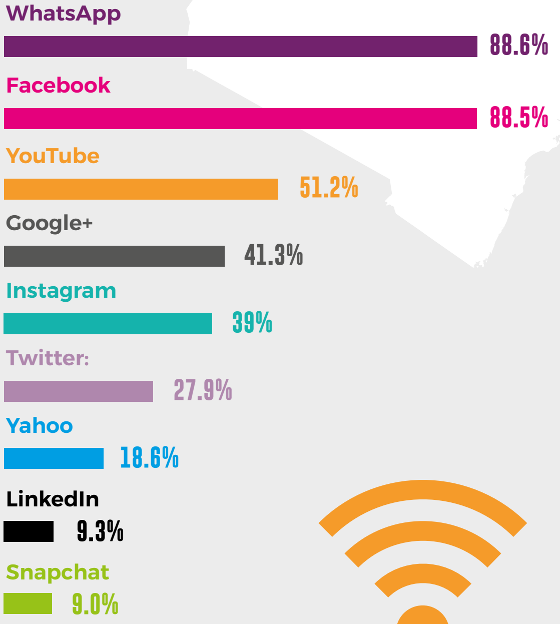
CHILDREN WHO USE INSTANT MESSAGING APPS ON A WEEKLY BASIS

Source: Disrupting Harm data



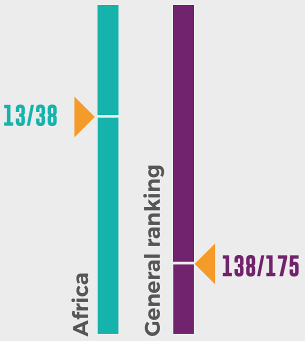
n = 1,014 internet-using children.

MOST POPULAR SOCIAL MEDIA PLATFORMS[43]

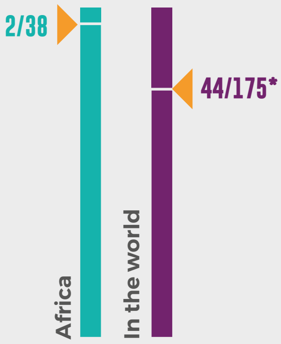


n = 3,269 Kenyans aged 14-55

ICT DEVELOPMENT INDEX RANKING (ITU)[44]

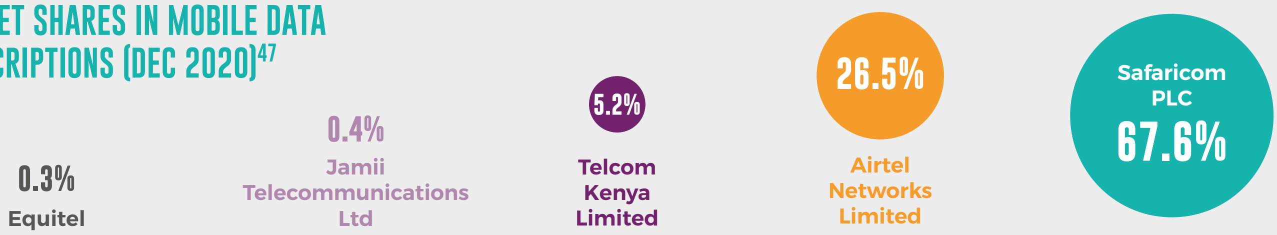


GLOBAL CYBERSECURITY INDEX RANKING 2018[45]



* behind Mauritius[46]

MARKET SHARES IN MOBILE DATA SUBSCRIPTIONS (DEC 2020)[47]



[43] United States International University – Africa. (2019). Social Media Consumption in Kenya: Trends and Practices.

[44] International Telecommunication Union. (2017). ICT Development Index 2017.

[45] The Global Cybersecurity Index measures the commitment of countries to cybersecurity based on the implementation of legal instruments and the level of technical and organisational measures taken to reinforce international cooperation and cybersecurity.

[46] International Telecommunication Union. (2019). Global Cybersecurity Index (GCI) 2018.

[47] Communications Authority of Kenya. (2020). Second Quarter Sector Statistics Report for the Financial Year 2020/2021 (October-December 2020).

Overview of legislation and policy

The most relevant pieces of legislation currently in effect regarding sexual offences, including OCSEA-related crimes, in Kenya are the Computer Misuse and Cybercrimes Act[48] and the Sexual Offences Act[49].

The Computer Misuse and Cybercrimes Act[50] provides a quite comprehensive definition of CSAM and explicitly criminalises acts associated with it[51] as well as the attempt to commit these crimes.[52] **The Sexual Offences Act** sets the age of sexual consent at 18[53] but provides no close-in-age exemption for consensual sexual relationships between peers under 18. It also prohibits certain forms of conduct associated with CSAM.[54]

The provisions of these laws relating to CSAM could potentially be applied to live-streaming of child sexual abuse. However, this is not explicitly stated and there is no separate provision criminalising live-streaming of abuse. Similarly, there are no provisions prohibiting online grooming for sexual purposes and sexual extortion committed in the online environment.

The upcoming **Children Bill 2021** was submitted to Parliament in 2020 but is yet to be enacted. According to interviews with three representatives from the Kenya Law Reform Commission, it will comprehensively criminalise online grooming and may also be applicable to live-streaming of child sexual abuse.

The **Victim Protection Act[55]** aims to secure victims of crimes from further harm. The Act includes a number of provisions to ensure that child victims receive support and protection immediately after the abuse is reported as well as during the legal proceedings.

Kenya has two national policies already in effect which touch on OCSEA: The **National Plan of Action Against Sexual Exploitation of Children in Kenya, 2018-2022** and the **National Information, Communications and Technology Policy (2019)**. The former includes an objective and activities related to the prevention of OCSEA, while the latter sets out the broad activities to be undertaken by the government on child online protection. However, interviews with representatives of the National Council of Children's Services (RA1-KY-02-A) and the Ministry of Information Communication and Technology, Innovation and Youth Affairs (RA1-KY-12-A) made clear that neither policy has been launched or disseminated widely to stakeholders.

Two policies exclusively concerned with child online protection are under development – namely, the **National Plan of Action on Online Child Sexual Exploitation and Abuse** and the **National Strategy on Child Online Protection**. The former is spearheaded by the Department of Children's Services and is in the final stages of development.[56] It is anchored in the WeProtect Model National Response. The National Strategy on Child Online Protection, which is led by the Communications Authority of Kenya, will embody the ITU Guidelines on Child Online Protection and will be formulated upon cabinet approval.

[48] Republic of Kenya. (2018). The Computer Misuse and Cybercrimes Act No. 5 of 2018.
[49] Republic of Kenya. (2006). The Sexual Offences Act No. 3 of 2006. (Last revised in 2019).
[50] Republic of Kenya. (2018). The Computer Misuse and Cybercrimes Act No. 5 of 2018. Section 24 (3).
[51] *Ibid.*, Section 24.
[52] *Ibid.*, Section 42(2).
[53] Republic of Kenya. (2006). The Sexual Offences Act No. 3 of 2006. Section 8. (Last revised in 2019).
[54] *Ibid.*, Section 16. (Last revised in 2019).
[55] Republic of Kenya. (2014). Victim Protection Act No. 17 of 2014.
[56] A representative from the Department of Children's Services confirmed that all the planned stakeholder consultations and focus group discussions had been completed and a draft policy developed. The only remaining activity was a validation, which was tentatively planned for May of 2021.

1. CHILDREN ONLINE IN KENYA

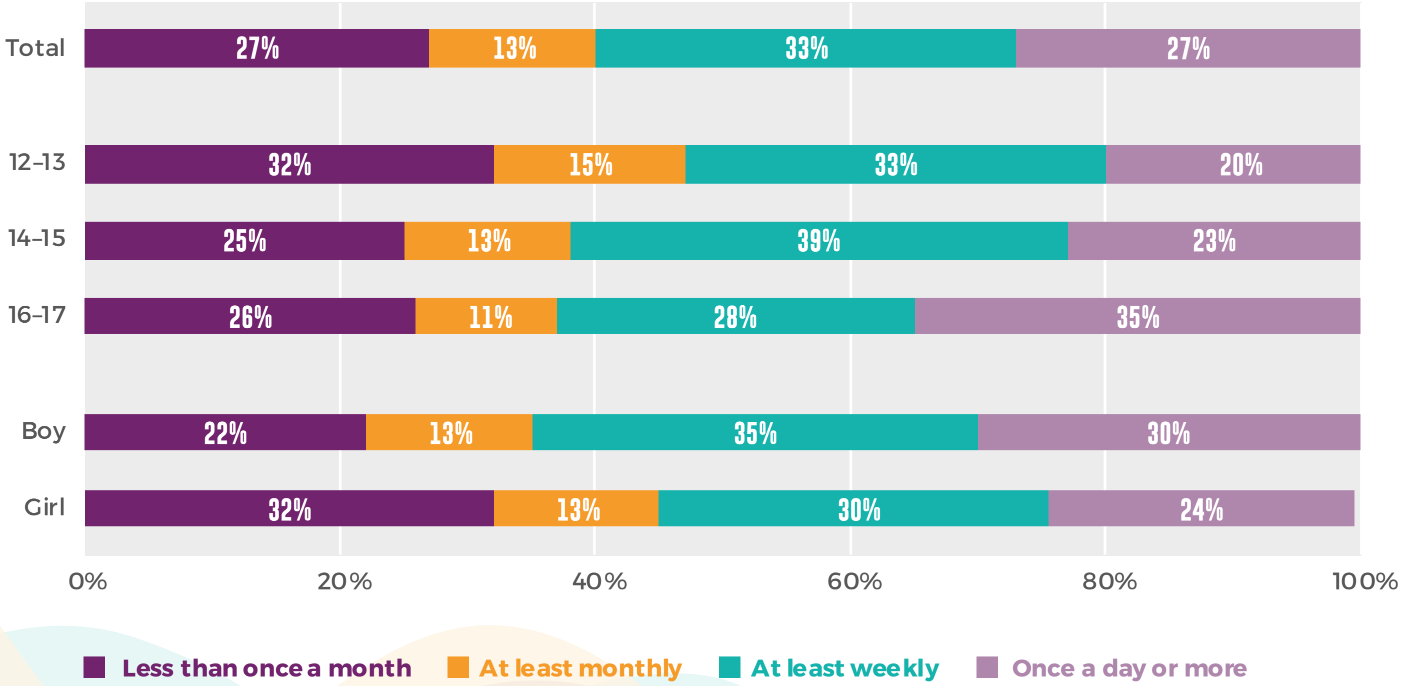
The main focus of this report is to present the perspectives of young people and duty-bearers around the sexual exploitation and abuse of children facilitated or committed through digital technologies. However, it is important to situate these offences within the wider context of children's internet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

1.1 INTERNET ACCESS AND BARRIERS

Sampling data from the *Disrupting Harm* household survey suggest that 67% of 12–17-year-olds in Kenya are internet users – i.e. they have used the internet within the past three months.[57,58] This figure rises from 55% among children aged 12-13 and 62% among children aged 14-15 to 83% among children aged 16-17. Boys and girls are just as likely to be internet users. In rural areas, 64% of children are internet users compared to 80% in urban areas.

Among internet-using children, 60% go online at least once a week. As is the pattern in other countries around the world,[59] older children are more frequent users. Boys go online somewhat more frequently than girls (see Figure 3). Children living in urban areas use the internet more frequently than children in rural areas.

Figure 3: Frequency of children's internet use

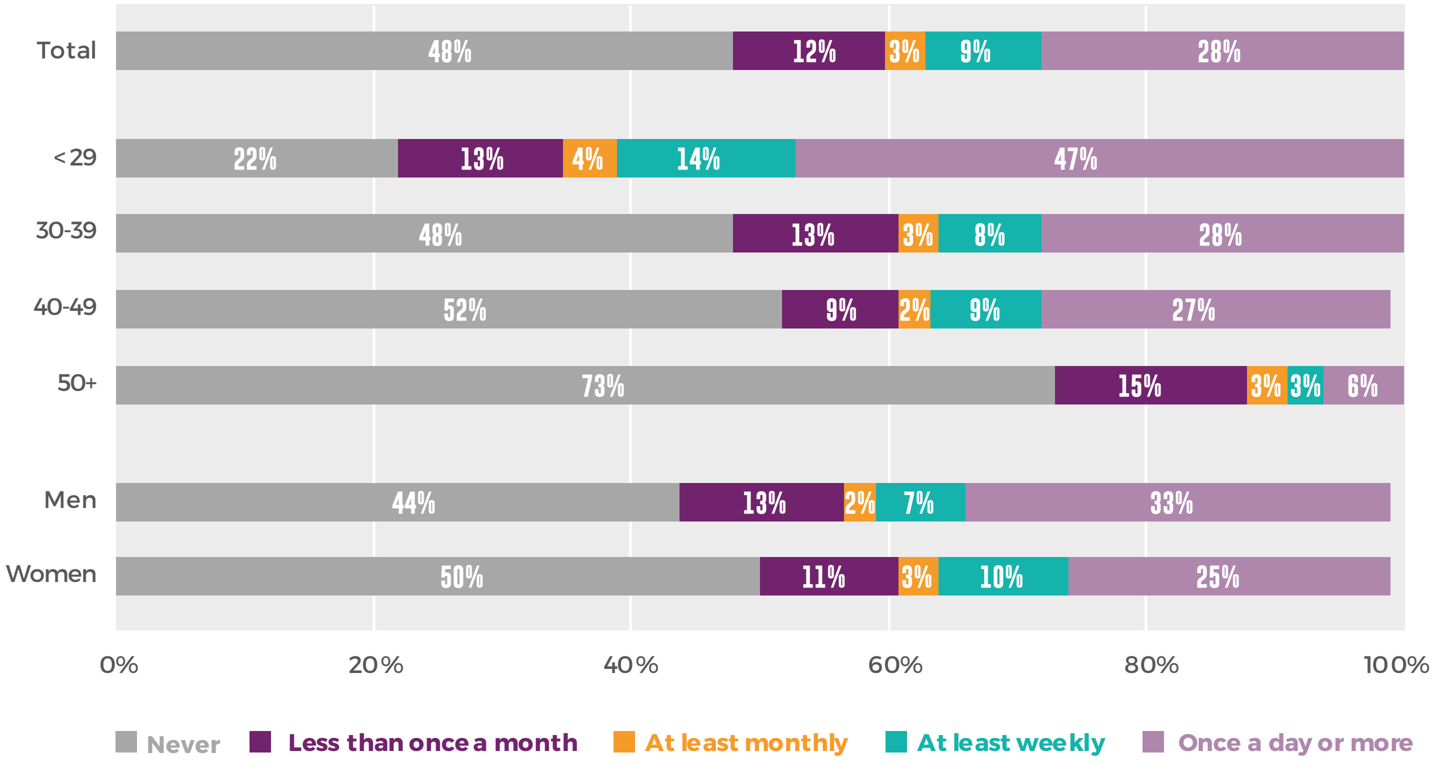


Base: Internet-using children aged 12-17 in Kenya. n = 1,014.

[57] While conducting the random walk to identify eligible children to partake in the main survey, we also collected data from every household visited about the number of 12–17-year-old children living there, their gender, age, and whether they had used the internet in the past three months. This allowed us to estimate internet penetration rates for all 12–17-year-old children in Kenya. n = 1,879 households.
[58] 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.
[59] See: Global Kids Online: http://globalkidsonline.net/.

Almost half of the caregivers surveyed have never used the internet. Those aged 50 and above are far less likely to be internet users than younger caregivers. Men are rather more frequent users than women (see Figure 4). As many caregivers have limited online experience, it is important to consider the support and knowledge they need, as well as the role that can be played by schools in guiding their children's use of the internet.

Figure 4: Frequency of caregivers' internet use



Base: Caregivers of internet-using children aged 12-17 in Kenya. n = 1,014.

Most children use the internet from home, which is consistent with data from other countries. Only 15% of children have ever used the internet at school, and very few do so regularly.

As in most other countries, smartphones are by far the most common device used by 12–17-year-old internet users to go online, probably due to their relatively low cost and portability.[60] As many as 99% use smartphones, while 13% also use computers and 6% tablets. There are no notable differences by age, gender or urban-rural location.

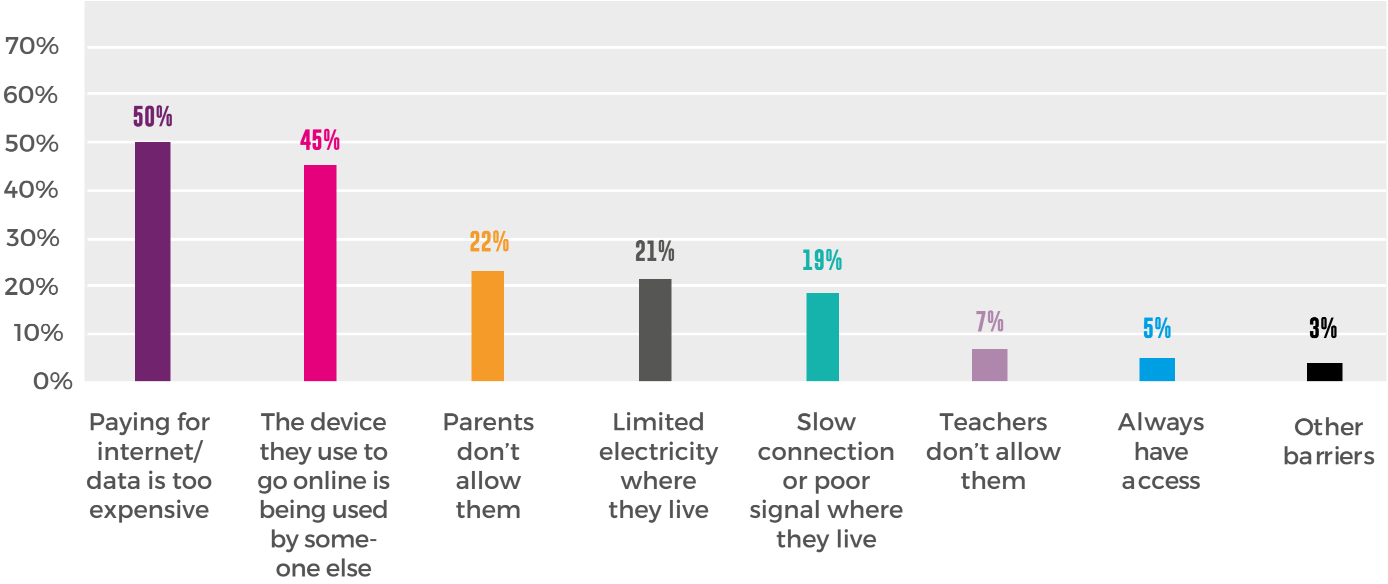
About four out of every five children who use a smartphone share it with someone else. Among those children who use computers to go online, almost all of them (93%) share the computer with someone else. Only 16% of girls have their own, unshared smartphone compared to 28% of boys. In rural areas, 19% of internet-using children have their own smartphone compared to 27% in urban areas.

Almost all internet-using children face barriers in accessing the internet and only 5% have readily

[60] Livingstone, S., Kardefelt Winther, D., & Saeed, M. (2019). Global Kids Online Comparative Report. Innocenti Research Report. Florence: UNICEF Office of Research – Innocenti.

available access whenever they want or need it. High internet and data costs are barriers to access for 50% of internet-using children, while 45% are unable to go online when they want or need to because someone else is using the digital device (see Figure 5).

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



Base: Internet-using children aged 12-17 in Kenya. n = 1,014.

Internet access is generally a little easier for older children with the main obstacle for 16-17-year-olds being high data costs. This may reflect the fact that older children use the internet more frequently than younger children and engage in more activities online (see Figure 6), therefore requiring more data.

Overall, girls are more likely than boys to name parental restrictions (25% girls; 18% boys) and shared devices (50% girls; 40% boys) as barriers to internet access.

1.2 CHILDREN'S ACTIVITIES ONLINE

The most popular online activities among the children surveyed are watching videos, using social media, instant messaging, online gaming and watching live-streams, followed by going online for school work and to look up new information. Older children generally engage in a wider range of online activities than younger children. However, gaming is most popular among the youngest children.

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 Kenya use the internet and the activities they enjoy. Gender differences in online activities are relatively minor, as has been observed in other countries.[61] As an exception, 40% of boys played online games compared to only 28% of girls. Girls were also less likely than boys to use instant messaging and social media while boys were more likely to search for news online compared to girls (see Figure 6).

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

Online activities	Total	12-13	14-15	16-17	Boy	Girl
Watching videos	57%	56%	61%	53%	58%	55%
Using social media	51%	33%	52%	63%	55%	47%
Using instant messaging	39%	24%	36%	54%	45%	35%
Playing online games	34%	44%	33%	27%	40%	28%
Watching a live-stream	34%	38%	34%	30%	36%	31%
School work	32%	28%	31%	37%	32%	32%
Searching for new information	25%	16%	26%	31%	30%	21%
Following celebrities and public figures on social media	20%	11%	20%	26%	21%	19%
Searching for news	19%	11%	21%	24%	24%	15%
Talking to family or friends who live further away	17%	13%	16%	21%	18%	16%
Participating in a site where people share their interests	15%	9%	17%	18%	17%	14%
Searching for information about work or study opportunities	13%	8%	11%	20%	13%	14%
Creating their own video or music	11%	12%	11%	10%	10%	11%
Searching for health information	10%	8%	9%	12%	10%	10%
Seeking emotional support	7%	4%	6%	9%	6%	8%
Looking for information on local events	6%	4%	8%	7%	8%	5%
Discussing political or social problems	6%	3%	6%	8%	6%	5%
Creating a blog or website	3%	1%	3%	5%	3%	4%

Base: Internet-using children aged 12-17 in Kenya. n = 1,014.

[61] *Ibid.*

1.3 PERCEPTIONS AND EXPERIENCES OF RISKY ONLINE ACTIVITIES

Discussion of online risks for children often hinges upon adult-centric perceptions. To ensure we also understood children's perceptions, we asked them and their caregivers about their engagement in, and perceptions of, various online risky activities.

1.3.1 Contact with strangers online and in person

Of the caregivers in our household survey, 82% rated talking to online strangers as 'very risky' for children, but children themselves were less concerned. Just 44% of internet-using children considered this activity 'very risky' for children of their age. Children aged 12-13, and girls, were most likely to describe talking to someone on the internet who they have never met in person, as 'very risky' (see Figure 7).

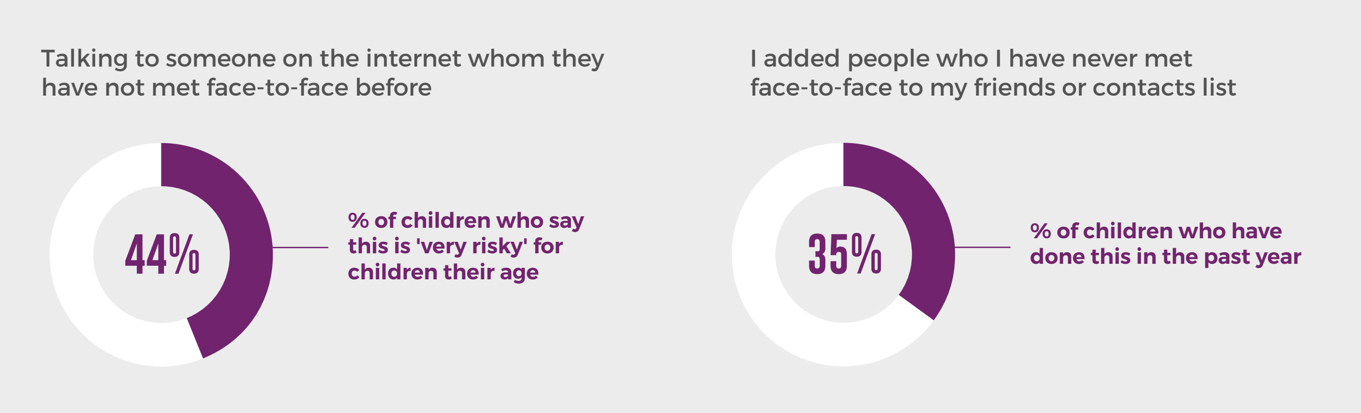
Similarly, 88% of the caregivers surveyed thought it 'very risky' for children to send their personal information to someone they have never met face-to-face, compared to 57% of the children.

While most children recognised that interacting with strangers carries some level of risk, a substantial proportion said that these activities were 'not risky at all' or were unsure about it. This may be because many such connections are not harmful and may simply be how young people now make new friends. Alternatively, this could indicate a lack of awareness of how speaking to strangers online might lead to harmful outcomes.

Child-centred workshops conducted in relation to the *Disrupting Harm* project with 27 children in Kenya suggested that children's understanding of online 'strangers' can be rather nuanced. While aware of the need to be careful, they reflected that a stranger has the potential to be good or bad. Many children said that whether or not they felt safe interacting with a stranger depends on the context of their interactions.[62]

Turning to the actual behaviour of the children in our survey in relation to people they first met online, 35% had added people they had never met before to their contact lists. Over one in four internet-using children had shared their personal information with someone they had never met face-to-face.

Figure 7: Children's risk assessment of speaking to online stranger versus children who have added strangers to their friends list in the past year.



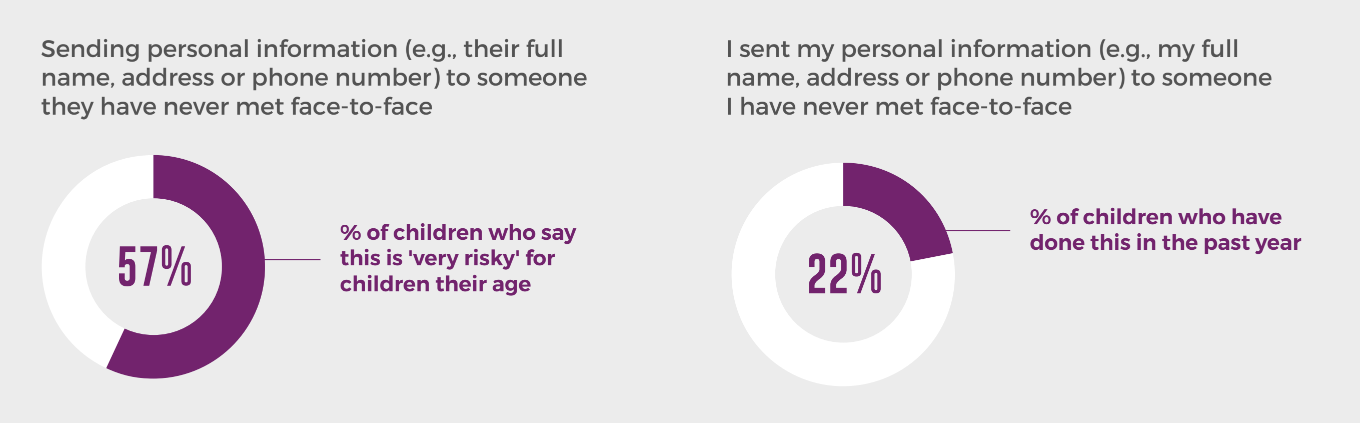
Talking to someone on the internet whom they have not met face-to-face before

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

Base: Internet-using children aged 12-17 in Kenya. n = 1,014.

[62] Third, A., Moody, L., & Theakstone, G. (2020). Children's Digital Experiences: Kenya Country Report.

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

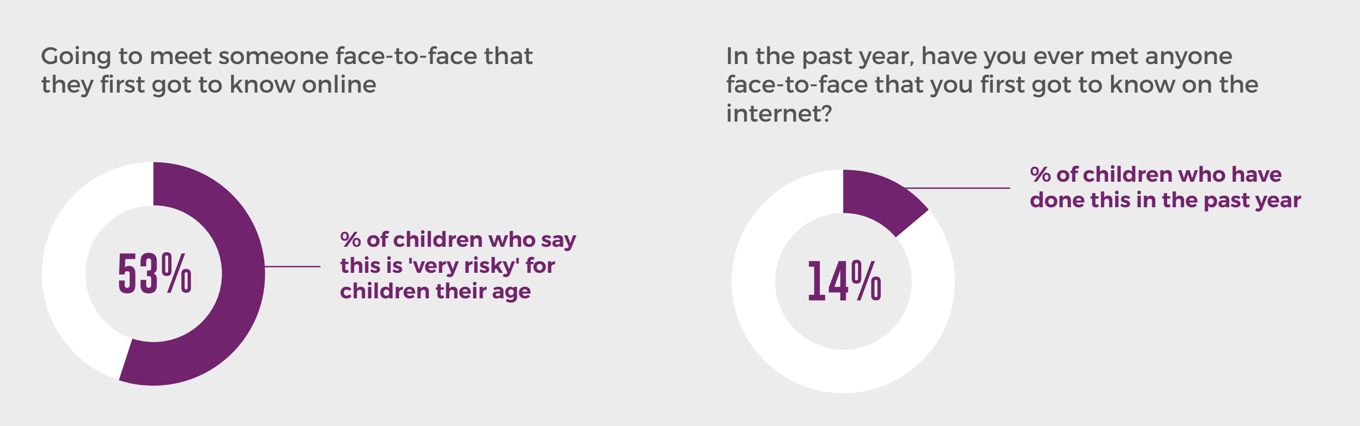


Base: Internet-using children aged 12-17 in Kenya. n = 1,014.

In our household survey, we also queried perceptions about situations where getting to know people online leads to face-to-face encounters. Over half of the children and as many as 86% of their caregivers thought that meeting 'online strangers' in person is 'very risky' for children. Girls were more likely than boys to regard this as 'very risky' behaviour (60% vs. 45%, respectively). However, 16% of children viewed this behaviour as 'not risky at all'.

Within the past year, 14% of the children surveyed had met someone in person whom they had first met online. Out of these children, the great majority were happy about the experience (see Figure 10). Research done across more than 30 countries around the world has produced similar findings.[63,64]

Figure 9: Children's risk assessment of meeting online strangers in person versus children who have engaged in this behaviour in the past year

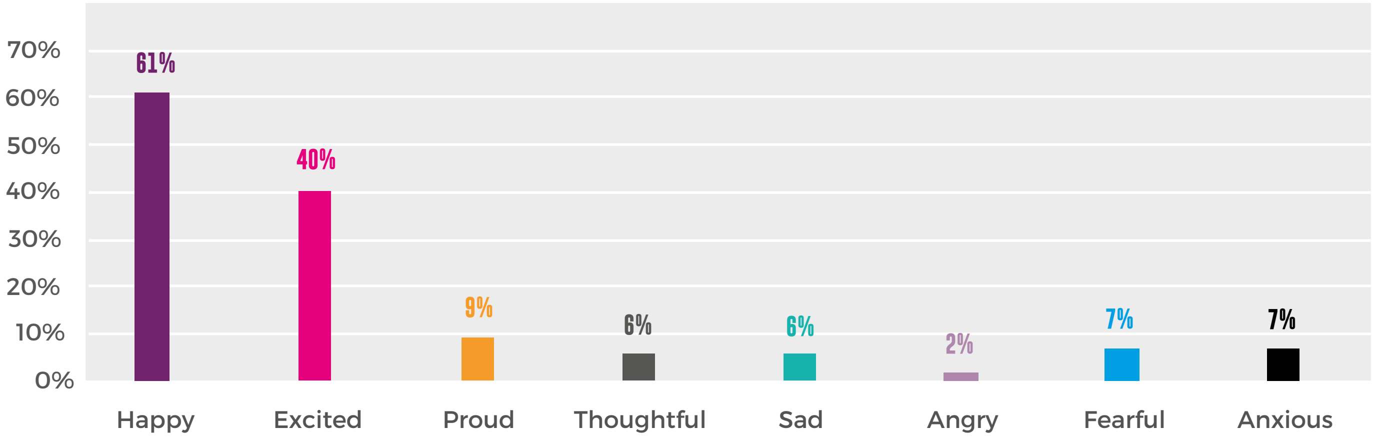


Base: Internet-using children aged 12-17 in Kenya. n = 1,014.

[63] *Ibid.*

[64] Smahel, D., Machackova, H., et al. (2020). EU Kids Online 2020: Survey results from 19 countries. Florence: UNICEF Office of Research – Innocenti.

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: Children who, within the past year, have met someone face-to-face whom they first got to know on the internet. n = 139.

There are clearly incongruences between children's and caregivers' perceptions. Clearly, meeting someone you do not know face-to-face for the first time can be very risky. This report mentions some cases which had severe consequences for doing so. Such cases probably explain why caregivers are so worried. But there are many different types of such encounters, like connecting with new children in the community first online and then in person, or going to group events with caregivers. The experiences of most internet-using children in Kenya and other countries around the world seem to indicate that the risk of harm is relatively low for children in general, although the harm might be severe if it occurs. While many children in Kenya are aware that engaging with online strangers carries a level of risk, we need to ensure all children are informed and taught how to engage safely and responsibly.

Is Restricting Children's Internet Access the Answer?

Many caregivers instinctively react to online risks by restricting their children's internet use in a bid to protect them. Such *restrictive practices* seem quite common in Kenya. For example, 38% of the children in our survey reported that they are not allowed to use social media, and 20% are not allowed to watch videos online. In addition, 23% said that their caregivers often limit how long they can stay online. When asked what they would do if their child was bothered by something online, one third of caregivers said they would restrict their child's internet access.

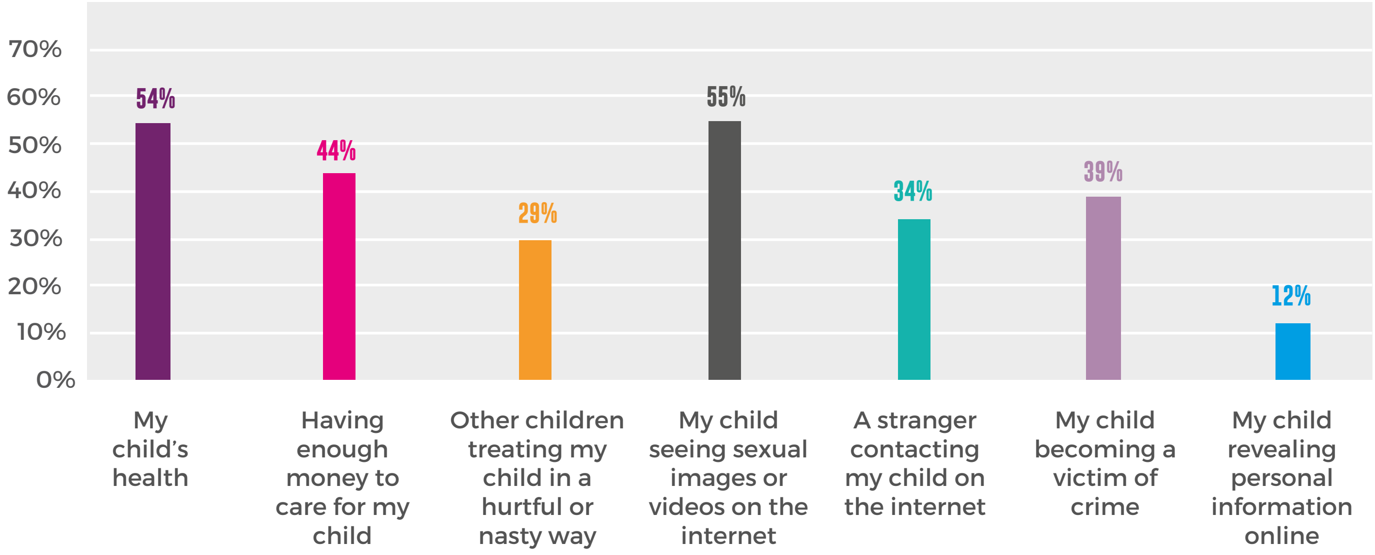
This approach might reduce children's exposure to online risks in the short term, but it also reduces their digital skills and familiarity with the online environment in the long term. On the other hand, *supportive engagement* by adults has been associated with positive skills development for children in other countries.[65] Supportive mediation could include engaging in activities together, talking to children about their internet use, and educating them about the risks that exist online and how best to avoid them. In these ways, we allow children to benefit from the many useful activities and skills that the internet has to offer, while providing parental guidance and support. While caregivers in Kenya use the internet less frequently than their children and may worry that they do not have enough knowledge to guide them, they can still talk to their children about what they do online and provide an open and supportive home environment. Information about online risks and how to avoid them might also be provided by schools or specialised organisations.

[65] Livingstone, S., Kardefelt Winther, D., & Saeed, M. (2019). Global Kids Online Comparative Report. Innocenti Research Report. Florence: UNICEF Office of Research – Innocenti.

1.3.2. Seeing sexual images online

As shown in Figure 11, when the caregivers surveyed were asked to select their top three concerns for the child being interviewed, seeing sexual images was the most common concern, along with their child's health. Worries over sexual content, concerns over their child becoming a victim of a crime and whether they would be able to provide for their child (see Figure 11). Among the children surveyed, a substantial 63% believed that seeing sexual images or videos on the internet is 'very risky' for children their age, but among caregivers, the ratio was 89%.

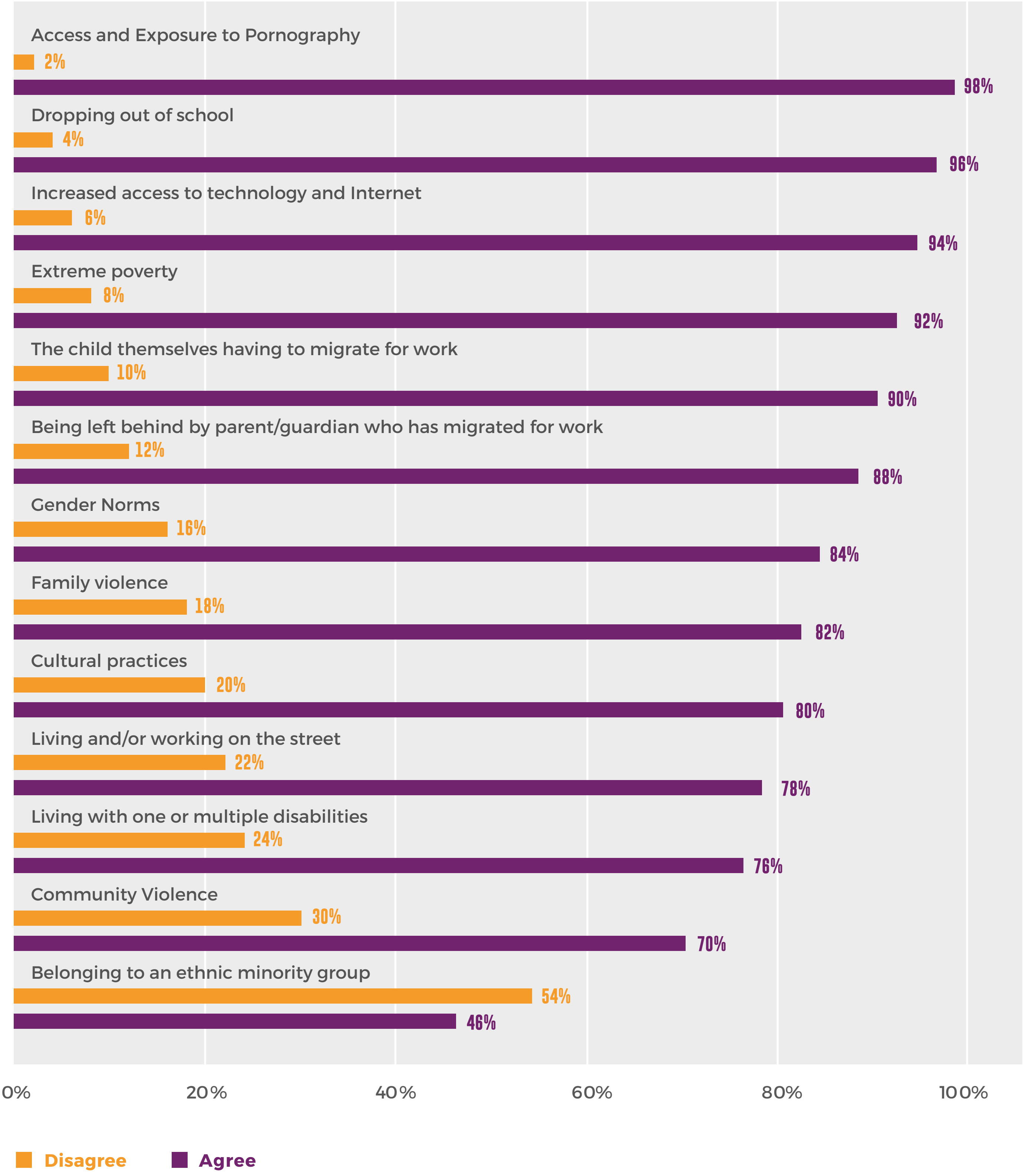
Figure 11: Caregivers' top concerns regarding their children.



Base: Caregivers of internet-using children aged 12-17 in Kenya. n = 1,014.

The frontline workers whom we surveyed regarded 'access and exposure to pornography' as the most important factor increasing children's vulnerability to OCSEA, ahead of issues like migration, experiences of family and community violence, or living on the street (see Figure 12).

Figure 12: Frontline workers' perceptions of factors affecting children's vulnerability to OCSEA.

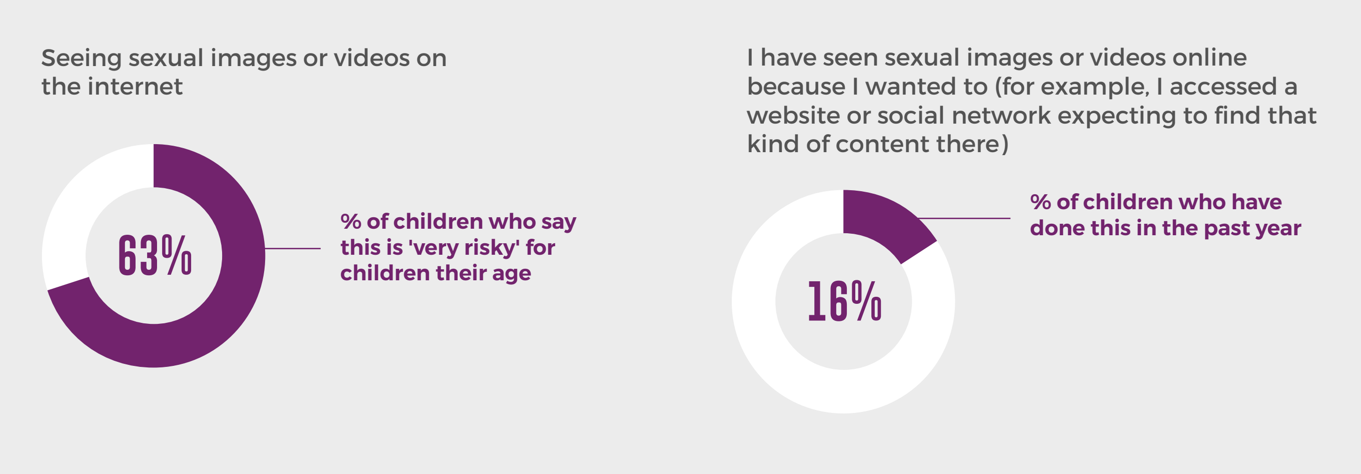


Base: Frontline workers. n = 50.

Accidental or intentional glimpses of sexual content are one thing; being exposed to sexual images as part of a grooming process intended to desensitise the child and pave the way for subsequent requests for images or sexual acts is another. While viewing violent or degrading sexual content can serve to normalise harmful gender norms and sexual behaviour, seeing some pornography appears to be an increasingly present experience for young people.[66] Addressing both phenomena is needed.

In practice, 37% of internet-using children in Kenya who took part in the household survey said they had seen sexual images or videos at least once in the past year. Only 16% reported actively looking for such material online, while 33% were exposed to sexual images or videos when they did not expect sexual content online.

Figure 13: Children's risk assessment of seeing sexual images or videos online versus children who have actively looked for this content in the past year



Seeing sexual images or videos on the internet

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

I have seen sexual images or videos online because I wanted to (for example, I accessed a website or social network expecting to find that kind of content there)

% of children who have done this in the past year

Base: Internet-using children aged 12-17 in Kenya. n = 1,014.

Among the children who reported seeing sexual images or videos online by accident, 42% said they saw these images or videos on their social media feeds. Around one in five saw them in online advertisements and 22% of children said the images or videos were sent to them via direct messaging apps.

Older children were more likely than younger children to see sexual images or videos on social media when they did not expect it. There were no major differences in accidental exposure to sexual content on social media by gender. Among the 21% of children who reported seeing sexual images or videos online by accident, nearly half said they saw these images or videos on their social media feeds, while one in five saw them in online advertisements. Around 22% of children said the images or videos were sent to them directly.

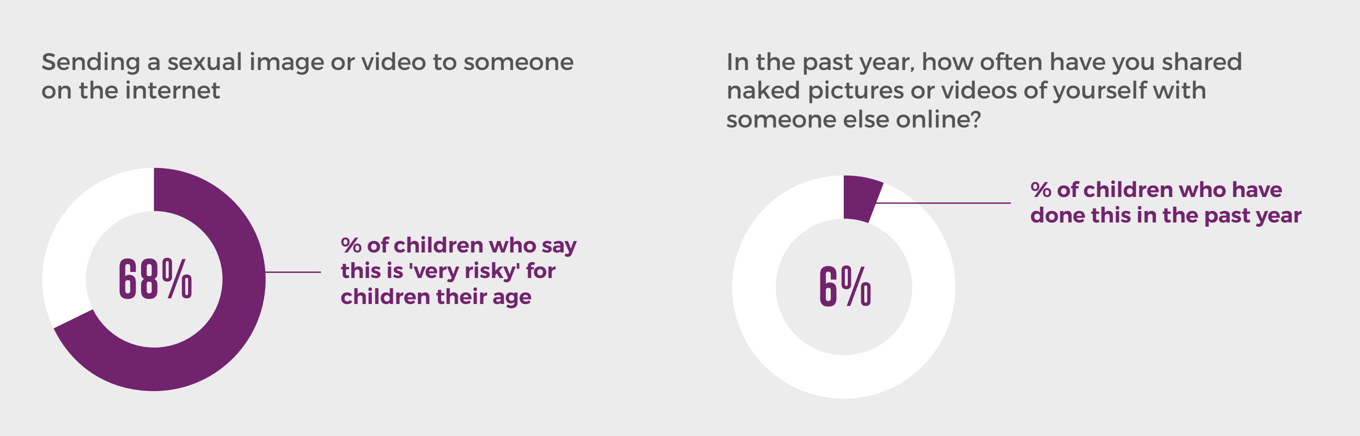
1.3.3 Making and sharing self-generated sexual content

Most of the children and caregivers surveyed agreed with the statement *"it is wrong for a person to take naked images or videos of themselves"*. In addition, 91% of caregivers and 68% of children thought it was 'very risky' to share a sexual image or video online, while only 3% and 12%, respectively, thought it was 'not risky at all'.

[66] See for example: Crabbe, M. & Flood, M. (2021). School based Education to Address Pornography's Influence in Young People: A Proposed practice framework. American Journal of Sexuality Education 16(1).

In practice, 6% of the children in the household survey said they had shared naked pictures or videos of themselves in the past year. There were no clear differences by age or gender.

Figure 15: Children's risk assessment of sending sexual content online versus children who have engaged in this behavior in the past year

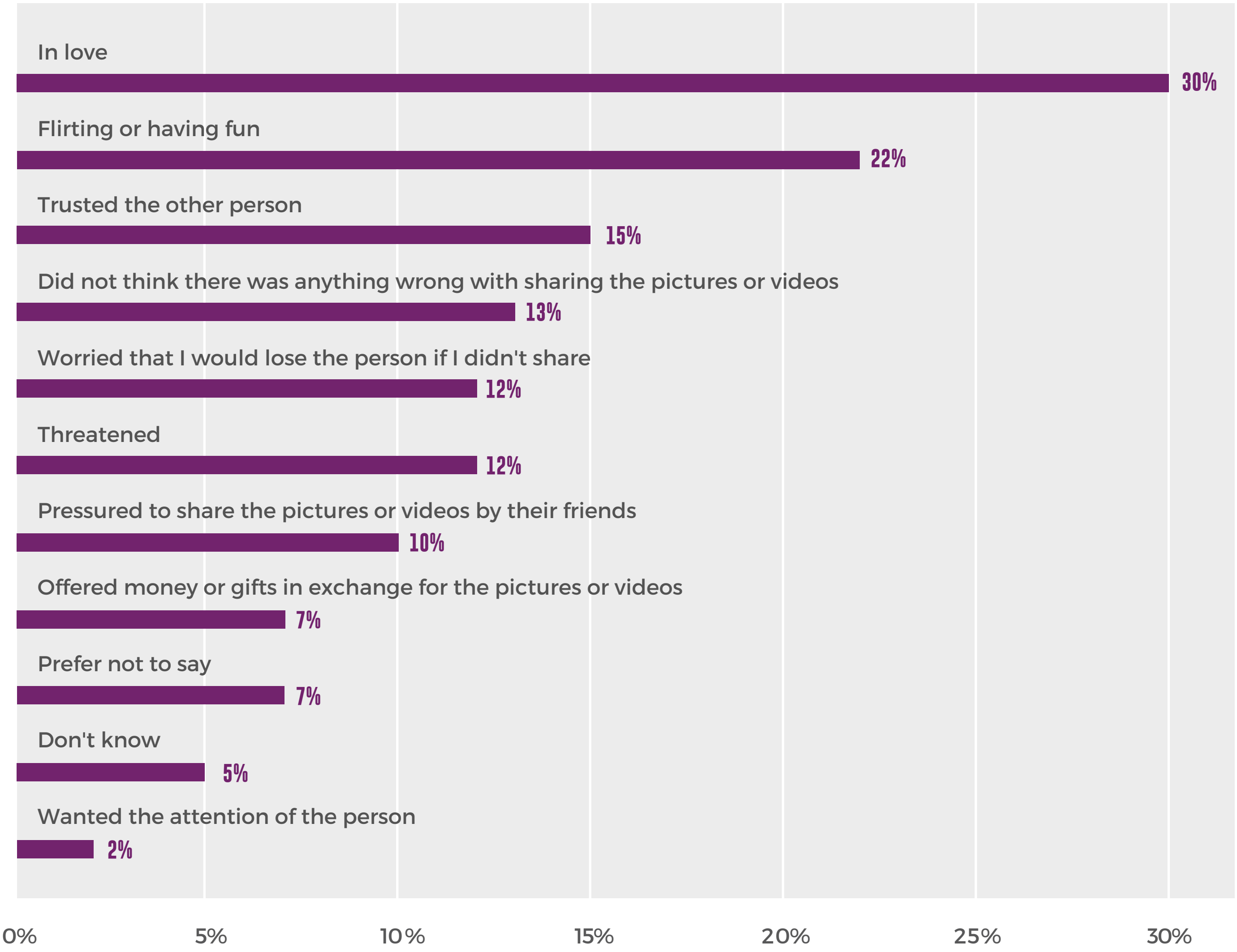


Base: Internet-using children aged 12-17 in Kenya. n = 1,014.

The main reasons given by children for sharing naked pictures or videos were that they were in love, flirting or having fun, that they trusted the other person, and that they found nothing wrong with sharing such content. Five percent had allowed someone else to take naked pictures or videos of them.

Seven of the 60 children had shared self-generated sexual content because they were threatened and six because they were being pressured by their friends (see Figure 16). Figures from the survey are representative of 12-17-year-old internet users. When scaled up to this population of children, the numbers are far greater.

Figure 16: Reasons given by children for sharing naked images or videos of themselves.



Base: Children who have shared naked images or videos of themselves in the past year. n = 60.

Most of the 60 children had shared the images or videos with a friend or someone else they knew in person (35%), or with a romantic partner (30%), but some children (12%) had shared them with someone they met online who had no other connection with their life.

Overall, although children in Kenya show some level of awareness about online risks, 56% of the internet-using children who took part in the household survey have not received any information on how to stay safe online. To ensure not only that children are aware of possible risks but that they know what to do about them, there is a need for comprehensive digital literacy and safety training. This should include information about what children can do if they are being bothered online, what content to share and not to share with others, and basic skills such as how to change their privacy settings and block people from contacting them.

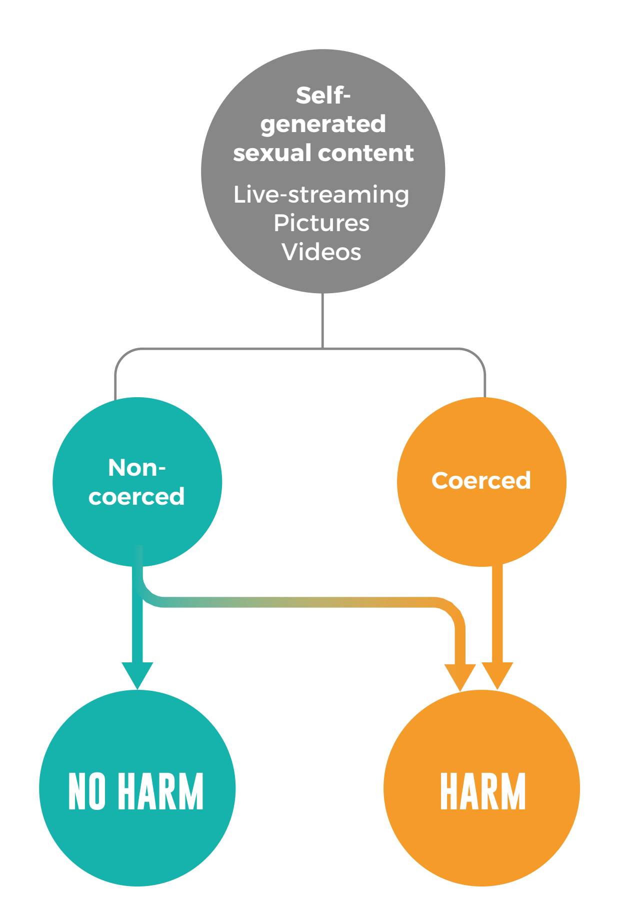
The rise in self-generated sexual content involving children

The increasing use of technology is leading to shifts in notions of privacy and sexuality among children in some parts of the world, particularly among adolescents as they mature.[67] Behaviours that are increasingly normative to young people can be bewildering for adults who grew up in a different time. For example, chatting and video live-streaming is frequent, 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.[68]

The sharing of self-generated sexual content by children is complex and includes a range of different experiences, risks and harms. As our data show, some self-generated content is created and shared by adolescents voluntarily. Such exchanges are increasingly becoming part of young people's sexual experiences. However, our data also shows that the creation and sharing of self-generated sexual content can be coerced, for example through grooming, threats or peer-pressure (see chapter 2.2).

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 voluntarily may not cause harm at first, but there remain risks 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.[69,70] (see Figure 14).

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



[67] Livingstone, S. & Mason, J. (2015). Sexual Rights and Sexual Risks among Youth Online: A review of existing knowledge regarding children and young people's developing sexuality in relation to new media environments. London: European NGO Alliance for Child Safety Online.
[68] Thorn & Benson Strategy Group. (2020). Self-Generated Child Sexual Abuse Material: Attitudes and experiences. U.S.: Thorn.
[69] Bracket Foundation. (2019). Artificial Intelligence: Combating Online Sexual Abuse of Children. 10.
[70] EUROPOL. (2019). Internet Organized Crime Threat Assessment 2019. Netherlands: EUROPOL.

2. ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE IN KENYA

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 Kenya. We draw on a variety of sources – including law enforcement data, mandated reports from U.S.-based technology companies to the NCMEC related to Kenya, surveys with frontline workers and surveys, interviews and conversations with children themselves – in order to create a well-rounded presentation of the nature of these crimes against children.

This chapter presents estimates of the occurrence of certain instances of OCSEA based on data from law enforcement units (chapter 2.1) and children's self-reported experiences (chapter 2.2 and 2.3). For several reasons, estimates are not intended to provide a conclusive picture of the prevalence of OCSEA. Firstly, the existing administrative data that we have accessed, such as that kept by law enforcement authorities, rarely delineates or classifies OCSEA elements. Secondly, with respect to the household survey, we would expect a degree of under-reporting due to privacy concerns and the discomfort of openly discussing sex. Furthermore, in households where sexual abuse occurs, we expect we would be less likely to be provided access to survey children. Finally, many estimates are based on analysis of sub-samples of the survey data which are small because OCSEA is still a rarely reported phenomenon, which results in a larger margin of error.

While we have full confidence in our data and the quality of the sample obtained, the challenges of researching specific and sensitive phenomena means that we inevitably lose precision in the final estimate. For these reasons, we suggest that the reader interprets the findings in this chapter as a *good approximation* of the occurrence of certain crimes against children related to OCSEA in Kenya and the extent to which internet-using 12–17-year-old children in Kenya are subjected to OCSEA.

2.1 LAW ENFORCEMENT DATA

The analysis in this chapter draws on qualitative and quantitative data from law enforcement authorities and a number of partner organisations, with a view to understanding offences relevant to OCSEA that were recorded in the country, offender and victim behaviours, crime enablers and vulnerabilities.

2.1.1 Recorded OCSEA offences

The Anti Human Trafficking and Child Protection Unit (AHTCPU) of the Kenyan National Police Service reported the following case numbers for 2017, 2018 and 2019:

Figure 17: Number of CSEA/OCSEA cases recorded by AHTCPU

	2017	2018	2019
Number of offline CSEA cases	25	33	21
Number of OCSEA cases	-	3,160	4,133

Base: Data provided by AHTCPU.

Because offline instances of child sexual exploitation and abuse (CSEA) are usually reported to local police stations, the number of CSEA cases investigated by the national specialist unit (presented in Fig 16 above) is not representative of the country as a whole. The larger numbers of OCSEA cases may be explained by the fact that the national specialist unit is the recipient of reports made via NCMEC (see Fig 17 below). The Unit did not begin to investigate OCSEA until 2018, hence the recording of 0 cases in the previous year.

The actual number of NCMEC CyberTipline reports (CyberTips) recorded by AHTCPU were 3,160 and 4,133 in 2018 and 2019 respectively, much lower than the total CyberTips sent by NCMEC (16,108 and 12,788 in 2018 and 2019 respectively). There is a discrepancy between the number of CyberTips sent by NCMEC and the number of recorded cases by AHTCPU. It appears that the discrepancy stems from AHTCPU only recording cases that they consider actionable.

It is likely that the difference lies in the number of so-called 'meme' reports: CyberTips based on material circulated on social media in bad taste, inappropriate humour, or in a misguided attempt to help the child. While the material or activity may not be actionable by law enforcement, it does constitute a breach of the terms of service of the reporting electronic service provider, and is thus reported.

2.1.2 International OCSEA detections and referrals

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

U.S. federal law requires that 'electronic service providers' (i.e., technology companies) based in the U.S. report instances of suspected child exploitation to NCMEC's CyberTipline. However, for providers not based in the U.S., this reporting is voluntary and not all platforms report suspected child exploitation to NCMEC. There is therefore a data gap for several platforms that are popular in the *Disrupting Harm* focus countries. Furthermore, it must be considered that this CyberTip data only represents cases *reported to NCMEC*, and not a full picture of the extent of OCSEA in Kenya. CyberTipline reports under this category may reference more than one file of CSAM. For example, some reporting ESPs include more files per report, as opposed to one image per report and multiple reports per suspect.

Figure 18: CyberTips concerning suspected child sexual exploitation in Kenya.

	2017	2018	2019	% Change 2017- 2018	% Change 2018-2019	% Change 2017-2019
Kenya	12,361	16,108	12,788	30%	-21%	3%
Global Total	10,214,753	18,462,424	16,987,361	81%	-8%	66%
Kenya % of Global Total	0.12%	0.09%	0.08%			

Base: Data provided by NCMEC.

Kenya shows a consistently low proportion of suspected child sexual exploitation in CyberTips, an average of 0.09% in the years 2017-2019. This is lower than might be expected, given that Kenya accounted for 0.68% of the world's population, and 1.00% of the world's internet using population according to United Nations and International Telecommunications Union estimates.[71]

Kenya also saw a much smaller percentage increase (just 3%) in CyberTips between 2017 and 2019 than the global distribution. Specifically, a reduction for Kenya of 21% between 2018 and 2019 was more marked than that for the global total (8%). This may be indicative of a move in Kenya away from misuse of the platforms that report suspected child exploitation to NCMEC, thereby raising the further question of where OCSEA offenders might move to.

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 Kenya in the reporting period (see Figure 19).

Figure 19: CyberTips concerning suspected child sexual exploitation in Kenya, by incident type.

Incident Type	2017	2018	2019
CSAM, including possession, manufacture and distribution (NCMEC classification: child pornography)[72,73]	12,359	16,101	12,779
Travelling child sex offences (NCMEC classification: child sex tourism)[74]	1	2	7
Child sex trafficking	-	-	-
Child sexual molestation	1	2	2
Online enticement of children for sexual acts	-	3	-

Base: Data provided by NCMEC.

CyberTips classified as relating to CSAM increased in 2018 and declined in 2019 in line with the trend for Kenya's total. In terms of priority level, NCMEC tagged two reports for Kenya as 'Priority 1', indicating a child in imminent danger.

[71] International Telecommunications Union. (n.d.). Statistics.
[72] The terminology used by NCMEC is 'child pornography', to align with U.S. legislation. *Disrupting Harm* advocates use of the term 'child sexual abuse material' in line with the Luxembourg Guidelines.
[73] 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.
[74] The terminology used by NCMEC is 'Child Sex Tourism', to align with U.S. legislation. *Disrupting Harm* advocates use of the term 'Travelling Child Sex Offences' in line with the Luxembourg Guidelines.

Nearly 100% of NCMEC CyberTips for Kenya in the period 2017 to 2019 had an electronic service provider as their source. A total of 29 electronic service providers submitted at least one CyberTip of suspected child exploitation for Kenya in the reporting period. This would indicate some diversity in the usage of platforms by the general population, in line with the level of internet connectivity in the country, and in the misuse of a range of platforms by OCSEA offenders.

Figure 20: NCMEC CyberTips concerning suspected child sexual exploitation in Kenya, by reporting electronic service providers.

Reporting Electronic Service Provider	2017	2018	2019	% of 2019 Total
Facebook	11547	15140	11592	90.66%
Instagram Inc.	397	570	770	6.02%
Google	366	332	349	2.73%
Tagged.com	19	12	27	0.21%
Snapchat	1	1	11	
WhatsApp Inc.	1	4	11	
Twitter Inc. / Vine.co	5	9	6	
Pinterest Inc.	4	6	4	
Microsoft – Online Operations	1	4	3	
MediaFire		1		
Multi Media, LLC/Zmedianow, LLC/Chaturbate		3	1	
Hacker Factor		1		
motherless			1	
4chan community support LLC			1	

Base: NCMEC CyberTips *sorted by 2019 counts, null results removed.*

Figure 20 shows that while Facebook accounts for 93% of total CyberTips for Kenya in the reporting period as a whole, this proportion reduced slightly in 2019. This correlates with an increase in the number of CyberTips submitted by Instagram, which almost doubled between 2017 and 2019. Although CyberTips from Facebook increased by 31% between 2017 and 2018, they subsequently fell by 23%. Small increases in CyberTips from popular services such as Snapchat and WhatsApp were also observed.

The variety of platforms among the reporting electronic service providers may also speak to the nature of suspected OCSEA offending. Multiple CyberTips from Tagged.com in 2017-2019 speak to the persistent misuse of adult dating sites for suspected distribution of CSAM in Kenya. Four CyberTips for Kenya from Chaturbate, a platform specialising in the provision of adult live-streamed sexual activity that is often paid for in tokens, raises the possibility of OCSEA with a commercial element. The presence in Kenya of OCSEA offenders with a level of technical sophistication and specialist interest is demonstrated by the appearance in the data of self-avowed 'moral free file host' motherless, anonymous image-based bulletin board 4chan, file sharing service Mediafire and digital forensics research company Hacker Factor (1 CyberTip each).

Data supplied by Kenyan law enforcement about platforms used to commit recorded OCSEA offences allows for comparison with those electronic service providers reporting to NCMEC (see Figure 21).

Figure 21: Online services misused in OCSEA cases recorded by AHTCPU.

Service Misused (mentions)	2018	2019
Facebook	2,500	4,009
Instagram	110	400
WhatsApp	11	60
Google	20	126
Snapchat	0	2
Twitter	2	14
Tagged.com	1	0
Pinterest	1	0
Total	2,645	4,611

Base: Data provided by AHTCPU.

This distribution is broadly consistent with the NCMEC CyberTip data insofar as Facebook is mentioned in 90% of cases. There are also notable differences, however, particularly in relation to WhatsApp. For this platform, the total number of mentions in OCSEA cases is larger than the number of CyberTips it made in 2018 and 2019. Whereas CyberTips have a single source, a case recorded by law enforcement can involve the misuse of more than one platform. Nevertheless, WhatsApp would appear to be more prominent in the OCSEA caseload of Kenyan law enforcement than is evident in the NCMEC data.

NCMEC data also permits analysis of headline statistics for unique internet protocol (IP) addresses used to engage in suspected child exploitation (see Figure 22).

Figure 22: NCMEC CyberTips concerning suspected child sexual exploitation in Kenya, number of unique upload IP addresses by year.[75]

	2017	2018	2019	% Change 2017-2019	% Change 2018-2019
Kenya Unique Upload IP Addresses	8,879	13,027	9,567	8%	-27%
Total Kenya Reports	12,361	16,108	12,788	3%	-21%
Reports per Unique IP Address	1.39	1.24	1.34	-4%	8%

Base: Data provided by NCMEC.

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, perhaps indicative of a more deliberate style of offending that is less likely to be committed through lack of knowledge. By the same token, Kenya's consistently low average number of reports per IP address may be suggestive of a tendency towards lower volume CSAM offending within individual online sessions.

One foreign law enforcement agency identified Kenya as a source of commercial forms of live-streaming of child sexual abuse,[76] accounting for 2% of that agency's reports on this crime type. Another reported sending ten referrals to Kenya regarding OCSEA-related offences in the period 2017-2019.[77]

[75] 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 ISPs 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.
[76] Also described as 'live distant child abuse'.
[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.

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. Although the data requirement for this project did not include systematic collection of data concerning OCSEA referrals from all law enforcement agencies outside Kenya, it is likely that there have been additional international referrals in the reporting period, over and above the NCMEC CyberTips discussed above.

2.1.3 Evidence of CSAM from other sources

Hosting: Kenya has not been identified as a hosting country for images and videos assessed as illegal by INHOPE member hotlines contributing to the ICCAM platform.[78] Moreover, the Internet Watch Foundation actioned 0 reports concerning confirmed CSAM hosting in Kenya 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 P2P 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 9th June 2019 to 8th June 2020 reveals that 76 Kenyan IP addresses were identified as engaged in distribution or downloading (see Figure 23). Since the system does not monitor all file sharing networks, this should not be taken to be representative of the sum total of CSAM offending on such platforms. Representation of data for Kenya alongside that for other *Disrupting Harm* focus countries in Africa allows for comparison.

Figure 23: CSAM distribution and downloading from African *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	2413	842
Tanzania	47	5
Uganda	4	4

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

CSAM distribution on the monitored peer-to-peer networks would appear to be less popular in Kenya than in Southern Africa, but more popular than in other Eastern African focus countries. In as much as data supplied by NCMEC indicates several thousand instances of suspected CSAM possession, manufacture and distribution in Kenya in 2017, 2018 and 2019, it would appear that Kenyan CSAM offenders may prefer using globally popular US-based platforms to exchange rather than peer-to-peer file-sharing networks.

Web Searches for CSAM: Research was conducted on Google Trends, with a view to identifying levels of interest in CSAM in Kenya.[79] In the first instance, a sample of 20 terms selected by the INTERPOL 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 Kenya returned a result of 'not enough data' for each of these 20 terms.

[78] For more information on the ICCAM project, see: INHOPE: What is ICCAM and Why is it Important?.
[79] Google Trends (trends.google.com) is a publicly available tool that returns results on the popularity of search terms and strings relative to others within set parameters. Rather than displaying total search volumes, the tool calculates a score (on a range of 1 to 100) based on a search term or strings proportion to all searches on all terms/strings. Data points are divided by total searches in the geographical and time parameters set, to achieve relative popularity. While Google Trends draws on only a sample of Google searches, the dataset is deemed by the company to be representative given the billions of searches processed per day. For more information on data and scoring, see: FAQ about Google Trends data.

Returns of 'not enough data' equate with a 0 relative popularity score, indicating a comparatively low level of interest in that term (as opposed to absolute 0 search volume) within the geographical and time limits set.[80] Comparing with 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 Kenya 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 Kenya 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', for material involving children of particular ethnicities and for familial abuse appear to indicate that some web searchers in Kenya have specific requirements reflective of a more persistent and active interest in CSAM that has progressed beyond initial curiosity.

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

2.1.4 Links to travel and tourism

Some data on travelling child sex offenders can also 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 also 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. Among the foreign law enforcement authorities consulted in the context of *Disrupting Harm*, one agency reported that in 2018 they investigated one of their nationals for CSEA offences committed in Kenya, while another identified the country as a bit of a hotspot for travelling child sex offenders.

In a number of countries, convicted sex offenders are required to notify a central authority of overseas travel. Analysis of data supplied by one foreign law enforcement agency reveals that 15 notifications concerned travel to Kenya between 2015 and 2020, representing 0.23% of their total global notifications in that period, and 23.8% of notifications concerning the *Disrupting Harm* focus countries.[81] A second foreign law enforcement agency reported that out of 283 notifications of convicted sex offender travel from May 2017 to June 2020, 3% were destined for Kenya.

In addition, United States 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, the centre made 42 referrals concerning travellers to Kenya, representing 29% of the total number of referrals to *Disrupting Harm* focus countries in Africa in those years. The agency received confirmation that nine of these individuals were denied entry to the country.

[80] Ramadanti, D. (2020). Telling stories with Google Trends using Pytrends in Python.
[81] 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 KENYA

Under the *Disrupting Harm* project, OCSEA was defined specifically to include CSAM, live-streaming of child sexual abuse and online grooming of children for sexual purposes. These concepts are used here to organise and present the results of our research. At the same time, we recognise that the ways in which children are subjected to OCSEA are far more complex and nuanced. The experiences or offences in question often occur in combination or in sequence. Moreover, as explored in the box *The Continuum of Online and Offline Child Sexual Exploitation and Abuse* on page 63 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 happen either completely online or 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 build of trust between the offender and the child over an extended period of time. The child is often 'prepared' for sexual abuse and made to engage in sexual acts online or in person by means of deceit, coercion or threats. However, online grooming can also be abrupt, with an offender suddenly requesting or pressuring a child to share sexual content of themselves or to engage in sexual acts, including via extortion. Of the nine Kenyan girls which *Disrupting Harm* experts spoke to as part of the survivor conversations research activity, all had experienced online grooming as a part of the sexual exploitation and abuse they were subjected to.

Legislation on grooming

At the time of writing, Kenyan law does not specifically criminalise the grooming of children for sexual purposes. An investigator from the AHTCPU highlighted this in one of our access to justice interviews, saying that they *"rely on the Computer Misuse Act which penalises exposing a child to sexualised content and the Sexual Offences Act where we use the child pornography section. But we cannot directly charge grooming as an offence."* (RA4-KY-08-A-justice) However, an interview with a representative from the Kenya Law Reform Commission confirmed that Section 20 (3) of the upcoming Children Bill 2021 will expressly criminalise proposing to meet a child for sexual purposes through electronic systems, networks or communication technologies. Convicted offenders would be liable to imprisonment not exceeding ten years or a fine not exceeding two million shillings (approximately US$18,000) or both. (RA1-KY-09-B)

The definition contained in the upcoming Children Bill 2021 will be in line with the international standard established by the Council of Europe's Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)[82] and the EU Directive 2011/93,[83] the only two legally binding international instruments containing an obligation to criminalise the grooming of children for sexual purposes. However, it has been noted that these definitions themselves warrant updates as they require an intention to meet the child in person. In 2015 the Lanzarote Committee issued an opinion recommending 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."*[84]

[82] Council of Europe. (2007). Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. Council of Europe Treaty Series – No. 201. Article 23.
[83] European Parliament and of the Council. (2011). Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. Article 6.
[84] Council of Europe's Lanzarote Committee. (2015). Opinion on Article 23 of the Lanzarote Convention and its explanatory note. Para 20.

In Kenya, the provision of the upcoming Children Bill 2021 addressing online grooming will only cover online grooming *with the intent of meeting the child* and may not therefore apply to situations where, for example, a child is asked to send sexual content to an offender via online platforms. The bill received cabinet approval on 25 February 2021 but as of early June 2021 it still required three readings in Parliament before going to the President for promulgation. It is hoped that a provision outlawing grooming where the sexual abuse occurs online could still be included.

Patterns of victimisation

Although Kenya lacks law enforcement data on the modus operandi of grooming, the conversations with survivors of OCSEA provided insights into the tactics used by offenders to commit offences and ensure victim compliance is achieved. In our conversations with nine survivors of OCSEA from Kenya, a pattern of flattery, offers of money and other goods emerged. For example:

- *"...the kind of things every young person wants to hear, like 'You are very beautiful'."* (RA5-KY-02-A)
- *"Yes, just those flattering words that men use, like 'You are beautiful' and 'I'll buy you a present'. He once sent me money through my aunt's number and she questioned me but I just told her to give me the money. It was after sending me the money that we met the week later."* (RA5-KY-09-A)
- *"After a while he started making promises like he'll pay my fees [school fees] and even give me pocket money any time I needed. So I was lured with money and decided to finally meet him."* (RA5-KY-07)

The men these children met were all older than them:

- *"He didn't live round here and he was way older than me."* (RA5-KY-01-A)
- *"At first I thought we were age mates considering he did not post his pictures but just quotes. I was even shocked when we met..."* (RA5-KY-07-A)

Potential grooming – children asked to talk about sex

Of the participants in our household survey of 1,014 internet-using 12-17-year-olds in Kenya, 13% (127 children) had been asked to talk about sex or sexual acts when they did not want to within the past year. There were no notable differences by gender whereas 16-17 year olds were somewhat more likely to receive this requests compared to 12-13 year olds (15% and 10%, respectively). 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; therefore, we report on it here and describe the figures above as instances of potential (versus actual) grooming.

Online or offline? One third of the children who were asked to talk about sex when they did not want to, received these requests in person, 37% on social media and 10% in an online game. The 47 children who were asked to talk about sex via social media were most likely to say it happened on Facebook or Facebook Messenger, WhatsApp and YouTube.

Because asking a child to talk about sex can happen without the involvement of technology, only children who most recently received these requests on social media or in an online game (58 of the 127 children) were included in the subsequent analysis, as they represent potential OCSEA cases.

How children felt: Of the 58 children who were asked to talk about sex when they did not want to via an online channel (i.e., social media or an online game), 75% reported negative feelings about the experience, while one in four said it did not affect them. The most common negative feelings cited by these children were feelings of embarrassment or annoyance. Other children said they felt angry, betrayed, guilty, distressed and scared.

How children respond: In our subsample of 58 children who were asked online to talk about sex when they did not want to, 36% refused to do so. About a quarter blocked the offender, while 17% of children ignored the problem and hoped it would go away on its own. Others asked the offender to leave them alone, stopped using the internet for a while, changed privacy settings, and deleted messages from the sender. Nevertheless, a small proportion (4 children) did as they were asked.

IN THE PAST YEAR

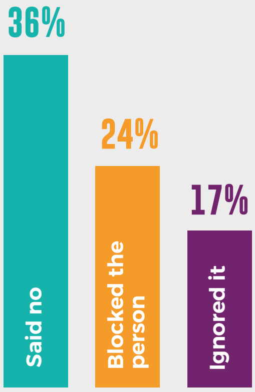
I HAVE BEEN ASKED TO TALK ABOUT SEX WHEN I DID NOT WANT TO

YES 13%

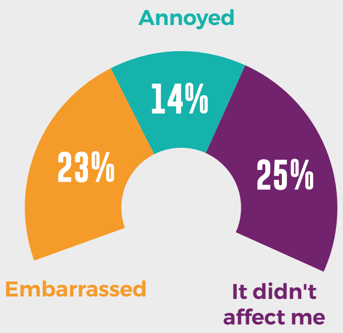
n= 1,014 children

THE LAST TIME THIS HAPPENED ONLINE...

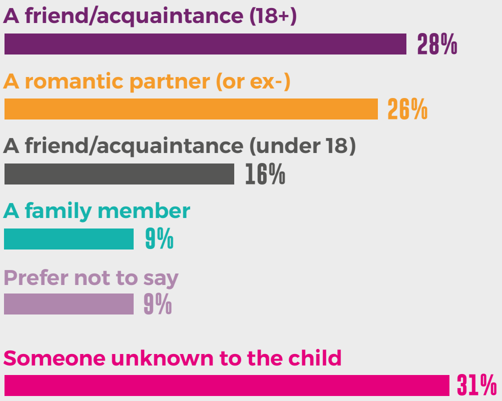
What did you do?*†



How did you feel?*

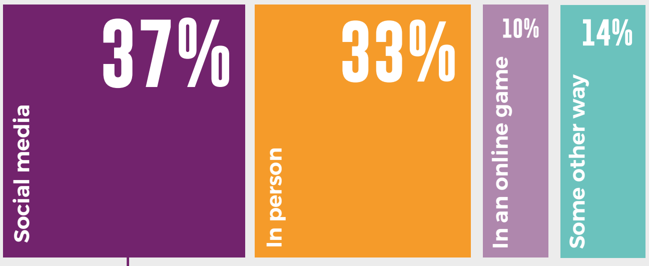


Who did it?*†



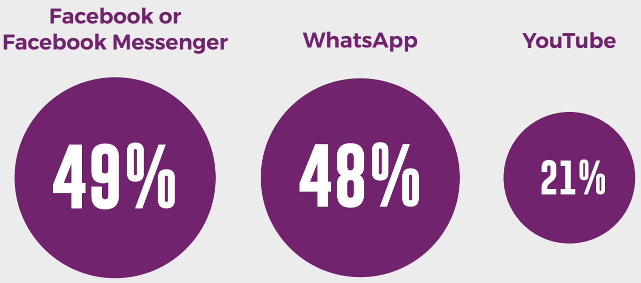
n= 58 internet-using children aged 12-17 who received unwanted requests *online* to talk about sex in the past year.

Where did it happen?*†



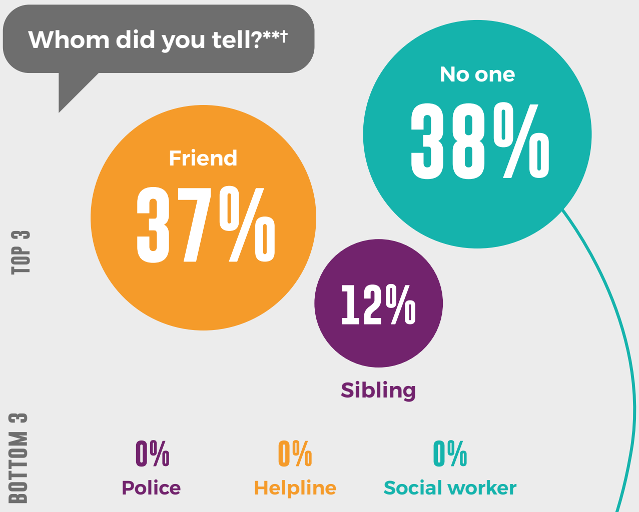
n= 127 internet-using children aged 12-17 who received unwanted requests to talk about sex in the past year.

On which platform did this happen?*†



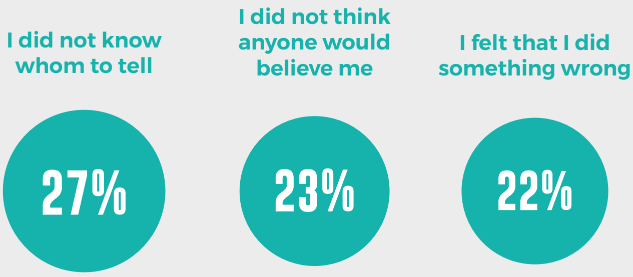
n= 47 internet-using children aged 12-17 who *most recently* received unwanted requests *via social media* to talk about sex.

Whom did you tell?**†



n= 58 internet-using children aged 12-17 who received unwanted requests *online* to talk about sex in the past year.

Why did you not tell anyone?*†



n= 22 internet-using children aged 12-17 who *did not tell anyone* the last time they received unwanted requests *online* to talk about sex.

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

Source: Disrupting Harm data

Who makes the requests: As illustrated on page 46, the people who most commonly asked children to talk about sex online were adult friends or acquaintances, followed by current or former romantic partners, friends or acquaintances aged under 18, and family members. Close to one third of children said the offender was someone unknown to them. Although this is not a small proportion of cases, when taken together, those who are already part of the child's life are more likely to send them these kinds of requests than individuals unknown to the child.

Whom children tell about it – if anyone: Twenty-two children who received unwanted requests to talk about sex online did not confide in anyone at all. Children who did disclose what happened were most likely to tell a friend, but few spoke to an adult about it.

None of the 58 children reported what had happened to them through an online reporting function. This could be because children do not know where to go or whom to tell about these experiences. This was the most common reason provided by children who did not talk to anyone about what happened. In fact, only 24% of the children in our full sample of 1,014 were confident that they knew how to report harmful content on social media, while 61% said they did not know where to get help if they or a friend were subjected to sexual harassment or abuse.

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 through digital technologies, whether or not they also intend to meet the child in person.

A behaviour that could be an indication of grooming is sending children unwanted requests to share sexual content of themselves. Within the past year, 10% of the internet-using children we surveyed (101 children) had received unwanted requests for a photo or video showing their private parts. There were only minor differences by gender or age group. While 20% of these children said they were not affected the last time they received such a request, 76% felt negatively about it. Feelings of embarrassment and anger were the most common, followed by being annoyed, scared or distressed.

> “Most children who received unwanted requests to talk about sex online did not confide in anyone all. Some of them told a friend, but few spoke to an adult about it.”

How children respond: Of the 101 children who received unwanted requests to share images of their private parts, 44% refused. Other common responses included blocking the other person, ignoring the problem and hoping it would go away by itself. Eleven percent of children changed their privacy settings.

Nine percent of children who were asked to share sexual images or videos of themselves complied. The youngest children (aged 12-13) were most likely to comply. Boys were more likely than girls to agree to send images or videos of their private parts even though they did not want to.

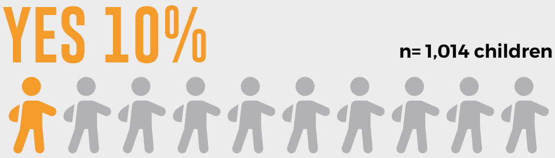
Who makes the requests: Of the children who had received unwanted requests to share a sexual image or video of themselves, 32% named a romantic partner as the source of the request. Adult friends or acquaintances accounted for 23% of the cases, a family member for 15% and a friend younger than 18 for 12%. A quarter of the children said the offender was a someone unknown to them.

Overall, children are more likely to receive unwanted requests to talk about sex or share sexual content by people they already know, rather than by individuals unknown to them. The fact that at least one request in five came from an adult makes it likely that some of these experiences constituted grooming.

Online or offline? More than half (54%) of the 101 children who were subjected to unwanted requests for sexual content said the requests were made via social media. Seven percent of children said the requests came through online games. About one in five said they were asked in person. Once again,

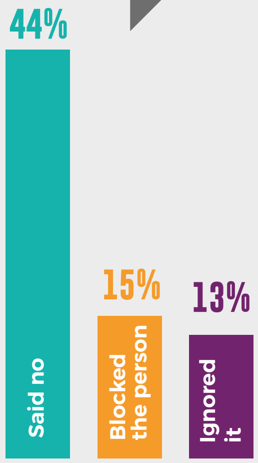
IN THE PAST YEAR

I WAS ASKED FOR A PHOTO OR VIDEO SHOWING MY PRIVATE PARTS WHEN I DID NOT WANT TO

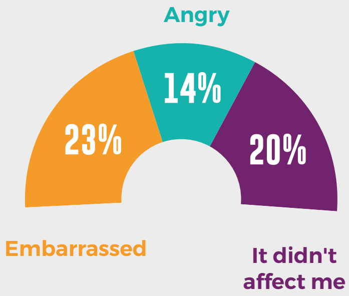


THE LAST TIME THIS HAPPENED...

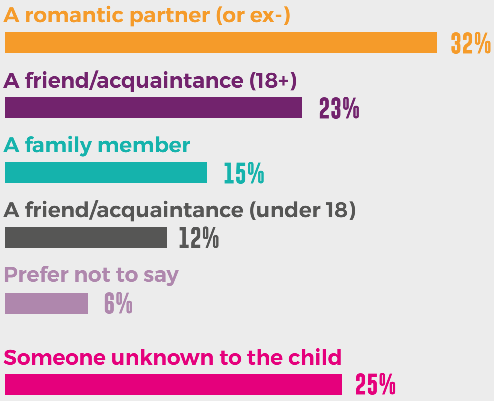
What did you do?*†



How did you feel?*

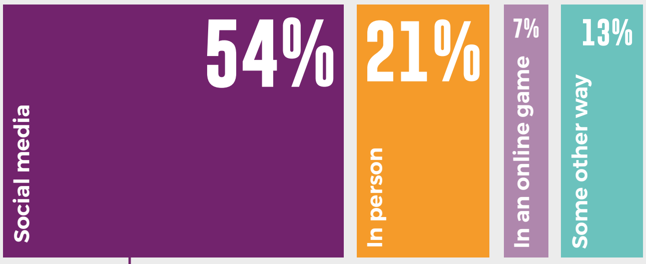


Who did it?*†



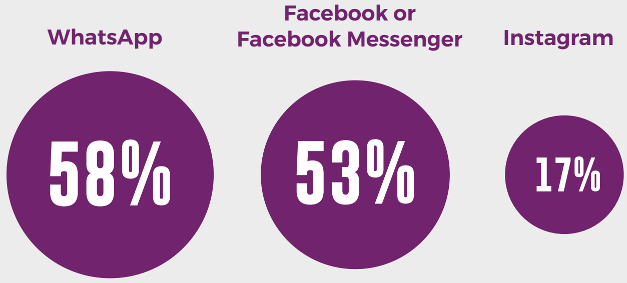
n = 101 internet-using children aged 12-17 who received unwanted requests for sexual images in the past year.

Where did it happen?*†



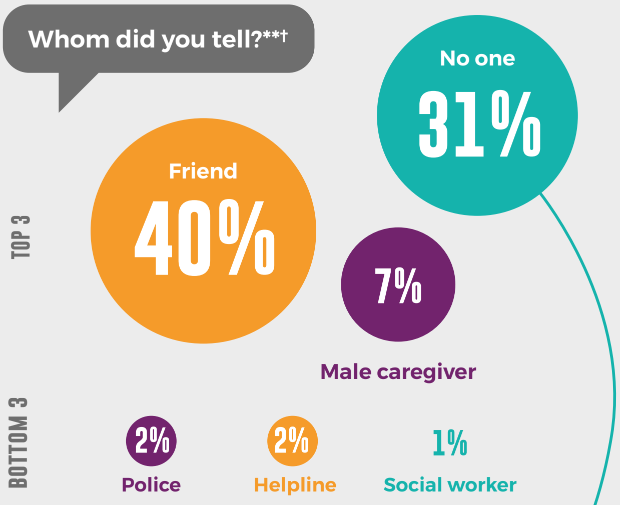
n= 101 internet-using children aged 12-17 who received unwanted requests for sexual images in the past year.

On which platform did this happen?*†



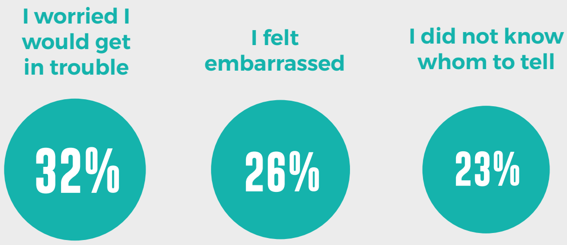
n= 54 internet-using children aged 12-17 who *most recently* received unwanted requests for sexual images *via social media*.

Whom did you tell?**†



n= 101 internet-using children aged 12-17 who received unwanted requests for sexual images in the past year.

Why did you not tell anyone?*†



n= 31 internet-using children aged 12-17 *who did not tell anyone* the last time they received unwanted requests for sexual images.

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

Source: Disrupting Harm data

WhatsApp and Facebook or Facebook Messenger were the social media and instant messaging apps via which children were most commonly targeted. This is probably because Facebook and WhatsApp – the two most popular social media platforms in Kenya[85] – are where children spend much of their time online.

Whom children tell about it – if anyone: Among children who received unwanted requests to send images or videos showing their private parts, 40% told a friend, but almost one in three did not share their experience with anyone. Very few survey respondents formally reported what happened to them through an online reporting system. For the 31 children who did not disclose the unwanted requests for sexual content to anyone, the main barriers were being worried about getting into trouble, feeling embarrassed, or not knowing where to go or whom to tell.

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. Seven percent of children in the household survey (67 children) said they had been offered money or gifts in return for sexual images or videos in the past year. There were no clear differences by age group or gender.

Asked about the last time they were offered money or gifts in exchange for sexual content, most of the 67 children said they received the offer from someone they already knew. Close to a quarter were offered money or gifts by romantic partners. These were followed by friends or acquaintances younger than 18, and adult friends or acquaintances. Among persons known to the child, family members were the least likely to make offers of this kind (12%) (see page 50 below). Individuals unknown to the child accounted for around one third of all cases.

While 25% of the children said that the offer of money or gifts was made in person, most offers were made online – 49% on social media and 18% via an online game. Among the 33 children who received such offers via social media, the most common platforms cited were Facebook or Facebook Messenger, WhatsApp and YouTube. Four children cited Instagram and two TikTok.

Over a third of the children offered money or gifts in return for sexual images told a friend the last time this happened. Caregivers were the next most common confidants – 16% told a male caregiver and 10% told a female caregiver. Only one of the 67 children spoke to a helpline and no one reported to the police or spoke to a social worker Twenty-eight percent did not tell anyone at all. The 19 children who did not disclose or report what happened said that the main barrier to reporting was not knowing where to go or whom to tell. Other children said that they would feel embarrassed or ashamed or that it would be emotionally difficult for them to share their experiences.

Offering children money or gifts for sexual acts in person

It is clear from the conversations with survivors of OCSEA conducted as part of the research for *Disrupting Harm* that the grooming of children online for the purpose of meeting in person to engage in sexual activities can be a real threat.

All nine of the Kenyan girls we spoke to in our OCSEA survivor conversations had met an offender in person after connecting online and then been subjected to sexual abuse and exploitation. Of note is that none of these children spoke of sexual images or videos being made or exchanged online. While this sample is not representative of all survivors, it provides some insight into the interactions between children and offenders.

- *"Yes. When I told him I was going home since it was late, he said he has to have sex with me. So when I wanted to escape he forced me."* (RA5-KY-05-A)

To return to our household survey results with 1,014 children, 7% of the internet-using children surveyed (67 children) said they had been offered money or gifts to meet someone in person to do something sexual within the past year. Like other findings, these numbers may be under-reported as children may not feel comfortable or safe enough to disclose their experiences of abuse and exploitation.

Online or offline? Of the 67 children who said they had been offered money or gifts to meet in person for sexual activities in the past year, almost half said that this unwanted request came through social media and 9% through an online game (see page 51). Nineteen percent of children received the offer in person.

[85] United States International University – Africa. (2019). Social Media Consumption in Kenya: Trends and Practices.

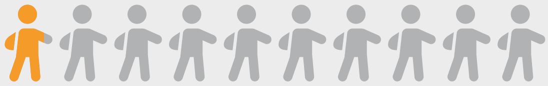
OCSEA

IN THE PAST YEAR

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

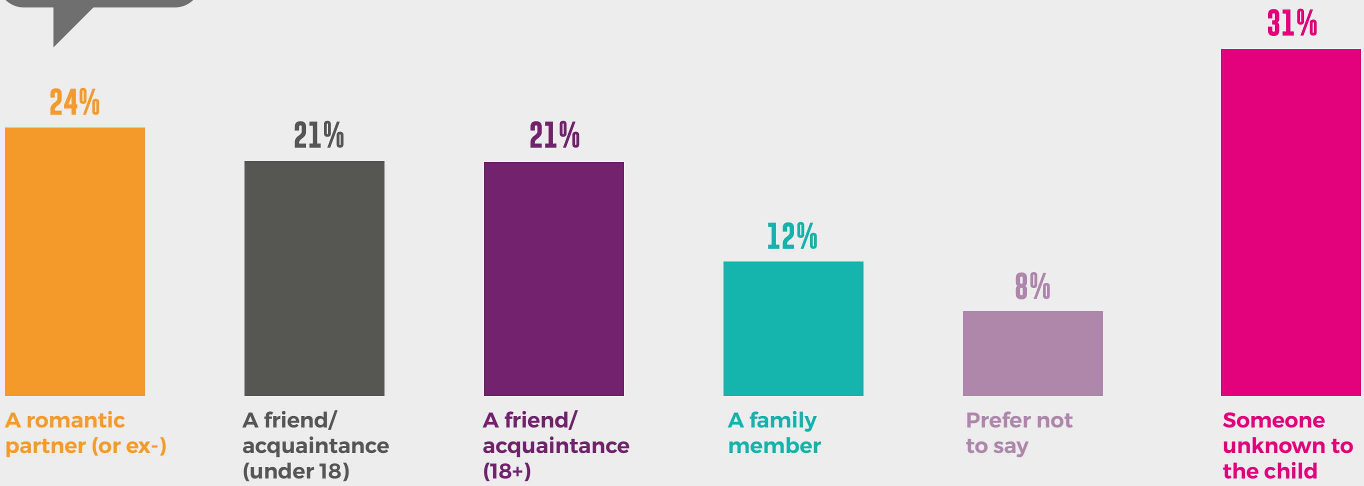
YES 7%

n= 1,014 children



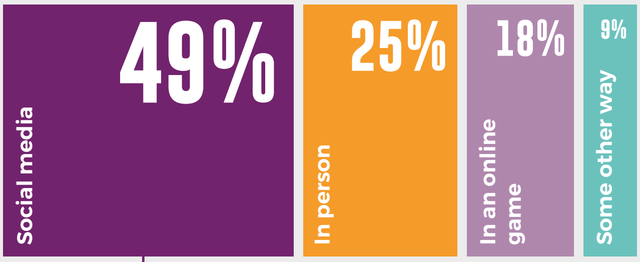
THE LAST TIME THIS HAPPENED...

Who did it?*†



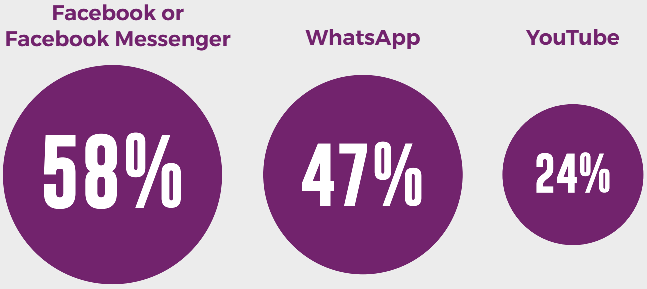
n= 67 internet-using children aged 12-17 who were offered money or gifts for sexual images or videos.

Where did it happen?*†



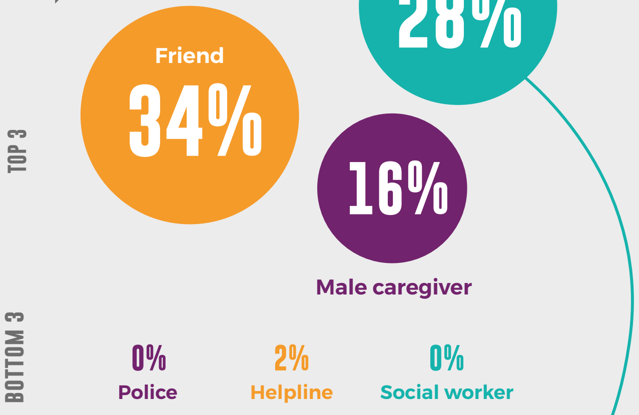
n= 67 internet-using children aged 12-17 who were offered money or gifts for sexual images or videos.

On which platform did this happen?*†



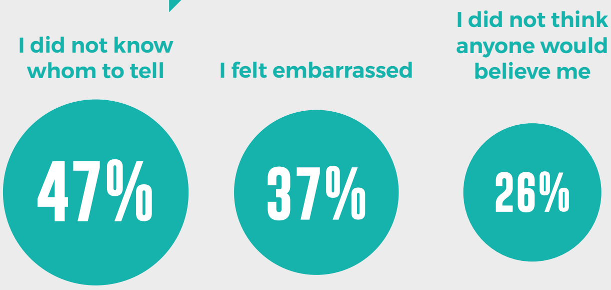
n= 33 internet-using children aged 12-17 who *most recently* were offered money or gifts *via social media* in exchange for sexual images or videos.

Whom did you tell?**†



n= 67 internet-using children aged 12-17 who were offered money or gifts for sexual images or videos.

Why did you not tell anyone?*†



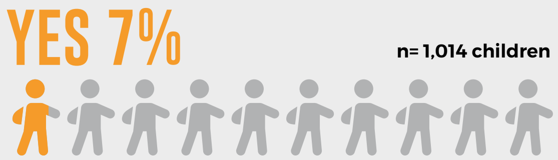
n= 19 internet-using children aged 12-17 who *did not tell anyone* the last time they were offered money or gifts for sexual images or videos.

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

Source: Disrupting Harm data

IN THE PAST YEAR

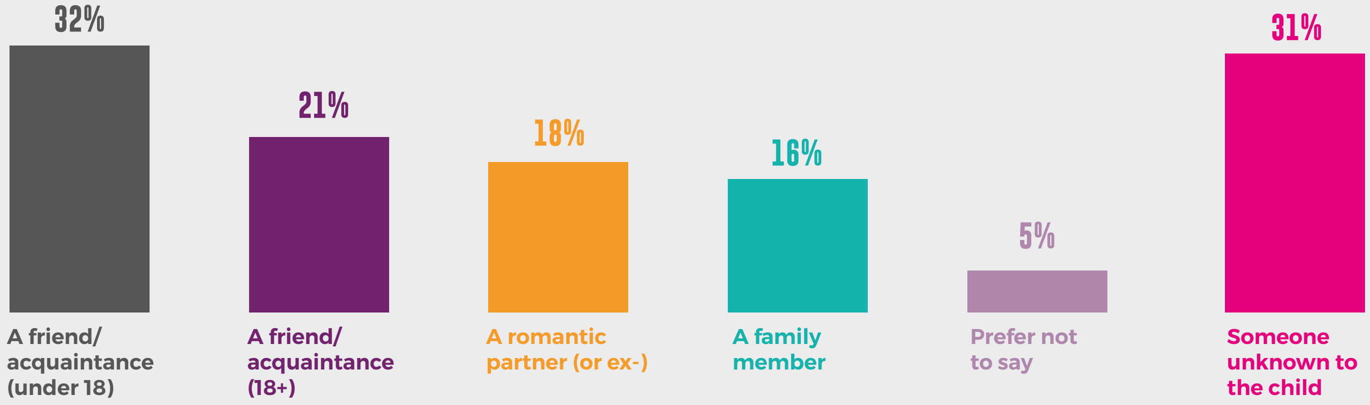
I WAS OFFERED MONEY OR GIFTS TO MEET IN PERSON TO DO SOMETHING SEXUAL



n= 1,014 children

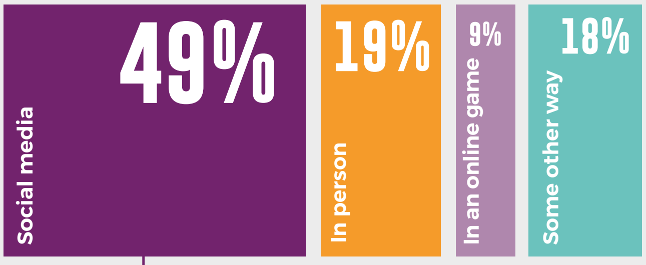
THE LAST TIME THIS HAPPENED ONLINE...

Who did it?*†



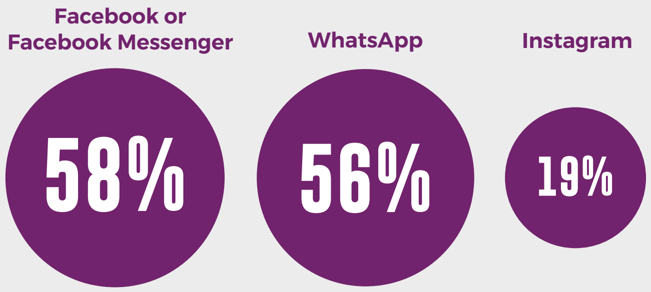
n= 38 internet-using children aged 12-17 who were offered money or gifts *online* for in-person sexual acts in the past year.

Where did it happen?*†



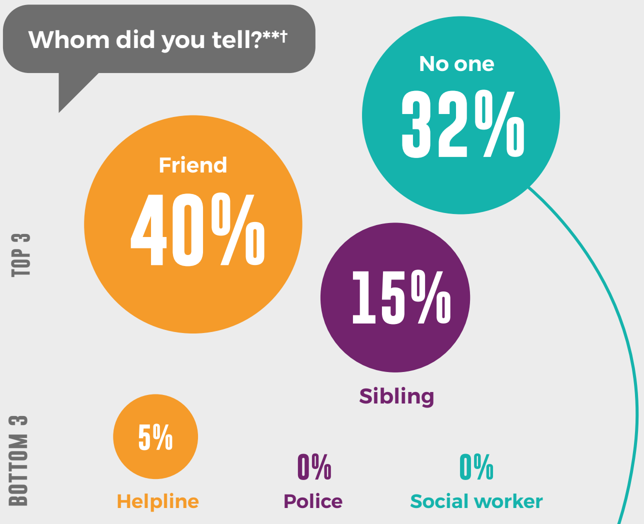
n= 67 internet-using children aged 12-17 who were offered money or gifts for in-person sexual acts in the past year.

On which platform did this happen?*†



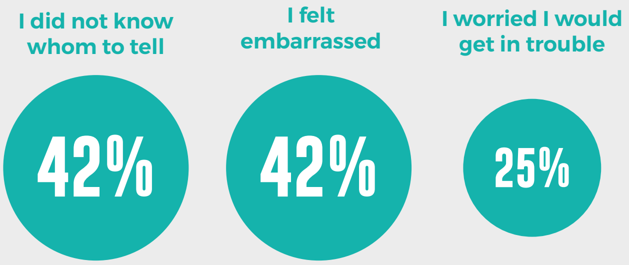
n= 33 internet-using children aged 12-17 who *most recently* received offers of money or gifts for in-person sexual acts *via social media.*

Whom did you tell?**†



n= 38 internet-using children aged 12-17 who were offered money or gifts *online* for in-person sexual acts in the past year.

Why did you not tell anyone?*†



n= 12 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.

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

Source: Disrupting Harm data

Among the 33 children who received offers of money or gifts to engage in sexual acts in person *via social media*, the most common platforms cited were Facebook or Facebook Messenger and WhatsApp, followed by Instagram.

Among the 38 children in the survey who had been offered money or gifts *online – i.e., via social media or an online game* – to meet in person for sexual acts, the offers came from a range of sources. These included offers from someone unknown to the child, from a peer younger than 18 and from an adult friend or acquaintance. Current or former romantic partners and family members were less likely to make offers of this kind.

Once again, children were very unlikely to report these incidents through formal channels and instead tend to confide in the people close to them, most commonly a friend or sibling. Almost a third of the children who had been offered money or gifts in return for sexual acts via online channels (12 children) did not tell anyone. The most common reasons which these children gave for not disclosing their experiences were feelings of embarrassment and shame (explored in more detail in the box 'Social and cultural barriers to disclosing OCSEA in Kenya' on page 67) and not knowing where to go or whom to tell.

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. In Kenya, sexual extortion committed online is not specifically criminalised by law.

Seven percent of the internet-using children in the household survey (71 children) said that they had been threatened or blackmailed to engage in sexual activities within the past year. It is unclear what kind of threats were used. No question was asked about the use of sexual images to extort money.

> **Seven percent of the internet-using children in the household survey said that they had been threatened or blackmailed to engage in sexual activities within the past year.**

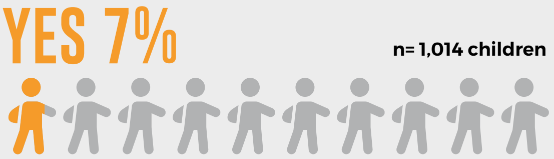
The use of online channels was common for this kind of abuse. Of the 71 children, 45% said that the last time this happened they had been threatened or blackmailed via social media and 9% through an online game. However, it also happened in person to a considerable extent. Among social media channels, the most common platforms where children experienced this were Facebook or Facebook Messenger and WhatsApp. Almost one third of these children cited Instagram. Twenty-eight percent of the children said that they had been threatened or blackmailed in person.

For the 38 children who were threatened or blackmailed *online* – i.e., via social media or an online game – the most common offender was an adult friend or other acquaintance, followed by someone unknown to the child, and a friend or acquaintance younger than 18 years. Seven children reported that current or former romantic partners did it, and three said that it was done by a family member. Overall, as with the other forms of OCSEA explored in this chapter, sexual extortion was more commonly committed by individuals known to the child than by people they do not know.

Of the 38 children, 18 told a friend about the incident, whereas nine did not tell anyone. Low disclosure of sexual extortion is perhaps to be expected as it is based on threatening to disclose images and cause embarrassment, making it even harder to seek help. Only one child reported to the police, one child spoke to a social worker and one child called a helpline.

IN THE PAST YEAR

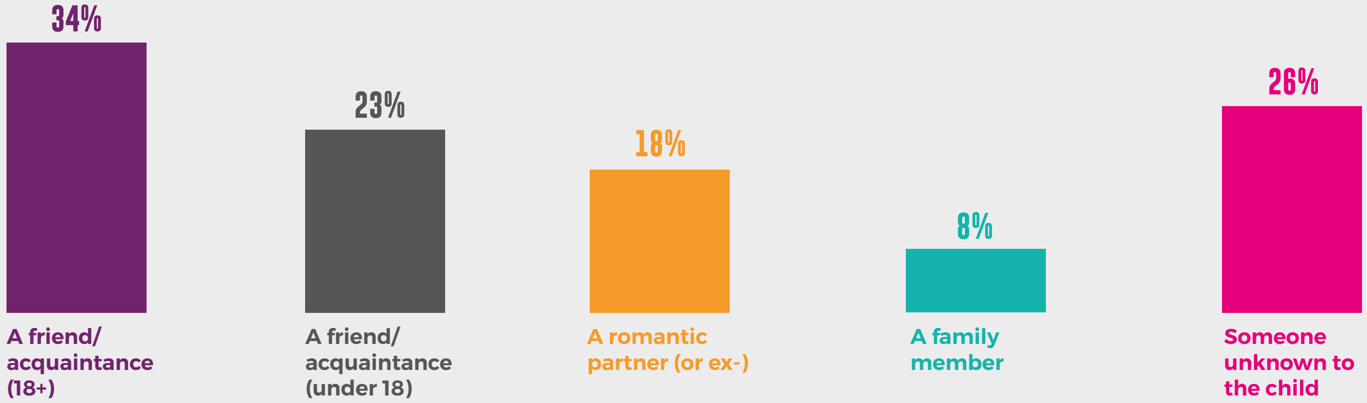
SOMEONE THREATENED OR BLACKMAILED ME TO ENGAGE IN SEXUAL ACTIVITIES



n= 1,014 children

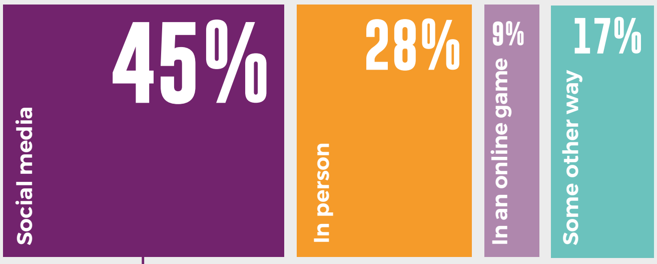
THE LAST TIME THIS HAPPENED ONLINE...

Who did it?*†



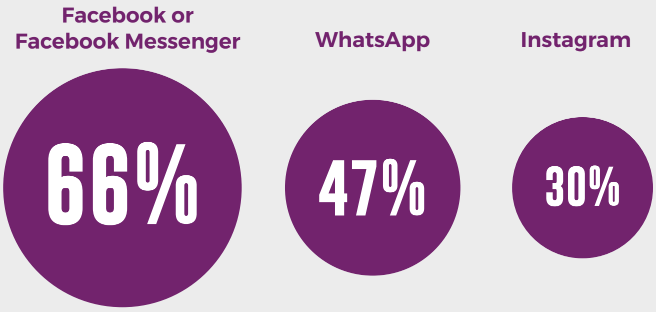
n= 38 internet-using children aged 12-17 who were threatened or blackmailed *online* to engage in sexual acts in the past year.

Where did it happen?*†



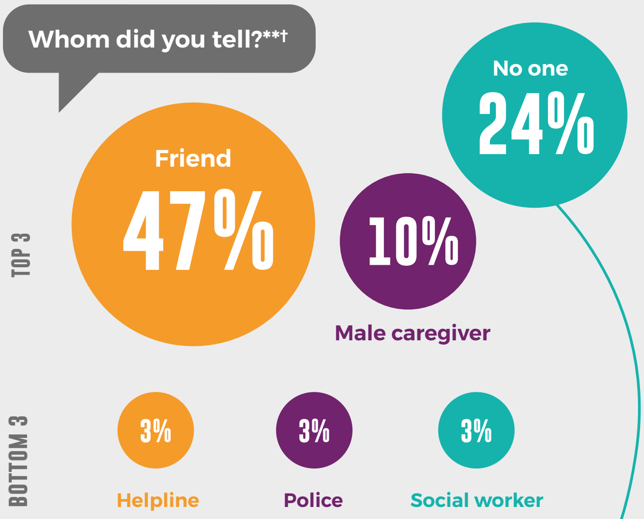
n= 71 internet-using children aged 12-17 who were threatened or blackmailed to engage in sexual acts in the past year.

On which platform did this happen?*†



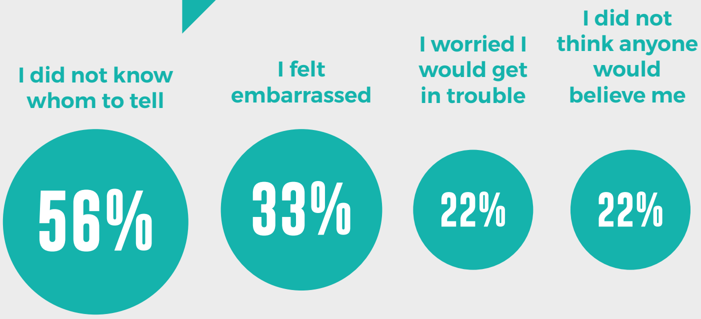
n= 32 internet-using children aged 12-17 who *most recently* received threats or were blackmailed *via social media*.

Whom did you tell?**†



n= 38 Internet-using children aged 12-17 who were threatened or blackmailed *online* to engage in sexual acts in the past year.

Why did you not tell anyone?*†



n= 9 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.

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

Source: Disrupting Harm data

The most common reasons given by the children who did not disclose the incident were not knowing where to go or whom to tell, feeling embarrassed, being worried about getting in trouble and not thinking anyone would believe them.

2.2.2 CSAM and live-streaming of child sexual abuse

Kenyan legislation explicitly defines CSAM and criminalises acts associated with it.[86,87] The legal definition covers visual and audio material as well as digitally-generated CSAM.[88] However, knowingly obtaining access to CSAM is not explicitly criminalised – a major loophole. Similarly, live-streaming of child sexual abuse is not an explicit offence in current legislation. This can pose challenges for prosecution. A respondent in one of our government duty-bearer interviews stated that *"Live-streaming is not defined in our law; so prosecuting such a case is difficult because it's not anchored and is not defined in any law."* (RA1-KY-08-A)

The upcoming Children Bill 2021 will not expressly define this crime either. However, a senior researcher from the Kenya Law Reform Commission argued that articles 20(3)(b) and (c) of the Act would implicitly cover live-streaming of child sexual abuse as they refer to *"transmission of obscene material"* and *"online abuse and exploitation."* (RA1-KY-09-B) While CSAM and live-streaming of child sexual abuse are currently considered separate concepts in law, the distinction is artificial because live-streaming of child sexual abuse is one way in which CSAM can be produced, disseminated and consumed. Legislators should be aware of the overlaps between these concepts.

How technological development has influenced OCSEA

The wide availability of faster and cheaper internet access has led to the increasing use of video tools in communications. Video chat and live-streaming tools have rapidly gained popularity and are changing the ways we engage with each other, particularly for young people (34% of 12-17 internet users in Kenya watch live-streams weekly). Live-streaming is increasingly used both amongst small private groups and for 'broadcasts' to large, public, unknown audiences. 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.

Concerningly for law enforcement authorities, many streaming platforms do not create any records, because video is not downloaded or retained by default, although metadata is. This means that when the streaming stops the CSAM vanishes, unless the offender deliberately records it. This increases the chances of impunity for offenders, and 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 chapter 1.3.3, 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 through non-consensual on-sharing or nefarious means, such as hacking. Governments and support services everywhere are grappling with how to address these issues.

[86] Republic of Kenya. (2018). The Computer Misuse and Cybercrimes Act No. 5 of 2018. Section 24.
[87] Republic of Kenya. (2006). The Sexual Offences Act No. 3 of 2006. Section 16 (3)(b). (Last revised in 2019).
[88] Republic of Kenya. (2018). The Computer Misuse and Cybercrimes Act No. 5 of 2018. Section 24 (3).

Children's experiences of non-consensual sharing of sexual images

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

Moreover, 7% of the internet-using children aged 12-17 in Kenya (72 children) who took part in the *Disrupting Harm* household survey stated that someone had shared sexual images of them without their permission in the past year, with no notable variations by gender or age group.[89] This is an alarming number considering the severity of this crime. These images, and particularly those shared online, can be circulated widely and repeatedly viewed all over the world, resulting in a continuous sense of fear of being recognised for the victims.

When these images or videos are recordings of severe sexual abuse, the trauma associated with those in-person experiences can also be repeatedly reactivated as the content is shared further.

Case Study – High school students' experiences of non-consensual sharing of sexual images

In April 2020, Kenya's Directorate of Criminal Investigations received a call from one of the banks in the country about a suspected case of non-consensual sharing of sexual images. The case concerned a student with a scholarship from the bank, an 18-year-old who had reported to the police that his schoolmate, a 17-year-old boy, had circulated the victim's nude photos via social media (WhatsApp, Instagram and Twitter) under fake accounts purported to belong to the victim. According to the victim, the suspect had posed as a girl on social media and tricked him into sharing the images. The accounts showing his images also portrayed him as gay (which is illegal in Kenya). The Directorate requested Instagram, Twitter and Facebook to preserve the evidence and pull down the fake accounts. The case is Pending Under Investigation.

> "In one of the cases we were dealing with, the caregivers were feeling like a case involving CSAM was not serious as it only involved a picture so their attitude was 'This child is only on the picture, no one has done anything to her, so why do you want us to pursue a court case?'"

According to the 72 children in the household survey whose sexual images had been shared without their permission the last time this happened to them, the persons most commonly responsible were individuals unknown to the child, friends or acquaintances younger than 18, adult friends or acquaintances, and (current or former) romantic partners. Family members were least likely to share sexual images without permission.

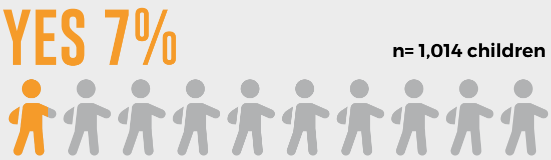
Fifty-five percent of the children whose images had been shared without their permission said that the they were shared via social media – particularly WhatsApp, followed by Facebook/Facebook Messenger and YouTube. Boys were more likely to have their images shared on social media than girls. Only 4% said the images were shared through an online game. Fourteen percent said they were shared in person.

The children abused in this way were most likely to confide in a friend or not to tell anyone at all. As shown on page 56, a few children confided in a sibling or caregiver. Almost no one turned to a helpline, and no children reported the incident to the police or a social worker. Among the 22 children who did not tell anyone, the most common reasons for not disclosing were not knowing where to go or whom to tell, worries over getting into trouble, embarrassment and not thinking anyone would believe them.

[89] Note that all sexual images of a child are in fact defined as CSAM under Kenyan law, regardless of whether the child shares them voluntarily or they are shared without permission.

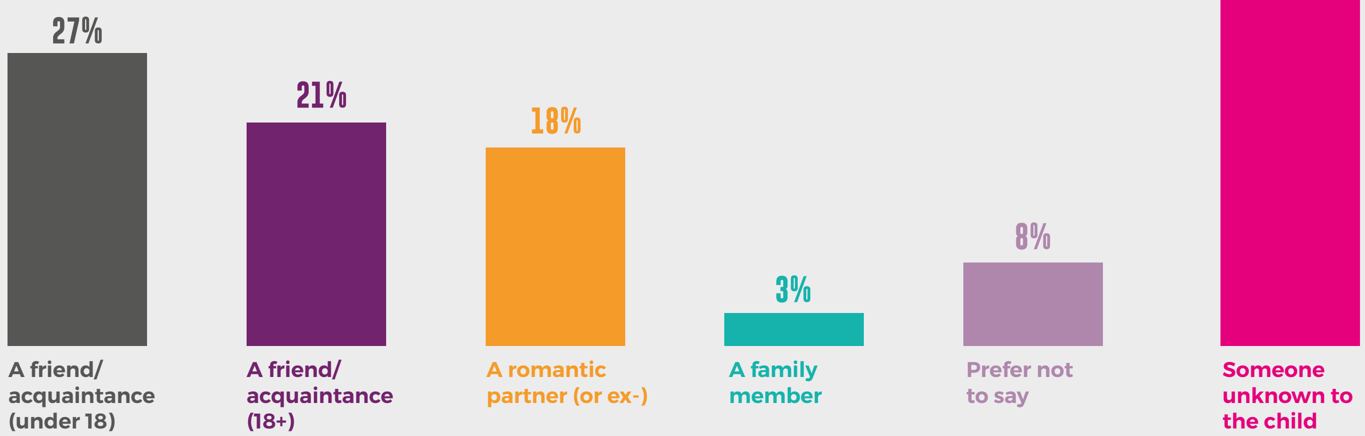
IN THE PAST YEAR

SOMEONE SHARED SEXUAL IMAGES OF ME WITHOUT MY PERMISSION



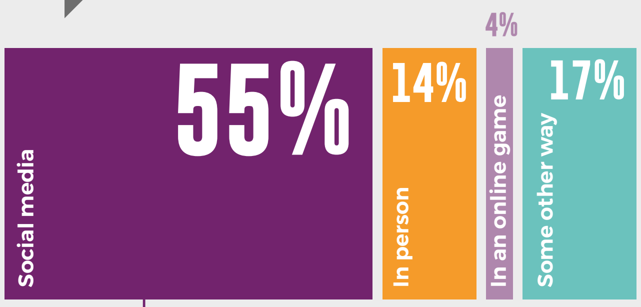
THE LAST TIME THIS HAPPENED...

Who did it?*†



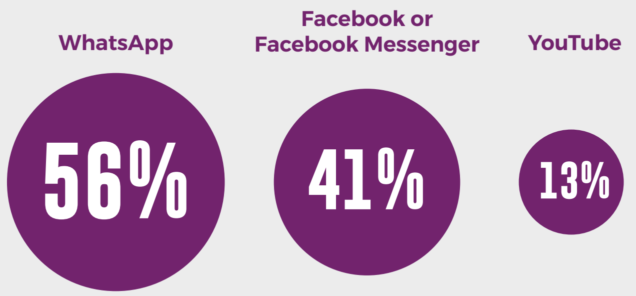
n= 72 internet-using children aged 12-17 whose sexual images were shared non-consensually in the past year.

Where did it happen?*†



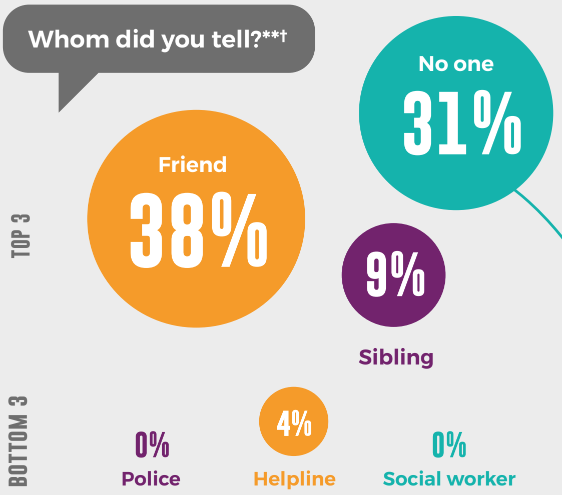
n= 72 internet-using children aged 12-17 whose sexual images were shared non-consensually in the past year.

On which platform did this happen?*†



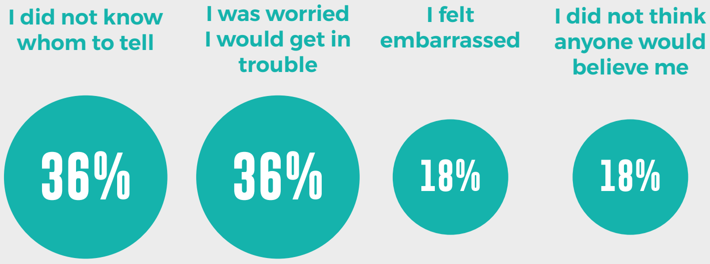
n= 39 internet-using children aged 12-17 whose sexual images were *most recently* shared *via social media.*

Whom did you tell?**†



n= 72 internet-using children aged 12-17 whose sexual images were shared non-consensually in the past year.

Why did you not tell anyone?*†



n= 22 Internet-using children aged 12-17 who *did not tell anyone* the last time their sexual images were shared non-consensually.

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

Source: Disrupting Harm data

Attitudes to non-consensual sharing of sexual images

Not everybody is aware of the gravity of sharing sexual images of others without their permission. According to one justice professional interviewed for this report: *"In one of the cases we were dealing with, the caregivers were feeling like a case involving CSAM was not serious as it only involved a picture so their attitude was 'This child is only on the picture, no one has done anything to her, so why do you want us to pursue a court case?'"* (RA4-KY-05-A-justice)

The findings of our household survey of 1,014 internet-using 12-17-year-olds and their caregivers show a degree of awareness. Sixty-seven percent of the children and 83% of the caregivers surveyed agreed that if a person has naked images or videos of someone else, it should be illegal to share them with other people. Among the same children and caregivers, however, 63% and 74% respectively were of the opinion that *"if someone takes naked images or videos of themselves, it is their fault if they are shared with other people"*. This kind of victim-blaming may partly explain the low levels of reporting by children subjected to various forms of OCSEA in the past year.

Accepting money or gifts in exchange for sexual images or videos

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

While the practice of accepting money or gifts in exchange for sexual activities is not new,[90,91,92] the use of digital technologies – including by children and young people – to self-produce and send images or videos of oneself in return for money or other material incentives is an emerging trend. This practice could increase the risk of non-consensual sharing: 90% of the 'youth-generated' sexual images and videos assessed in a study by the Internet Watch Foundation and Microsoft were 'harvested' from the original online location and shared on third party websites.[93]

> “This suggests that one out of every twenty internet users in Kenya in this age group may receive money for sexual images or videos at least once a year.”

Given the sensitivity of this topic, only the 15–17-year-old respondents in the household survey were asked whether they had accepted money or gifts in exchange for sexual images or videos of themselves. Among the 563 respondents who were asked, 5% said they had done this in the past year. This suggests that one out of every twenty internet users in Kenya in this age group may receive money for sexual images or videos at least once a year. Some children may have been hesitant to reveal their involvement in such activities – even in an anonymised survey – so the true figure could be even higher.

By making financial micro-transactions easy and instant, the growing use of digital and mobile payments may facilitate this form of OCSEA. Kenya is known for its widespread use of digital payments.[94,95] As of March 2019, 223,084 mobile money agents and 32 million subscriptions to mobile money transfers were recorded in the country. More than 80% of the mobile money transactions were referred to M-Pesa – the first mobile money service launched in 2007, which offers retail financial services via mobile phones to Kenyans, especially those in under-served rural areas.[96] Globally, there has long been concern, particularly within the law enforcement community, of the risk of 'borderless' cryptocurrencies being misused to facilitate child abuse.[97]

[90] Zulu, E.M. , F.N. Dodoo and A.C. Ezeh (2002). "Sexual Risk-Taking in the Slums of Nairobi, Kenya, 1993-98." Population Studies 56(3):311-323.
[91] Kabiru, C. W., Beguy, D., Undie, C.-C., Zulu, E. M., & Ezeh, A. C. (2010). Transition into first sex among adolescents in slum and non-slum communities in Nairobi, Kenya. Journal of Youth Studies, 13(4), 453–471.
[92] Stoebenau, K., Heise, L.,Wamoyi, J., & Bobrova, N. (2016). Revisiting the understanding of "transactional sex" in sub-Saharan Africa: A review and synthesis of the literature. Social Science & Medicine, vol. 168, 186-197.
[93] Internet Watch Foundation & Microsoft. (2015). Emerging Patterns and Trends Report #1 Online-Produced Sexual Content.
[94] The Kenyan Wall Street. (2019). Kenya Tops in Mobile Money Penetration Globally.
[95] World Bank. (2018). The Little Book on Financial Inclusion.
[96] World Bank. (2018). What Kenya's mobile money success could mean for the Arab world.
[97] Internet Watch Foundation. (2014). Briefing Paper – Preliminary Analysis of New Commercial CSAM Website Accepting Payment by Bitcoin.

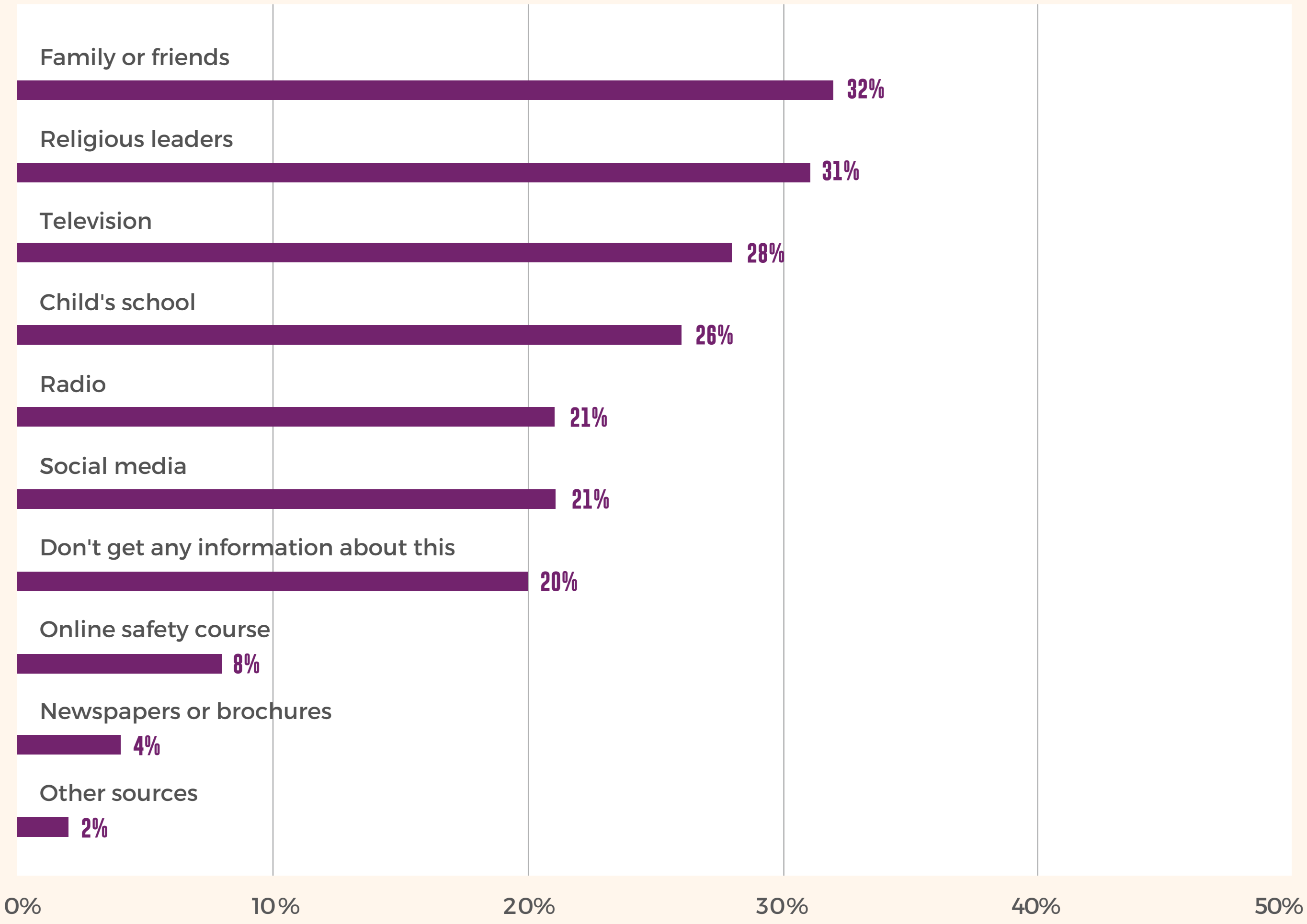
Caregivers' knowledge about OCSEA

Six of the ten caregivers of young people who had accessed the justice system who were interviewed for *Disrupting Harm* said that they had previous knowledge of OCSEA. The other four only became aware of the phenomenon after children in their care were abused. Although they said that they now know what OCSEA is, when asked to describe it, most of the caregivers gave limited explanations:

- *"It is an exploitation that happens online for children on the internet they are exposed to for the purpose of exploitation or abuse."* (RA4-KY-10B-caregiver)
- *"It is where children are abused online."* (RA4-KY-06B-caregiver and RA4-KY-09B-caregiver)
- *"…things that happen to children when they are exposed to things online and when there's no limitations or supervision by their caregivers"* (RA4-KY-05B-caregiver)

According to our household survey of internet-using children and their caregivers, caregivers in Kenya are most likely to obtain information from family or friends, religious leaders, television, and schools on how to keep their children safe online (see Figure 24).

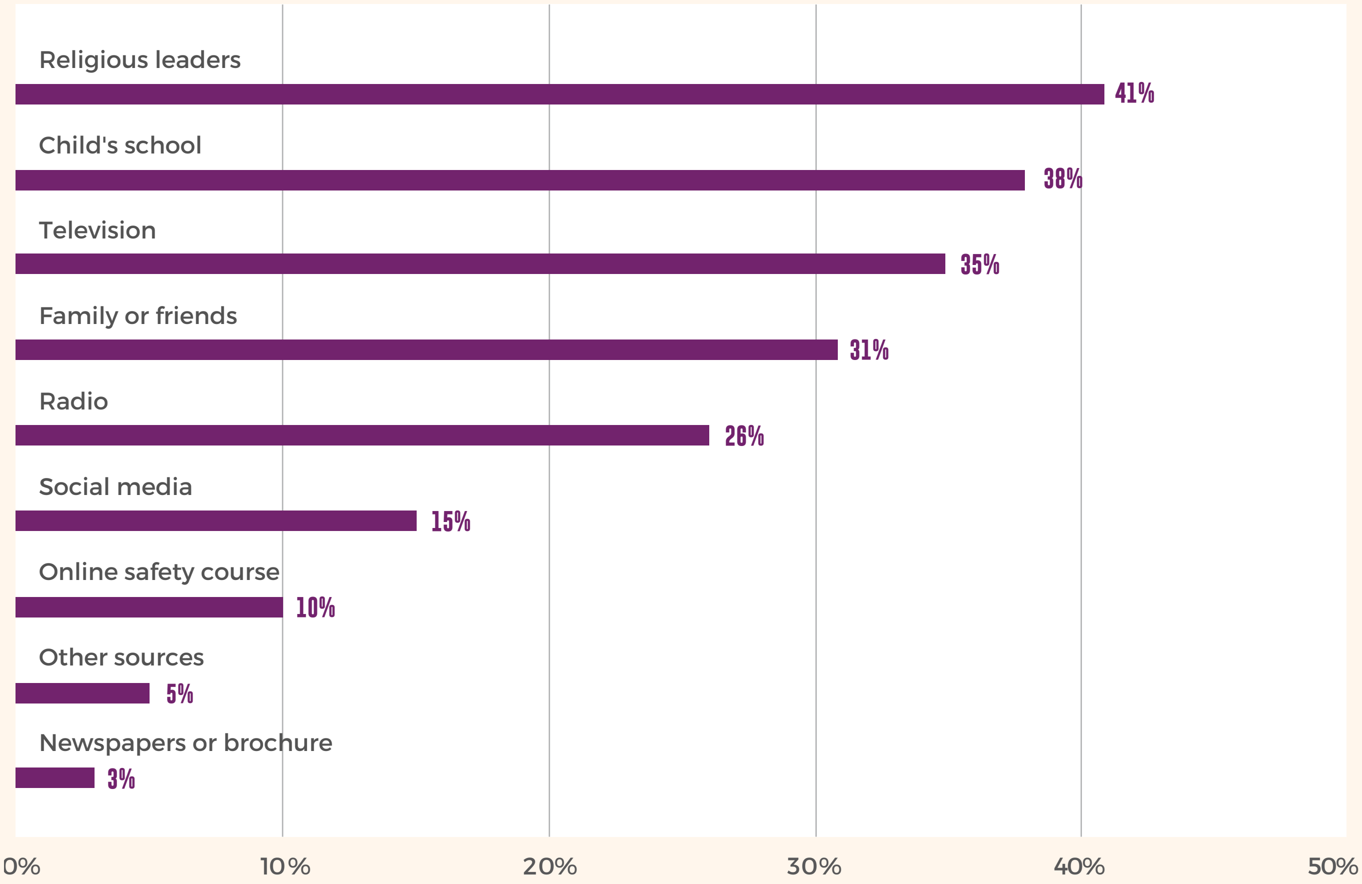
Figure 24: Caregivers' sources of information on how to support their children's internet use and keep them safe online



Base: Caregivers of internet-using children aged 12-17 in Kenya (For 'online safety course' and 'social media': Caregivers who use the internet). n = 1,014 (For 'online safety course' and 'social media', n = 522).

Figure 25 shows the channels through which caregivers would ideally like to obtain information on the same subject. While these channels broadly coincide with their existing sources of information, religious leaders and the child's school are the two most popular answers.

Figure 25: Caregivers' preferred sources of information on how to support their children's internet use and keep them safe online



Base: Caregivers of internet-using children aged 12-17 in Kenya. n = 1,014.

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

Kenyan legislation does not explicitly criminalise online sexual harassment of children. However, section 27 of the Computer Misuse and Cybercrimes Act makes 'cyber harassment' an offence. In view of the broad wording used, this provision could be invoked for sexual harassment of children online. Duty-bearer interviews with representatives from the Kenya Law Reform Commission also confirmed that the concept of online abuse referred to in subsection 20(3)(c) of the upcoming Children Bill 2021 will encompass cyber harassment and cyber bullying, among other phenomena.

Our household survey of 12-17-year-olds shows that in the past year, 21% internet-using children in Kenya have been exposed to sexual comments about them that made them feel uncomfortable, including jokes, stories or comments about their bodies, appearance or sexual activities. Older children aged 16-17 years were slightly more likely to be subjected to these comments (26% compared to 16% of 12-13-year-olds). There was no difference by gender. Among the 212 children who had been harassed in this way, more said they were harassed online – via social media and/or an online game – than in person (see page 61). Children aged 12-13 were more likely to be sexually harassed in person (40% compared to 30% of 16-17-year olds). And less likely than the oldest children to be harassed on social media (24% and 44% respectively). Boys were more likely than girls to be sexually harassed on social media (42% and 34%).

Among the 80 children who said they were last harassed on social media, the most common platforms cited were WhatsApp and Facebook or Facebook Messenger. Although Snapchat was only mentioned by 6% of this subgroup of children, it was one of the platforms on which children aged 12-13 were more likely to be exposed to sexual harassment compared to older respondents.

The most common offenders of verbal sexual harassment of children were a current or former romantic partner, a friend or acquaintance younger than 18 and an adult friend or acquaintance. Around one in four children said the offender was someone they did not know. The youngest respondents were most likely to receive these comments from a family member (24%) compared to 5% of 14-15-year-olds and 8% of 16-17-year-olds. Older children were more likely to be targeted by strangers (16-17: 31% vs. 12-13: 20%).

As with other forms of sexual violence, most children either told a friend or did not tell anyone at all the last time they were subjected to this kind of harassment. Among the 74 children who did not tell anyone the last time this happened to them, the most common barriers were not knowing where to go or whom to tell, and feeling embarrassed or ashamed or that it would be emotionally too difficult.

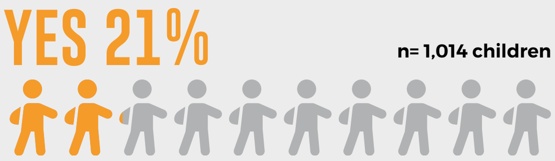
2.3.2 Receiving unwanted sexual images

Twenty percent of the children surveyed said that someone had sent them unwanted sexual images in the past year. This experience was more common among older children (26%) compared to the youngest age group (14%). There were no notable differences by gender. When these 200 children were asked about the last time they were sent these unwanted sexual images or videos, over half said they were targeted on social media. Fifty-nine per cent of children ages 14-15 and 16-17 received these unwanted images via social media, compared to 41% of 12-13-year-olds. The platforms most commonly mentioned by those 111 children targeted on social media were WhatsApp, Facebook or Facebook Messenger and YouTube, followed by Instagram (12%).

Children were most likely to receive unwanted sexual content from someone unknown to them, followed by an adult friend or acquaintance, a romantic partner (or ex-), and a friend or acquaintance younger than 18. The easily-abused anonymity provided by the internet could help to explain why unwanted sexual images are generally sent via social media and why the offender is someone unknown to the child in one-third of cases. The oldest children were most likely to say they most recently received unwanted sexual images from a stranger (12-13: 15%; 14-15: 35%; 16-17: 39%).

IN THE PAST YEAR

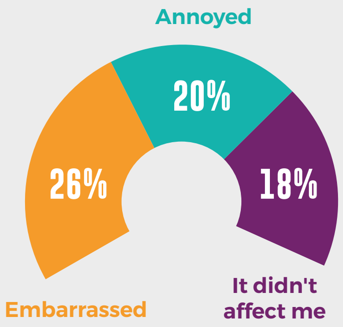
SOMEONE MADE SEXUAL COMMENTS ABOUT ME THAT MADE ME FEEL UNCOMFORTABLE



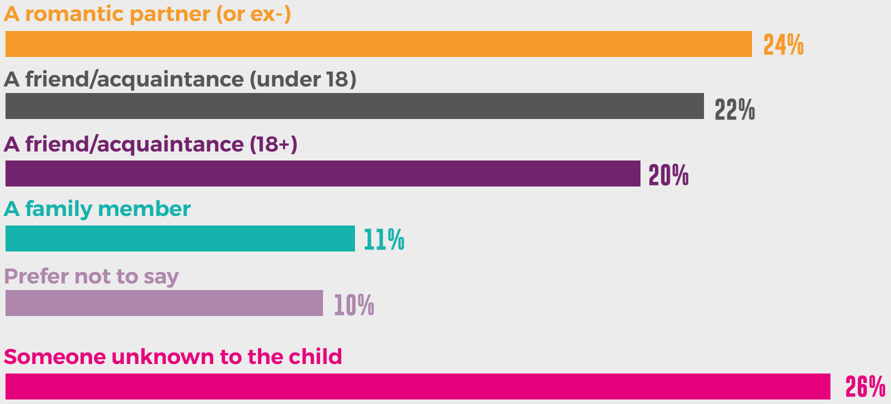
n= 1,014 children

THE LAST TIME THIS HAPPENED...

How did you feel?*

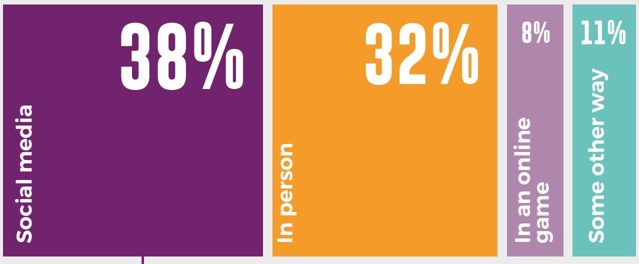


Who did it?*†



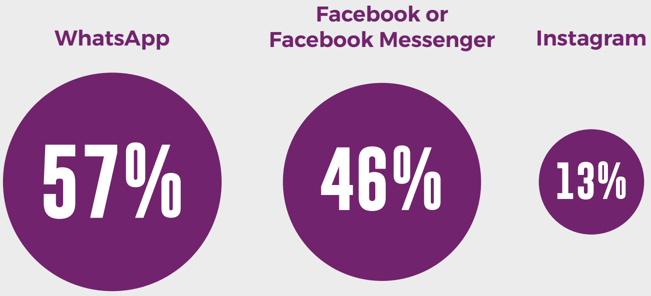
n= 212 internet-using children aged 12-17 who were subjected to verbal sexual harassment in the past year.

Where did it happen?*†



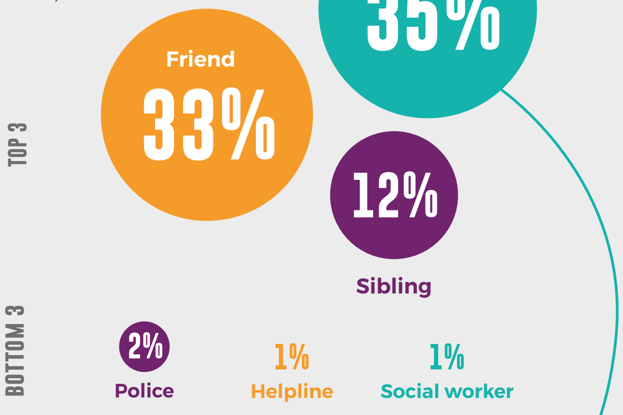
n= 212 internet-using children aged 12-17 who were subjected to verbal sexual harassment in the past year.

On which platform did this happen?*†



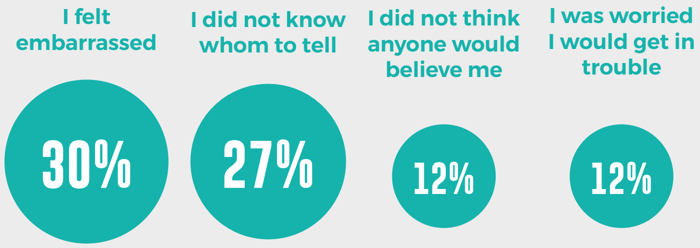
n= 80 internet-using children aged 12-17 who were *most recently* subjected to verbal sexual harassment *via social media*.

Whom did you tell?**†



n= 212 internet-using children aged 12-17 who were subjected to verbal sexual harassment in the past year.

Why did you not tell anyone?*†



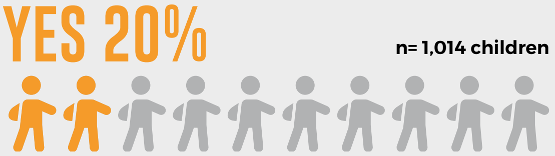
n= 74 internet-using children aged 12-17 who *did not tell anyone* the last time they were subjected to verbal sexual harassment.

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

Source: Disrupting Harm data

IN THE PAST YEAR

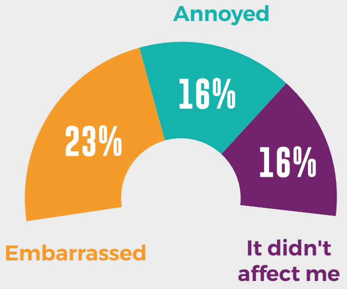
SOMEONE SENT ME SEXUAL IMAGES I DID NOT WANT



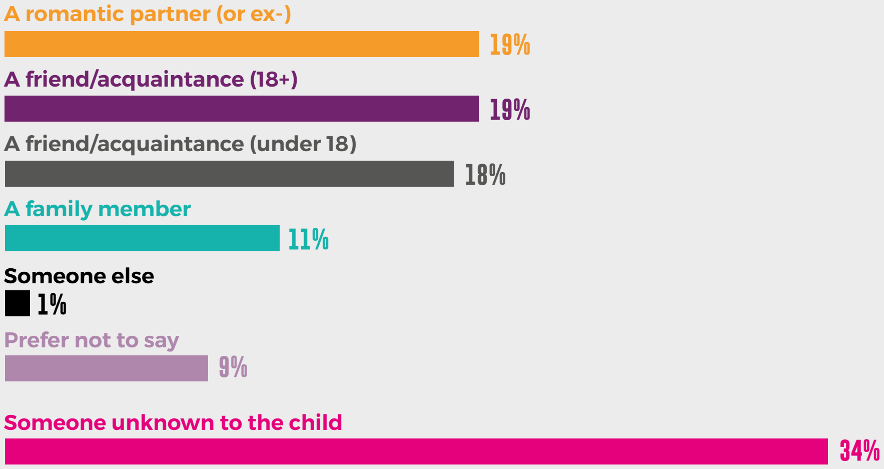
n= 1,014 children

THE LAST TIME THIS HAPPENED...

How did you feel?*

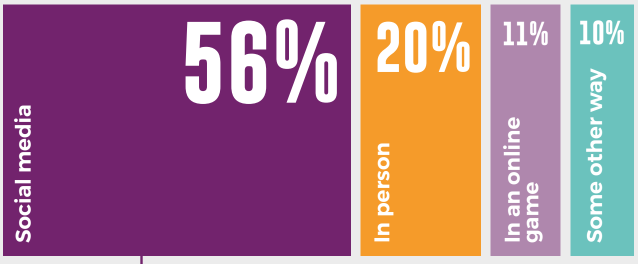


Who did it?*†



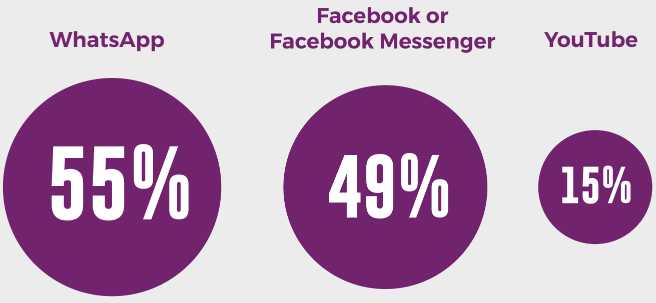
n= 200 internet-using children aged 12-17 who received unwanted sexual images in the past year.

Where did it happen?*†



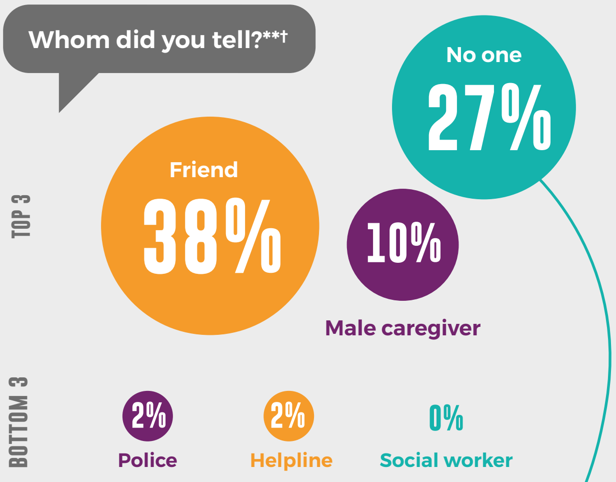
n= 200 internet-using children aged 12-17 who received unwanted sexual images in the past year.

On which platform did this happen?*†



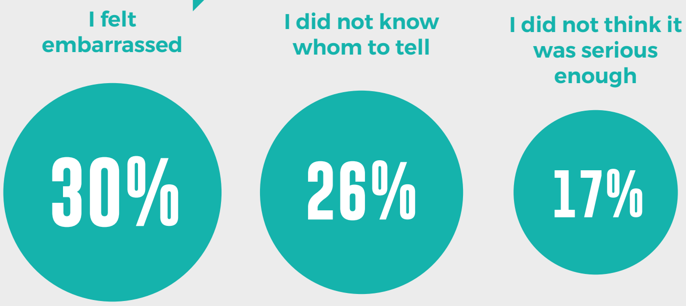
n= 111 internet-using children aged 12-17 who *most recently* received unwanted sexual images *via social media.*

Whom did you tell?**†



n= 200 internet-using children aged 12-17 who received unwanted sexual images in the past year.

Why did you not tell anyone?*†



n= 54 internet-using children aged 12-17 who *did not tell anyone* the last time they received unwanted sexual images.

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

Source: Disrupting Harm data

As shown on page 62, over one in four children who received unwanted sexual images did not tell anyone the last time this happened to them and 38% turned to a friend for support. Eight children told a teacher. Few respondents turned to formal reporting mechanisms such as helplines or the police. Among the 54 children who did not tell anyone, the main reason was that they felt embarrassed or ashamed or that it would be emotionally difficult to tell. The second most common response was that they did not know where to go or whom to tell, followed by the belief that what happened to them was not serious enough to report. Some also said that they did not think anyone would believe or understand them (15%), or were worried they would get into trouble (11%).

The Continuum of Online and Offline Child Sexual Exploitation and Abuse

Case Study – Child Trafficking and Defilement[98]

In March 2020, a suspect travelled to Kisumu where he rented a house. On 4 May 2020, detectives from the AHTCPU in Nairobi, acting on intelligence, arrested the 71-year-old male European national and rescued one minor aged 14 years in Nairobi. The suspect led the officers to a guest house in Nairobi where he had been lodging with the minor since their arrival from Kisumu in April 2020. The suspect travelled by a public vehicle and *bodaboda* (motorcycles) to manoeuvre through the police road blocks mounted during the Covid-19 lockdown of Nairobi City. He was prosecuted in a Nairobi law court, in May 2020 on charges of child trafficking and defilement.

It turned out that the suspect had first come to Kenya in 2012 and stayed in the Coast region. With the assistance of INTERPOL, police established that he had been incarcerated for drug trafficking in South Korea in 2013 and served five years there before he returned to the Kenyan Coast in 2018. He informed police that he produced CSAM for commercial trading via Facebook. He had six local mobile phone numbers which he used for financial transactions and networking but none of the phones was registered in his name. He claimed that his intention of travelling with the minor to Malindi was to sponsor his education because the boy came from a low-income family.

The victim told police that the suspect had promised to give him 500 Kenyan shillings if he allowed him to touch him and keep the matter secret. The boy also received a cell phone from the suspect, who would buy him airtime and data bundles, which the suspect would then use to download *"pornographic"* materials. The boy informed police that he and two other boys who were his friends, had got to know the suspect at a neighbourhood shopping centre in Kisumu and had frequently visited the suspect's house to watch TV and play video games. He told police that the suspect used to touch them and they would watch *"adult things"* [pornographic videos] on the phone.

The suspect is currently remanded in a prison in Nairobi. The case is pending before court. For the other two victims, the case is pending under investigation.

The types of sexual exploitation and abuse of children presented throughout this chapter illustrate some of the ways that digital technologies can be used to harm children. However, our findings – including the case study presented above – also reveal that creating a distinction between online and offline violence does not always reflect the reality of children's

Continued...

[98] The term "defilement" is the legal terminology in Kenya for penetrative acts with a child, and while outdated, is also used in common parlance. "A person who commits an act which causes penetration with a child is guilty of an offence termed defilement" Sexual Offences Act, No. 3 (2006) (Kenya) 8(1)

experiences. For example, children can be asked or coerced to share self-generated sexual images, and this can happen online, offline, or in both spaces. In addition, digital technologies can also be used as a *facilitator* of sexual exploitation and abuse. For example, social media or instant messaging can be used to convince or coerce children to meet offenders in person, leading to 'offline' child sexual exploitation and abuse. The data in this report include OCSEA that takes place in the online environment, OCSEA that takes place offline but is facilitated by digital technology, and OCSEA that is committed 'offline' and then repeated by sharing it online.

Interviews with various stakeholders show that systems are not fully adjusted to this reality, and that OCSEA is sometimes perceived as a 'new kind of abuse' that requires an entirely different response. However, as one respondent summarised, *"The channel [the internet] is just the variable; abuse is still the same."* (RA3-KY-10-A) The same respondent explained that *"People do not understand the online environment; they think it is harmless to discuss certain things online as opposed to physically touching someone."* (RA3-KY-10-A) Another interviewee, from the International Justice Mission, recalled that *"In all the years we worked in that field, we didn't have an outright case of online abuse standing alone. It had to have a component of contact or offline abuse, so that should just tell you about the landscape in Kenya in terms of just appreciating that online abuse even without contact is still abuse."* (RA4-KY-05-A-justice)

In line with this, our data clearly show that only a small proportion of children experience exclusively OCSEA; almost all children who had experienced OCSEA in our sample had also experienced an instance of in-person sexual, physical or emotional abuse in the past year. This could indicate that OCSEA is an extension of existing abuse already experienced by the child, or that there are a common set of vulnerabilities that make children who experience violence 'offline' more likely to also experience violence 'online'.

The Department of Children's Services and the UNICEF Kenya Country Office both indicated that responses to OCSEA are and should continue to be embedded within the broader child protection framework and not handled in a silo. This means enabling OCSEA victims to benefit from the same services that exist for other child victims of violence. In addition, OCSEA should be included within *existing coordination mechanisms* for violence against children: *"For the Department of Children's Services, we look at OCSEA from the broader perspective of child protection, maybe within sexual exploitation. We do not want it to be in a silo"* (RA1-KY-08-A); *"OCSEA should be part of the regular work on violence against children and the regular child protection coordination mechanism"* (RA1-KY-01-B)

Despite this important consensus, there remains a lack of clarity around the responsibilities of various agencies in addressing cases of child exploitation and abuse with an online element. Furthermore, there are cases where online abuse requires a specialised response, for example in law enforcement investigations involving the use of digital forensics. In other instances, a lack of clear laws around OCSEA make it difficult for law enforcement to act and for children to obtain justice through courts. A former counsellor at Childline Kenya also recalled that *"After finding out the case is an OCSEA case, we would sit in a case conference and the office of public prosecution would be represented. In regard to charging the offence, he would advise we continue pursuing it as truancy or defilement or sexual abuse or early marriage but specifically OCSEA, no. The explanation we got from public prosecution is that the case could not be taken to court as OCSEA because there is no policy on it."* (RA4-KY-06-A-justice)

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

2.4.1 Victims

Beyond household survey data which gives an indication of who the OCSEA victims are, very little quantitative data was identified by the *Disrupting Harm* team. One identified source was Child Helpline International data – reported by Childline Kenya. These data showed that of the 16 contacts concerning CSAM that they received in 2018, five related to exposure to adult pornography,[99] three to online sexual exploitation of a boy, and the remaining eight to online sexual exploitation of girls. In 2019, 189 contacts for online child sexual exploitation for Kenya were recorded[100] – 100 contacts for girls and 89 for boys.

There were no data available from law enforcement quantifying victims and offenders that was specific to OCSEA offences in Kenya. While offline CSEA is not the focus of this report, data on offline offending is included here as a reflection of possible unreported or unrecognised OCSEA offending. Other areas of the report or case studies describe how victims and offenders may meet in person but correspond online, or meet initially online and then meet in person. Data on offline offending may thus provide context in which online offending may occur, or may already be occurring.

The AHTCPU had 79 offline CSEA cases in its caseload between 2017-2019. The majority (72%) of offline CSEA victims for whom age was stated (n=76) were aged 13 or over. In terms of gender, 91% of those for whom age was stated (n=78) were female. All victims in the national specialist unit's offline CSEA caseload were Kenyan nationals. As mentioned above, these data represent only those cases investigated by the national specialist law enforcement unit, and does not reflect all CSEA cases recorded by police in Kenya.

2.4.2 Offenders

Again, very little data about the profile of offenders was able to be identified. One indication came from the frontline workers' survey where respondents described the most common relationships between offenders and children in the OCSEA cases that they worked with were community members over the age of 18, followed by strangers (nationals), other relatives over 18, parent/step-parent, family friend and community member under 18. More than half of the frontline workers (29 out of 50) said that men were most commonly identified as offenders and facilitators of OCSEA in the cases that they were seeing.

Facilitators[101] were reported most often to be members of the community over 18, followed by strangers (nationals) and other relatives over 18: *"I have encountered cases of OCSEA by biological father, step father, teacher and rescue home/shelter manager and caregiver"* (RA3-KY-29-A). These data from frontline social support workers seem to contradict the commonly held assumptions of foreigner offenders of OCSEA.

In the AHTCPU data about offline CSEA, individuals in the 18-29 age group made up the largest proportion (48%) of the offenders for whom age was stated in data from the national specialist unit's caseload (n=79). One offline CSEA offender in the reporting period was identified as under 18. The majority (91%, n=72) of offline CSEA offenders investigated by the AHTCPU were adult family friends of their victim(s); a further seven offenders were family members. Three offenders investigated by the AHTCPU during the reporting period were foreign nationals. Just one offender was female.

[99] This categorisation of the data was provided by Child Helpline International. It is assumed that this was purposeful exposure of a child to pornography by an adult.
[100] In 2019, Child Helpline International adopted a new definition of online child sexual exploitation for their data. Prior to this only cases involving CSAM were captured in their metrics.
[101] 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')."

2.5 BARRIERS TO CHILDREN SPEAKING TO ADULTS ABOUT OCSEA

Children in Kenya broadly feel that they can depend on strong interpersonal networks. In our household survey, 82% of children said it was 'fairly' or 'very' true that there is at least one teacher they can go to if they have a problem. As many as 94% of children agreed or strongly agreed that members of their families will help them if they have a problem. In spite of this, as seen in the previous chapters, about one-third of children subjected to OCSEA never tell anyone, and those who do so are most likely to confide in friends. Only a small proportion of children mention it to their caregivers and even fewer turn to formal reporting mechanisms like helplines or the police. This is true of all the forms of OCSEA explored through the household survey.

2.5.1 Four reasons for not telling

Data from our household survey, access to justice interviews with children, survey of frontline workers and interviews with government duty-bearers all indicate that children in Kenya might not report OCSEA due to:

Lack of awareness of OCSEA: Children are not taught what OCSEA is and might not perceive OCSEA acts as criminal. According to our findings from the household survey, 53% of internet-using children have received sex education and 33% received information on how to stay safe online. Information about OCSEA could be integrated into these activities, which need to reach all children.

The lack of awareness of many children about OCSEA also reflects a wider lack of awareness in society. According to the caregiver of a child who has been through the process of accessing justice: *"More awareness needs to be created on the online sexual exploitation for children, caregivers and legal officers because it is real and people are afraid to report the cases."* (RA4-KY-05-B-caregiver)

Lack of knowledge of reporting mechanisms: One of the most common barriers to the reporting of OCSEA mentioned by the children in our household survey was not knowing where to go or whom to tell. This may indicate both hesitation about whom to tell and insufficient familiarity with reporting mechanisms including helplines, the police and the social media platforms they use.

A former officer from ChildLine Kenya commented: *"Our reporting protocols are not clear when it comes to online abuse in general. The way you know when you are sexually abused you can just call 116, you can report to the children's officer in the sub-county or you are going to report to the police station gender desk, when it comes to matters online, it's really not clear where and how you're going to report. That is a challenge to children and the public."* (RA4-KY-04-A-justice) (click here to read more about the issue of distinguishing between online and offline abuse in investigations).

Almost all of the survivors we spoke to during access to justice interviews and survivor conversations in Kenya said that they only spoke to the police after being helped by others to reach that decision.

Fear of repercussions: One frontline worker indicated that fears of being denied access to the internet and social media, as well as stigmatisation (see below), might lead children to avoid reporting abuse: *"Factors such as stigmatisation make children shy away from sharing their experiences especially when it comes to online abuse. Technology is presumed to be fashionable hence catching up with technology is the dream of everyone and therefore it will be difficult for a child to share [concerns] since he/she might fear that he/she will be denied access"* (RA3-KY-19-A)

Such fears may be well founded, as 31% of the caregivers in our survey said that they would restrict a child's internet use if they knew that the child had experienced something that bothered or upset them online.

Shame, stigma and victim-blaming: According to our household survey of children in Kenya aged 12-17, feelings of embarrassment or shame stopped them from talking to others about their OCSEA experiences. They say it would be emotionally too difficult to speak out, worry about getting into trouble, or feel that no one would believe them or understand their situation.

Social and cultural barriers to disclosing OCSEA in Kenya

The fact that many children subjected to OCSEA do not tell anyone, particularly an adult, can be attributed in part to taboos and stigma around sexual experiences. In fact, 31 of the 50 frontline social service providers we surveyed believed that stigma from the community influences the reporting of OCSEA in Kenya. Likewise, 60% believed that taboos around discussing sex and sexuality influence the reporting of OCSEA. According to one frontline worker:

> *"My society finds it challenging to transition children into adults through building their confidence and esteem to communicate on matters of sexuality or abuse. A child is expected to be shy as a sign of respect so speaking out becomes a concern."*
> (RA3-KY-04-A)

In other research, women in East and Central Africa report that disclosure could reduce their marriage prospects and result in stigmatisation by family and community members, which could be another reason for not telling anyone about such experiences.[102]

One parent of a child who had reported and gone through the justice process said that their child struggled to: *"digest the whole defilement[103] ordeal. It was very traumatising at first because she was blaming herself and because she was questioning herself and what other people might say, she was questioning her integrity and she didn't know what the future would look like. She was afraid that people would laugh at her, so she was I don't know if I can say apprehensive, she was confused in the beginning because of her morality now that she had been defiled. So that was a very difficult period for her, but she was counselled, and she has been able to overcome those issues."* (RA4-KY-10-B-caregiver)

Continued...

[102] Boudreau, C. L., Kress, H., Rochat, R. W., & Yount, K. M. (2018). Correlates of disclosure of sexual violence among Kenyan youth. Child Abuse & Neglect, 79, 164–172.
[103] The term 'defilement' is the legal terminology for sexual assault in Kenya and used in common parlance.

Under-detection and under-reporting of male child sexual exploitation and abuse is a global problem, due to a range of social and legal implications.[104] One reason is that a child abused by an offender of the same-sex may have difficulty reporting the offence due to the stigma associated with homosexuality.[105] Norms about masculinity and fear of being viewed as a homosexual have been identified as common reasons for the non-disclosure of sexual abuse by boys in Kenya.[106] Moreover, *"unnatural intercourse"* remains a crime under the Kenyan Penal Code, [107,108] and this may affect the protection accorded to children aged 12-17 years sexually exploited by an offender of the same-sex. These children may fear legal consequences if they report the case. When sampling children who had accessed the justice system to interview them for *Disrupting Harm*, we were unable to identify a single male child victim, even though our survey data clearly shows that boys experience OCSEA to a similar degree as girls. This suggests that boys may not feel safe to report.

2.5.2 Why children subjected to OCSEA hesitated to disclose

The stories of children subjected to OCSEA captured in our survivor conversations in Kenya graphically illustrate how the above factors combine to block or delay the reporting of OCSEA offences.

- None of the nine Kenyan girls who we talked to in our survivor conversations reported the requests they received for sexual chat or face-to-face meetings to the social media platforms they were using – perhaps partly because they did not grasp the malign intent of the person they were talking to: *"He always said nice things to me and I ended up trusting him so much and I thought he wouldn't harm me, and that's why I am still wondering why he would do this to me and after the incident, I couldn't find him online anymore, maybe he had blocked me and we never spoke again."* (RA5-KY-01-A)
- The girls also reported feeling ashamed and that they had let themselves and others down: *"I did not go straight home because I did not know how I could explain that to my mother, since she had warned me against using phones... That I was underage."* (RA5-KY-09-A)
- As time passed, it became difficult to say anything: *"I didn't tell her because I felt she would be so hurt and blame me and reprimand me for not reporting it earlier."* (RA5-KY-02-A)
- Some of the children also expressed a fear that disclosure would cause a rupture in their relationships: *"I would just tell my mum and she would fix it for me but when this incident happened, I didn't want to embarrass her. She is my mother and she has raised me and provided everything I needed. I didn't want to make her feel bad, why would I tell her and spoil everything we had?"* (RA5-KY-01-A)
- There was also an explicit need for the children to protect themselves from others. As one of them explained: *"It was kind of hard because I didn't want people to judge me because nowadays not everyone is willing to help; they will just listen to your story and spread it all over and since I was in high school brutal because you can trust a friend and you know this one is a friend and then after listening they would go and spread it so I just felt it was better to keep it to myself..."* (RA5-KY-02-A) However, this young person did confide in her teacher's daughter, who then shared the information with the teacher.

[104] Josenhans, V., Kavenagh, M., Smith, S., & Wekerle, C. (2019). Gender, rights and responsibilities: The need for a global analysis of the sexual exploitation of boys. Child Abuse & Neglect, 110, 4.
[105] Ibid., 6.
[106] Boudreau, C. L., Kress, H., Rochat, R. W., & Yount, K. M. (2018). Correlates of disclosure of sexual violence among Kenyan youth. Child Abuse & Neglect, 79, 164–172.
[107] Republic of Kenya. (1930). The Penal Code of Kenya (Cap. 63) (Rev. 2012). Section 162.
[108] Human Rights Watch. (2019). Kenya: Court Upholds Archaic Anti-Homosexuality Laws.

- When disclosures were made about the abuse it was often to organisations outside the family: *"Here I have written got help from someone… from Love and Hope… it gave me a new beginning and a chance to open up…"* (RA5-KY-01-A) – or to someone known within the community: *"So I went to a counsellor in our neighbourhood who advises girls."* (RA5-KY-09-A)
- Of the nine children who took part in the survivor conversations, four became pregnant as a result of the sexual assault, which forced the disclosure of at least some of what had happened. Mothers in particular were seen as supportive: *"When I realised I was pregnant I told my mother. She did not judge me; she decided to stand by me. My parent surprisingly accepted me."* (RA5-KY-07-A) This included providing care for the baby: *"… And when I was pregnant I told her about it and she convinced me to keep it and assured me I could count on her and that was a huge weight off my shoulder. I cried because I didn't think she would react like that."* (RA5-KY-04-A)

> "When sampling children who had accessed the justice system to interview them for *Disrupting Harm*, we were unable to identify a single male child victim, even though our survey data clearly shows that boys experience OCSEA to a similar degree as girls."

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

This chapter presents evidence about current Kenyan response mechanisms. This includes formal reporting options, and responses by police and the court system. Finally, it considers the contributions which government, civil society and the internet and technology industry make to combating OCSEA in Kenya. Much of the data is drawn from qualitative interviews with government, law enforcement, court professionals and children and caregivers who accessed the formal justice system. Responses may not reflect the full range of experiences of those accessing the Kenyan response mechanisms to OCSEA.

3.1 FORMAL REPORTING MECHANISMS

As seen in the previous chapter, few children report cases of OCSEA to formal reporting mechanisms like the police or helplines.

In our household survey of 1,014 caregivers, 63% said that they would tell the police if their child was subjected to sexual harassment, abuse or exploitation. Others said they would not report the incident due to concerns about negative consequences, fear of not being treated properly and/or the belief that reporting would have no effect.

In our survey of 50 frontline workers, 29 said that they believed OCSEA cases are not being reported because services are not trusted.

The ability to recognise OCSEA and knowledge about how to report may also affect the level of reporting. *"Currently, there is little awareness among the public on OCSEA and how to report it" said the head of the Children Division and Anti-Female Genital Mutilation Unit of the Office of the Director of Public Prosecutions, in one of our duty-bearer interviews. "There is therefore a need to sensitise the public so they can be reporting these emerging cases."* (RA1-KY-07-A)

The main channels through which children and adults can report cases of OCSEA are the Childline Kenya 116 helpline, civil society organisations, the police, and the online reporting portal of the National Kenya Computer Incident Response Team Coordination Centre, which aims to counter internet crime including CSAM offences.

Child hotlines and helplines

There are several channels through which children and adults can report cases of OCSEA. These include child hotlines and the one child helpline. OCSEA hotlines focus on working with industry and law enforcement agencies to take down content, they often now use web-based formats rather than phone numbers. While some child helplines may specifically focus on online child sexual exploitation and abuse, they generally tend to respond to a broader range of child protection concerns. Some might provide immediate crisis support, some referral and sometimes ongoing counselling and case management services.

3.1.1 Childline Kenya 116 and civil society organisations

Childline Kenya was founded as an NGO by Plan International, SOS Children's Villages and the Kenya Alliance for the Advancement of Children. Established in 2006, it is the only dedicated 24/7 toll-free phone helpline, online chat and SMS service for children to report abuse and other issues of concern. Childline Kenya is a member of Child Helpline International and operates in partnership with the Department of Children's Services, in close cooperation with the Directorate of Criminal Investigations and AHTCPU.

Duty-bearers and frontline workers interviewed or surveyed for *Disrupting Harm* considered Childline Kenya 116 to be a critical stakeholder in the response to OCSEA. The helpline did not receive any reports in 2017. However there has been a big increase between 2018 and 2019 (16 and 189 cases, respectively).[109] In 2019, OCSEA cases accounted for 78% of reported CSEA. In comparison, OCSEA cases made up only 2% of total contacts received by the hotline that year.[110] Eighty-six per cent of calls to Childline Kenya were information enquiries related to issues such as child maintenance.

A representative of the Communications Authority of Kenya indicated that Childline Kenya lacks financial and human resources to adequately respond to OCSEA: *"Concerning support of child victims, the Child Helpline does this but they are severely incapacitated and don't have sufficient personnel to tackle this issue [OCSEA] which is time-consuming. The work they do is commendable, but the government needs to offer the strategic commitment that would strengthen their role both from a reporting perspective and from the perspective of providing psychosocial support to victims."* (RA1-KY-03-A)

3.1.2 Law enforcement

Reports of OCSEA can be made at any police station. In addition, Kenya has the specialised AHTCP unit in Nairobi, mandated to respond to OCSEA cases.[111] A second Unit has also been established in Mombasa and a third is planned for Kisumu.[112] These Units are a product of close partnership efforts between Kenya and other international law enforcement agencies. A total of 27 police officers serve in the two existing units but only a total of five are dedicated to investigating OCSEA cases.

According to interviews with representatives from the AHTCPU (RA8-KY-01), OCSEA cases are reported to them by:

- members of the public
- civil society organisations
- children's officers from the Department of Children's Services
- the National Kenya Computer Incident Response Team Coordination Centre
- the Directorate of Criminal Investigation cybercrime unit
- regular police stations
- NCMEC
- the INTERPOL National Central Bureau.

National Kenya Computer Incident Response Team Coordination Centre

The National Kenya Computer Incident Response Team (KE-CIRT) is the core agency mandated to remove or take down harmful content reported to it by the general public and public institutions and agencies. Its coordination centre has an online Child-Related Cyber Incident Reporting system,[113] an email address and two dedicated hotline numbers for reporting internet material suspected of being illegal.

[109] 2017 data submission confirmed by Child Helpline International, November 2020.

[110] These percentages have been calculated using statistics provided by Childline Kenya and Child Helpline International. For 2018, cases of 'child prostitution' and 'sexual abuse' were combined to calculate the number of CSEA cases. For 2019, cases of 'sexual abuse', 'child prostitution', 'sexual abuse (sodomy)' and 'sexual abuse (incest)' were taken into account. Other categories that might be relevant in some cases (such as child marriage or female genital mutilation) were consciously excluded to provide the closest possible figures for explicit (rather than potential) offline CSEA.

[111] See: National Police Service Directorate of Criminal Investigations: Anti-Human Trafficking and Child Protection Unit.

[112] Both AHTCPU units are well equipped with relevant tools for investigation of OCSEA, including Celebrite, mobile forensic laboratories and internet connections. While the AHTCPU in Nairobi conducts preliminary investigation through triage of seized OCSEA gadgets using Celebrite for the rapid identification of victims and evidence to assist in the immediate judicial outcome, the unit has no certified forensic experts and relies on expertise from the Cybercrime Unit at the DCI Headquarters for detailed analysis and written expert's opinions for purposes of prosecution (RA8, INTERPOL). Further, Kenya lacks a national image database on OCSEA. This is understood to have been discussed by the Technical Working Group on Child Online Protection (see Chapter 3). The existing Child Protection Information Management System under the Department of Children's Services does not currently capture data on OCSEA.

[113] See: Child Related Cyber Incident Reporting Form.

This Team does not undertake criminal investigations of CSAM cases itself but refers them to the AHTCPU. In our duty-bearer interviews, a Team official explained: *"When we receive cases, the initial investigation – triaging – is done by the Kenya Computer Incident Response Team to determine what direction will serve the best interest of the child. If it is counselling, that is a decision that can be made and we direct the case to a pool of counsellors; if it's the criminal investigations, we will liaise with our sister agency which is the AHTCPU to run with the investigations. We continue providing technical support for them to finalise the investigations."* (RA1-KY-11-A)

According to one professional working with children, *"The portal for the Communication Authority of Kenya is not very user friendly. I have used it a couple of times. It takes you round and round and round. If it's urgent stuff, it's very difficult for you to report."* (RA4-KY-02-A-justice) After the *Disrupting Harm* interviews were conducted, the system, seems to have undergone some improvements. For example, a 'Child-Related Cyber Incident Reporting Form' has been added on the reporting portal.

Quantitative data on the number of reports to the KE-CIRT were not available at the time of writing.

3.1.3 Views on reporting to law enforcement agencies

The Directorate of Criminal Investigations website[114] states that reports can be made directly to the AHTCPU through the local offices of the Directorate of Criminal Investigation. However, even public officials and professionals acknowledge that reporting to the Unit is not straightforward:

- *"I would say there is a challenge on how to reach out to this particular agency. We need a number. I cannot just be raising awareness and saying, 'Go talk to the AHTCPU'. Sometimes it's not so simple if you are in Mandera [a county in Kenya], you know, you need a way. That's a lapse in terms of reporting,"* said an interviewee from the justice sector. (RA4-KY-03-A)
- The Principal Children's Officer from the Department of Children's Services added: *"If you want to report to the AHTCPU, you have to call an individual you know within that unit, and tell them there is this case, then that person passes it on. It should not be like that. Suppose you don't know any individual who is working there, does that mean the case will go unreported?"* (RA1-KY-08-A)

The Head of the AHTCPU confirmed that reporting has been a challenge: *"Reporting is something that we have been working on as it has been a challenge. We have got an email address, and then we use the Directorate of Criminal Investigations as well as 116. But there is no number."* (RA4-KY-08-B-justice)

Despite these problems, a representative of the Watoto Watch Network gave an example of a successful referral: *"There was a case where a man was having sexual intercourse with a minor and he was recording it. He recorded it and posted it on Facebook so there was public outcry. We got the report and we did our diligence and reported to the AHTCPU and it was taken down immediately and that particular man was actually arrested. This is an example of a case we reported, action was taken immediately and we got to know the person was arrested and the case is in court."* (RA4-KY-03-A-justice)

One of the justice professionals interviewed for *Disrupting Harm* said that civil society organisations working on matters of child online protection have good working relationships with law enforcement agencies. This working relationship facilitates flagging of OCSEA cases both for investigation and for the quick take-down of CSAM. (RA4-KY-02-A-justice)

> **Reporting is something that we have been working on as it has been a challenge.**

[114] See: National Police Service Directorate of Criminal Investigations. (The website also provides links to Childline Kenya and the police toll-free hotline 112).

Moreover, thirty-five of the 50 frontline workers whom we surveyed indicated that at least one case of OCSEA which they had managed directly within the past one year resulted in a complaint filed to the local police/judicial authorities.

Nevertheless, there appears to be a need to clarify procedures for reporting directly to the AHTCPU and to make it more accessible for organisations working on OCSEA and the general public. In addition, civil society organisations and the general public may not be well informed about the roles of different agencies. In the words of a justice professional dealing with OCSEA cases, *"I think there needs to be clarity between the two agencies – the AHTCPU and the National Computer Incident Response Team. They are both government agencies but we need to understand exactly what we need to tell the public during awareness raising sessions about the category of cases to report to which agency. Right now, it's confusing."* (RA4-KY-03-A-justice)

Our interviews with representatives of civil society organisations that support the reporting of OCSEA cases point to a need to establish appropriate mechanisms for sharing evidence. Currently, some civil society organisations share evidence (CSAM images/videos) with law enforcement authorities through informal mechanisms such as WhatsApp groups. While done with good intentions, this is illegal as it contributes to the circulation of CSAM.

3.1.4 International reporting

As seen in Chapter 2, NCMEC received 16,108 reports for Kenya in 2018 and 12,788 in 2019. The vast majority are reports from technology companies. The Nairobi office of the AHTCPU is responsible for receiving these reports, which are disseminated daily.

On 27 January 2021, the AHTCPU and the Internet Watch Foundation launched a dedicated online portal for law enforcement authorities in Kenya to report cases of OCSEA.[115] Internet Watch Foundation analysts in the United Kingdom will assess reported CSAM and block and remove it from the internet if necessary.

> **"The new dedicated online portal for reporting OCSEA, launched in 2021 by the AHTCPU, will improve Kenya's OCSEA investigation collaboration through connections to other hotlines via the INHOPE network."**

At the regional level, KE-CIRT collaborates with its East African peers under the East African Communications Organization Cybersecurity Working Group, which is chaired by Kenya.[116] On the global level, it works with the International Telecommunication Union and various national computer incident response teams.

KE-CIRT does not focus solely on OCSEA, but addresses all kinds of cyber-crimes. This may affect its cooperation with hotlines around the world. The new dedicated online portal for reporting OCSEA, launched in 2021 by the AHTCPU, will improve Kenya's OCSEA investigation collaboration through connections to other hotlines via the INHOPE network. It will be important for KE-CIRT and the AHTCPU to work together in this context.

[115] Internet Watch Foundation. (2021). Kenyan reporting portal to play 'huge role' in improving global internet safety.
[116] See: National KE-CIRT/CC: Partners.

3.2 LAW ENFORCEMENT RESPONSE

3.2.1 The law enforcers

The AHTCPU and regular police stations are mandated to investigate the OCSEA cases reported to them. Regular police units may refer cases of OCSEA to the specialist unit, but they are not obliged to do so. Moreover, many police officers may not be aware of the unit's existence. On the other hand, the AHTCPU has the authority to take over OCSEA cases from regular police stations for further investigation.

AHTCPU: Duty-bearers and justice professionals interviewed for *Disrupting Harm* regard the establishment of this unit as a great success – not least because it has catalysed action in other mandated government agencies, including the Department of Children's Services and the Office of the Director of Public Prosecutions, which now have officers dedicated and trained in handling OCSEA related cases.

As the Principal Children's Officer from the Department of Children's Services explained: *"The AHTCPU is a victim-centred unit, so whenever an OCSEA case is reported, we [the Department of Children's Services and the Anti-Trafficking Unit] sit down together, to know where the location of this case is. If it's somewhere nearby we go there, if it's somewhere outside of Nairobi, then I get in touch with our officers there, then the investigators from the unit travel there for investigations purposes. When we get to our officers on the ground, if it's a case of rescue, we rescue even before the investigators go down there, because the safety of the child is paramount, and we start providing the support that is needed by the child. We also try to get in touch with the family, because it's not just about the investigation, it's the whole spectrum of psychosocial support."* (RA1-KY-08-A)

International Cooperation on Law Enforcement

- Through the AHTCPU, Kenya has become the first country in East Africa to be connected directly to **NCMEC's** CyberTip line, and **INTERPOL's** International Child Sexual Exploitation Database. At the time of writing, however, Kenya is not actively using the database due to the termination of the internet service provision in the Unit.
- According to a professional from the International Justice Mission Kenya field office: *"For detection and reporting to improve then we must collaborate with international law enforcement like now what we are doing with INTERPOL. For example, how we worked in the Simon Harris case. If it were not for UK law enforcement, we would have never achieved convictions for these cases as we didn't have the pictures, but the pictures were found in the UK and we were only able to identify the abuse through that collaboration."* (RA4-KY-05-A-justice)
- Kenyan law enforcement has also been cooperating with **embassy law enforcement liaison officers** to arrest offenders: *"there was a case of a German who was arrested the other day. We had already heard that he had been abusing children in Kwale. The German Embassy informed us that the man had applied for a passport and he would definitely be going for it (...) When he went to collect his passport, he was arrested."* (RA1-KY-08-A)
- Several **international organisations** including UNODC and UNICEF, the United States Department of Homeland Security, the UK National Crime Agency and the British High Commission in Kenya have provided Kenya with mentorship, training, and equipment including the forensic mobile laboratory, vehicles, computers and desks. (RA8-KY-01)

In addition to its role in investigating OCSEA cases, the Unit can advise regular police stations and provides training to professionals on handling cases of OCSEA. In the words of one frontline worker, *"The Directorate of Criminal Investigations Child Protection Unit in my country are doing quite a lot in regard to OCSEA and they have been in the frontline creating awareness and responding to issues of OCSEA."* (RA3-KY-17-A)

Regular police stations: There are currently five officers dedicated to the investigation of OCSEA cases in Nairobi's AHTCPU. Accordingly, most cases are likely handled by regular police stations. Some regular police stations have specialised child protection units with trained personnel, but this is not the norm.

Our interviews highlighted several challenges for investigations by regular police stations:

- **Police officers might lack awareness of OCSEA.** A respondent from the Department of Children's Services noted that *"A person or a guardian may go to a children's officer, and what they report as the presenting case, unless you probe deeper, you might not know that is a case of OCSEA. (...) We therefore need to empower our officers, our staff, even the police, everyone at the grassroots how can they identify a case of OCSEA."* (RA1-KY-08-A) *"People do not consider digital crime as a crime like physical crimes, so if you say a child has been abused online, you find a policeman will not see the damage,"* said the Chief Executive Officer of the Kenya Film and Classification Board. (RA1-KY-06-A) Seventy-eight percent of the frontline workers surveyed rated the awareness of law enforcement officers as fair or poor, and 84% their response to OCSEA, as 'poor' or 'fair'. *"Generally awareness of OCSEA as an important issue of concern is low among people including law enforcers,"* (RA3-KY-03-A) commented one of the frontline workers.
- **Police officers may be insufficiently aware of the law on OCSEA.** According to one Court of Appeals judge, *"We are not short of laws [but] we have a very serious knowledge gap (...) OCSEA, because of its insidious nature, may not be obvious to a local police officer, an investigator, a prosecutor, a magistrate, and even to the victims themselves."* (RA1-KY-04-A) A professional with experience in OCSEA cases suggested that police officers hesitate to institute criminal proceedings in cases where there is no element of in-person, contact abuse (RA4-KY-05-A-justice). The fact that some forms of OCSEA are not explicitly covered by law (click here to read an overview of legislation and policy) may also be a factor here. A former legal officer from Childline Kenya told us some police are not clear on how to categorise this: *"so they were asking, 'You Madam, charge sheet itakaa namna gani?' (Madam, what will the charge sheet look like?) (...) What is the area of law?"* (RA4-KY-01-A-justice) In contrast, the AHTCPU works closely with the prosecutor's office to charge OCSEA cases correctly, using the available laws. As a representative from the Department of Children's Services said in our duty-bearer interviews: *"At the [AHTCPU] we have a designated prosecutor, so when an OCSEA case is reported, the police investigators and the prosecutor will sit and discuss the case. It makes it so easy as opposed to when the police come up with whatever charges and we are told this is not how the charge sheet should read. So, there is a prosecutor who drafts the charges so that we avoid the back and forth of the court."* (RA4-KY-11-A-justice).
- **Police officers might lack technical knowledge on how to handle cases of OCSEA.** An AHTCPU investigator said, *"You find that police stations try to handle an OCSEA case outside maybe without knowledge on how to seek support or how to do the referral. So, then we chip in when they are already handling the matter (...) Sometimes we find they have already done the interrogation of the victim without counselling and dismissed the case because they are not specialised, so we have to get a counsellor and we then do the interview process again with different results."* (RA4-KY-08-A-justice)
- **Police officers trained in handling OCSEA cases may be transferred to other units.** One of the justice professionals interviewed drew attention to the rapid turnover of staff at the child protection units: *"When you're carrying out a training to police officers, you pick the police officer manning the children and gender desk but (...) they keep transferring and rotating, so you could have trained*

> "[The police officers were asking], 'You Madam, charge sheet itakaa namna gani?' (Madam, what will the charge sheet look like?) (...) What is the area of law?"

> *this person, they are so good at their work because they understand OCSEA and the unique things that come along when collecting evidence and recording the statement of such a case. But the police service in its normal course of work decided to transfer the police officer to another unrelated unit so you are left with someone who is not trained."* (RA4-KY-04-A-justice) Another justice professional recommended *"that the officers handling children's cases, the professionals who have been trained on children's rights and child protection, these people should not be transferred, and if it's to be transferred, the person brought in their place should be someone handling children's matters."* (RA4-KY-06-A-justice)

In summary, as a professional from the International Justice Mission Kenya Field Office put it, *"Having dedicated professionals, you see like the way we have the AHTCPU, this is something that we would want replicated around the country. Because what it means is that you are well trained, it means that now you're well-resourced because we know that you are there and you're specifically targeting big cases and it means that you are effective and efficient. Since the inception of the unit, it has become easy to make referrals of cases when you see OCSEA materials. So just having dedicated professionals whether within the police force, whether within the judiciary, whether within the children's department, these are the most critical people."* (RA4-KY-05-A-justice)

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

STEP 1. Children's and caregivers' first encounters with the police

Eight of the ten children we interviewed as part of the access to justice interviews who reported a case of OCSEA to the police only decided to engage the police after consulting with other people. Six of the ten said they felt comfortable when going to the police. Of the four who felt uncomfortable, two did not clarify why. The other two noted that the discomfort when going to the police was because *"I was forced to go by my family, it pained me"* (RA4-KY-09-A-child) and *"I was uncomfortable telling them in front of everyone."* (RA4-KY-03-A-child)

First encounters with the police were generally positive: *"I felt good, they tried to help me write the statement so they could help me further"* (RA4-KY-01-A-child) *"I was really free, because they did not harass me, they talked to me like anybody else."* (RA4-KY-10-A-child) However, some children struggled to understand what was said: *"At that time, I didn't know Kiswahili very well and they used to use Kiswahili which I could only understand a bit."* (RA4-KY-05-A-child) Another child couldn't keep up with the mixed use of English and Kiswahili stating that *"as a result I was not confident to ask questions."* (RA4-KY-09-A-child)

Among caregivers, some felt optimistic about the involvement of the police: *"I was very happy to get the police involved because I want justice for my child."* (RA4-KY-01-B-caregiver; RA4-KY-02-B-caregiver; RA4-KY-04-B-caregiver and RA4-KY-07-B-caregiver) However, others were apprehensive: *"I was scared of facing the police, I did not think the police could help, I was afraid of being arrested as a caregiver."* (RA4-KY-10-B-caregiver)

When asked about their motivations for going to the police, caregivers were largely looking for *"help with the case and the arrest of the perpetrator."* (RA4-KY-05-B-caregiver)

Information about rights and process: Out of the ten children we spoke with in the access to justice interviews, only three were informed about the process and their rights by the police. To most of the caregivers, it was not clear what rights they and their children had. There was a general feeling that the outcome of the police report depended to a large extent on the officers they met: if they were lucky, they would be properly informed about the process; otherwise they would receive no information whatsoever and reported feeling helpless.

Six of the ten caregivers felt the police did not explain the process to them and their rights properly. According to one: *"I didn't know my rights. I was confused about the law, how the case would go. I didn't have a headway, so I had to wait until the police explained to me what I should do next, they didn't tell me my rights as a caregiver of the child."* (RA4-KY-10-B-caregiver) Another caregiver said: *"I wasn't told anything, they just sent me back and forth. Someone told me my rights but they were not around to guide me through the process. I was very sad and the process was tiring. I was hurt as a parent. In the end, I got help from some organisation."* (RA4-KY-04-B-caregiver)

Those caregivers who did receive information about the process and their rights were satisfied with this guidance: *"Someone explained the process to me at the station, I was told of my right to testify and I felt good about knowing my rights. I got full information on how I could find justice for my child and as a result, I was able to support my child."* (RA4-KY-01-B-caregiver)

Referral to support services: Kenyan law, via the Victim Protection Act stipulates that immediate psychosocial support to the victim[117] and the provision of services to help them deal with emotional trauma[118] must be available to all victims of crimes.

An investigator from AHTCPU who took part in the access to justice interviews said that child victims of OCSEA are given counselling before their statements are taken. (RA4-KY-08-A-justice) A professional with experience in OCSEA cases noted that the AHTCPU in Nairobi is equipped with a room that provides privacy for the victim during counselling and when taking the statement. (RA4-KY-11-A-justice) According to the AHTCPU investigator, *"The counselling room is soundproof and has the recording equipment which we use to record the statement if the victim provides consent."* (RA4-KY-08-A-justice)

The same investigator added: *"I would say for the cases that the AHTCPU handles, because we have that approach where we bring in the Department of Children's Services and the Office of the Director of Public Prosecutions, most of the OCSEA victims get services especially the psychosocial support. (..) When we get the victim, and we bring them here, and introduce the children officers for counselling then we interview and record statements."*

While it is unclear how far the Victim Protection Act guidelines are followed in regular police stations, several of the caregivers of children who had accessed the justice system whom we interviewed confirmed that their children received psychological support/ counselling during the investigation and perceived this as a crucial element which helped their children cope with the situation. (RA4-KY-05-B-caregiver, RA4-KY-02-B-caregiver)

Children also described being offered other support services: *"They told me that they are going to take me to a place where I can be taken care of,"* recalled one child. (RA4-KY-10-A-child) *"I was sent to a hospital for a medical examination before being interviewed by the police,"* stated another. (RA4-KY-04-A-child). A third child said *"They told me they would help me and asked for my mother's number and if not, they would take me to court themselves."* (RA4-KY-05-A-child) (click here to read more about support services).

STEP 2. The interview process

The AHTCPU investigator confirmed that AHTCPU staff, but not other officers, are trained to interview child victims sensitively: *"For the AHTCPU, partners support us with training. Therefore, officers at the unit have received special training on how to work with child victims. You find however that the other law enforcement officers are many but do not normally receive this training."* (RA4-KY-08-A-justice)

Child-friendly measures: Our interviewees stated that child protection units in regular police stations have adopted measures to make the judicial process easier for child victims. However, as such units only exist in a few police stations, many victims of OCSEA are unlikely to benefit.

The children we spoke to in the justice to access interviews had mixed experiences of interaction with police officers. One of the children said that *"they used words of encouragement"* and promised *"it will be over soon."* (RA4-KY-01-A-child) However, other officers made the children very uncomfortable. *"The first thing police officer told me was that I was too young to be pregnant,"* one child recounted. (RA4-KY-09-A-child)

Some OCSEA victims complained of officers expressing harsh opinions and judging them: *"They blamed me for my situation saying that I asked for it, so they were asking why I was reporting it"* (RA4-KY-04-A-child) As a former counsellor pointed out in one of our interviews with justice professionals, *"You see when children are explaining what happened, they [police officers] don't have 'that' language. (....) So sometimes the police officer is forcing them to use the words that you would expect from an adult. Even culturally, a child is shy to mention certain words. Or they don't know how to describe. They only say 'tabia mbaya' (bad manners). (...) sometimes the child is recording a statement and the child is crying and someone (the police officer) is losing patience as they want to finish and handle another case."* (RA4-KY-04-A-justice)

[117] Republic of Kenya. (2014). Victim Protection Act No. 17 of 2014. Section 11(2 (c) (ii).
[118] *Ibid.*, Section 14(2).

Caregivers of children who had been through the justice system expressed the following criticisms: *"The police should be friendlier"* (RA4-KY-03-B-caregiver; RA4-KY-05-B-caregiver and RA4-KY-09-B-caregiver); *"The police should adjust their attitude and attend to people better […] so that even the children get courage to come out and speak the truth"* (RA4-KY-08-B-caregiver), and *"they should attend to everyone, rich or poor."* (RA4-KY-08-B-caregiver) *"They should create child-friendly spaces at the police stations and courts,"* added one of the caregivers. (RA4-KY-05-B-caregiver)

Opportunity to select a police officer: About half of the OCSEA victims we interviewed who had accessed the justice system (all girls) were allowed to choose who would be in the room when they made their statements. Given the opportunity to select a police officer, most of them selected female officers. Only two felt that the choice of officer was unimportant. The children who interacted with female officers were more comfortable about sharing details of their stories. One child said: *"The officer was very friendly and when she asked me the questions, I answered her"* (RA4-KY-02-A-child) Other children *"did not want men to know"* what had happened to them (RA4-KY-03-A-child) or said *"There is no way I could tell a man how I was feeling."* (RA4-KY-07-A-child)

Caregiver support: Some of the caregivers interviewed felt that they were able to support their children during the process with the police. One caregiver said: *"I went with her to the station to write a statement and after we went to the hospital for tests."* (RA4-KY-01-B-caregiver; RA4-KY-02-B-caregiver) However, another caregiver commented that *"The whole process was private and I was just updated afterwards."* (RA4-KY-07-B-caregiver)

According to a third caregiver, *"They hid her and I got reports that she was sick, I felt really bad and it wasn't right, something like that, they should allow the parents to see their child and support them."* (RA4-KY-07-B-caregiver)

This mother's experience of being separated from her child could be related to a tendency from some practitioners to remove children from their homes after reports of abuse even if no-one in the family is implicated (despite this not being preferred practice by the government).

Other issues: Children and caregivers also voiced suspicions about corruption: *"They should have a heart instead of taking bribes and destroying other children's lives […]"* one child said. (RA4-KY-08-A-child) A caregiver claimed that *"it was very hard to get justice because sometimes the police can be bribed and bought to dismiss the case by the perpetrator."* (RA4-KY-01-B-caregiver) According to another caregiver, *"I'm sorry to say but the police like bribes and I think that was the influence that derailed our case because the perpetrator's mother would send them money and I didn't and that made them take her side and the case was dropped."* (RA4-KY-04-B-caregiver)

Five of the Kenyan girls we spoke to in our OCSEA survivor conversations had been supported by staff from NGOs when approaching the police. None of them felt that their cases had been adequately investigated. *"We went to the hospital and I was examined, then to the police so he could be arrested but they kept saying they didn't get him, and the longer he was missing the more money we were spending for his search, so we just gave up because the police couldn't find him but they kept asking for money,"* recounted one survivor (RA5-KY-04-A) According to another survivor, *"They did not help with anything (…) They used to call and ask whether we have found him and we just said we hadn't found him, and they would say that they would see what they can do."* (RA5-KY-05) There was an overwhelming sense that these crimes were not taken seriously: *"I would also like that those who do such things to girls be put behind bars so that they don't ruin a girl's future."* (RA5-KY-08-A)

STEP 3. Passing the case on to the Children's Court

After the investigation, a case might be referred to the Children's Court. There are six dedicated children's courts in Kenya, two are gazetted while the remaining four are not yet gazetted. In court stations without dedicated children's courts, normal magistrates courts are converted short term to hear children's matters.*"OCSEA cases will go to a Children's Court. If it is Nairobi, the OCSEA case will go to the Milimani Children's Court"*, explained a Court of Appeal judge who is also Chairperson of the National Council on the Administration of Justice Special Task Force on Children Matters (RA1-KY-04-A). Eight out of the ten children in our access to justice interviews who had reported OCSEA to the police saw their cases proceed to court.

3.3 OBTAINING JUSTICE AND ACCESS TO REMEDIES

The Victim Protection Act makes it the duty of courts, administrative authorities and other persons with functions under the Act to preserve the dignity of a victim at each stage of the trial and subsequently.[119] The Act further provides that each victim should be dealt with in accordance with his or her age and level of intellectual development.[120] According to the Victim Protection Act, every victim deserves protection from secondary victimisation in all types of proceedings.[121] Every vulnerable witness is entitled to legal and social services at the expense of the State. [122]

3.3.1 Court proceedings

Technical capacity of justice staff

In order to deliver justice, courts need to be more familiar with OCSEA. According to a Judge of the Court of Appeal: *"I think the level of knowledge on OCSEA is nil. Other than knowing that it is a crime to exploit a child (…). I know there has been some training, but very little. Very few judicial officers have been trained."* (RA1-KY-04-A) Only ten prosecutors in Nairobi have received specific training to support OCSEA cases, and none in the other 46 counties. (RA1-KY-07-A)

Child-friendly courts

The Children's Court Practice Directions provide that *"The facilities within the Children's Court must be distinctive from the ordinary courts and therefore must be customised to be child-friendly."*[123] However, there are no specific guidelines that define child-friendly standards. As a member of staff of the Makadara Law Courts put it, *"The Children Act just says child-friendly, so what is child-friendly for an autistic child? What's friendly for a child that has suffered trauma? Is it child-friendly the environment, is it child-friendly the set up? What is this child friendliness? It has been left to us to define."* (RA4-KY-07-A-justice)

Moreover, only a few places have designated Children's Courts with designated children's magistrates who exclusively handle cases involving children. Elsewhere, these cases are handled by regular courts on specific days of the week in accordance with the provisions of the Children Act.[124] Although the magistrates hearing children's cases are gazetted as children's magistrates, and are trained in the special safeguards for children provided under the law, some child-friendly measures are tougher to deliver when not working in a dedicated children's court. This situation can also contribute to a backlog of cases.

Participation in the court procedure

According to a resident magistrate of the Makadara Law Courts, the hardest part for the child is meeting the offender *"because then when the child walks in, they see the perpetrator and first thing they do is they freeze."* (RA4-KY-07-A-justice) Every effort should be made to ensure that child victims do not have to face the offender. If this is unavoidable, a witness protection box should be used to allow the child to give evidence without seeing the offender (Boxing the offender rather than the child may be preferable). However, only a few courts are equipped with witness protection boxes and justice professionals reported that no courts were equipped for children to give evidence by video. Mechanisms that are the least stressful for the child should be adopted whenever possible.

For a conviction, the victim needs to testify against the offender. This can result in re-traumatisation. Some prosecutors apply for a child to be declared a vulnerable witness in line with the law.[125] The resident magistrate puts it as follows: *"So most of the times when you realise the child is not in a position to proceed with the matter (…) the prosecutor will say, 'We declare the child vulnerable, let the mother*

[119] *Ibid.*, Section 4(2)(c).
[120] *Ibid.*, Section 4(2)(d).
[121] *Ibid.*, Section 4(2)(f).
[122] *Ibid.*, Section 4(2)(g).
[123] Republic of Kenya (2016). The Children Act (Protection of Fundamental Rights and Freedoms of the Child) Children Court Practice Directions , Section 28.
[124] Republic of Kenya. (2001). Children Act No. 8 of 2001. Section 74.
[125] Republic of Kenya. (2006). The Sexual Offences Act No. 3 of 2006. Section 31(1).

of the child speak on behalf of the child'. Then we proceed with the mother explaining what the child is trying to say." (RA4-KY-07-A-justice) During our interviews with children who had accessed the justice system, we encountered one case where a children's officer spoke on behalf of the child, thus protecting her from the need to re-tell her ordeal in court. The child still felt included and heard, even though someone else spoke on her behalf. (RA4-KY-09-A-justice)

At least seven of the respondents in our interviews with justice professionals noted that in instances where child victims of sexual abuse were called upon to testify, they always testify in closed court in accordance with the Children Act.[126] They described this as standard practice: *"When listening to a children's case, (..) the court is empty. That is normal practice."* (RA4-KY-04-A-justice) Nevertheless, some children recounted having had to speak in an open court.

Although it is not always done, the victim may also be asked to participate in a victim impact assessment to guide the judge in the severity of the sentence. This could be particularly important in cases concerning OCSEA-related offences committed without in-person contact, to increase the understanding of the impact that online child sexual exploitation and abuse without in-person contact can still have.

Duration of process and trial

Rapid processing of OCSEA cases would allow the child victims to move on quickly and reduce the costs families face as they seek justice for OCSEA victims. However, at least half of the justice professionals we interviewed cited the time it takes for cases to come to court and be heard as an additional source of re-traumatisation.

> "The Children Act just says child-friendly, so what is child-friendly for an autistic child? What's friendly for a child that has suffered trauma? Is it child-friendly the environment, is it child-friendly the set up? What is this child friendliness? It has been left to us to define."

An official of the AHTCPU informed us that all of the OCSEA cases that had been filed as of March 2019 (when the unit was established) are still in the initial stages within the criminal justice system: *"The very first operation to arrest perpetrators of OCSEA was done in March 2019 and all the cases are still in the initial stages before the court. Before March of 2019, there was another OCSEA case already ongoing in Lamu involving a security guard which is handled by the Department of Criminal Investigation Cyber-Crime Unit* [127] *and I believe it is still in court."* (RA4-KY-08-A-justice)

According to a civil society justice professional: *"When we report a case of OCSEA, we try to follow up to see if the child has been rescued or if the case has progressed to court but you know for some reason online cases take forever. We get to hear maybe six months later something has happened."* (RA4-KY-02-A-justice)

According to an interviewee from the AHTCPU, some of the delays caused by issues specific to OCSEA cases – namely, a lack of specialised knowledge and understanding of OCSEA within the judicial professions, especially outside Nairobi, and delays by internet service providers in sharing information: *"Challenges come in when you are involving industry like ISPs. (...) When we request for IP address data, you find they take time to respond or they don't even respond at all. Because we are relying on that to even reach the victim and the offender, at times, it is a challenge."* (RA4-KY-08-A-justice) (See also chapter 3.4.3 on cooperation between law enforcers and ISPs and global platforms).

[126] Republic of Kenya. (2001). Children Act No. 8 of 2001. Section 75.
[127] We were not able to interview the Cyber Crime Unit to get more details of the case.

In spite of the delays mentioned, two of the children we interviewed appreciated the pace at which their cases moved through the judicial system. (RA4-KY-07-A-child, RA4-KY-05-A-child)

Experiences of children in court

An overwhelming majority of the child victims accessing the justice system whom we interviewed stated that they would be unwilling to interact with criminal justice actors again in the future – a significant deterrent for victims to seek justice.

Negative experiences were mainly related to:

- **A sense of exclusion:** One caregiver observed that the hardest part for the child was the feeling of helplessness: *"My child felt deceived by the perpetrator and also did not understand what was going on [at court]."* (RA4-KY-06-B-caregiver)
- **Re-traumatisation:** Almost all the children were upset by having to recount their ordeal repeatedly to different people including the person that helped them make the decision to go to the police, various law enforcement officers, lawyers and finally the court. They found it hard to talk about their experience to *"strangers"* and to *"talk in open court – it felt like there was no privacy."* (RA4-KY-04-A-child)
- **Language and communication barriers:** The use of English, Kiswahili or a mixture of different languages made it hard for some caregivers and child victims to follow proceedings. This was made worse by the suggestion that officials did not use age-appropriate language. Police, judges, court staff, prosecutors and lawyers may not be trained to use child-friendly/victim-sensitive language and procedures. Interpretation facilities may not be available in the child's mother tongue.
- **Victim-blaming and stigma:** One caregiver noted that some questions asked by the judge made the child uncomfortable. (RA4-KY-10-B-caregiver) In contrast, one of the children stated that the hardest part of her interaction with criminal justice workers was that *"They did not listen to what I wanted, they refused to release my perpetrator."* (RA4-KY-09-A-child) This child victim, who was pregnant as a result of the abuse, still intended to pursue an intimate relationship with the offender.

Victim-blaming and stigma were also highlighted by the justice professionals interviewed. The role of children can be unfairly emphasised in grooming cases. Cases involving male child victims with a same-sex offender entail additional issues. *"They are very defensive about it,"* one prosecutor noted, *"They don't want to admit. It's a mixture of guilt, remorse and shame. So, for girls it comes across a bit differently than for the boys from what we have seen. (….) the boys need more counselling to be able to open up."* (RA4-KY-09-A-justice) The fact that *"unnatural intercourse"* is criminalised by Kenya's Penal Code[128] may compound the stigma associated with same-sex relations to which boys who are victims of online grooming by male offenders, for example, are exposed, regardless of their sexual orientation.

Among one of the better experiences, one of the caregivers interviewed said their child coped well as *"She was treated well at the court and she was comfortable, and when we got to Nairobi, we were offered free transportation to the court, which took two days."* (RA4-KY-06-B-caregiver). In addition, two of the children felt their experiences were empowering: *"I felt the judge listened to me and I felt like I was free to ask questions."* (RA4-KY-07-A-child) Another child appreciated the reassurance she heard from a female judge: *"She said I would move to a better place and I would deliver my child safely."* (RA4-KY-09-A-child)

Legal aid

The Children Act entitles every child to legal representation at the expense of the State[129] through the National Legal Aid Service.[130] In practice, however, of the eight child victims we interviewed whose cases made it to court, only three had access to a lawyer. One of the reasons for this situation could be a shortage of available lawyers. In two cases, there were no government-appointed lawyers available. Nonetheless, the caregivers felt sufficiently supported by social workers who were present at the court hearings.

On the other hand, a representative of the National Legal Aid Service told *Disrupting Harm* researchers that they rarely receive applications for support from child victims of any kind of crime.[131] A follow-up with at least two justice professionals suggested a lack

[128] Republic of Kenya. (1930). The Penal Code of Kenya (Cap. 63) (Rev. 2012). Section 162.
[129] Republic of Kenya. (2001). Children Act No. 8 of 2001. Section 77.
[130] Republic of Kenya. (2016). Legal Aid Act No. 6 of 2016. Section 36(1).
[131] Information provided by telephone on 11 November 2020.

of awareness about this service. Very few know that this service it is available to child victims (of OCSEA and other crimes) as well as child offenders, and the procedures for applying. (RA4-KY-11-A-justice, RA4-KY-01-A-justice)

According to a representative of the Department of Children's Services, *"The National Legal Aid Service has branches in various parts of the country, but people don't make use of them because they don't know about them. There is a need to create awareness and hold legal clinics in communities so people can know that they exist. People do not know what they do."* (RA4-KY-11-A-justice)

In Nairobi, the gap in legal aid for OCSEA cases may be of less consequence as cases are prosecuted by public prosecutors. The officer-in-charge of the AHTCPU explained: *"For Nairobi, even if we don't have lawyers watching brief on behalf of the victim of OCSEA, we have not felt a gap in legal representation. This is because the cases in Nairobi are prosecuted by prosecutors from the Children's Division under the Office of the Director of Public Prosecutions. They are also lawyers and hence we don't feel a gap. In other parts of the country we don't have these prosecutors so there is more need for legal aid."* (RA4-KY-08-B-justice).

The majority of the frontline workers that we surveyed rated the legal services for OCSEA cases as either 'poor' or 'fair', both in terms of their availability and quality. One participant mentioned that *"Much is focused on psychosocial support; we still don't have trained legal experts to support issues of OCSEA."* (RA3-KY-19-A).

Be that as it may, victims with the assistance of a lawyer had a less negative experience in court, and those who did not have legal support experienced greater stress: *"I went to court alone and did not understand the proceedings. I was afraid but I had to speak, I had no other choice."* (RA4-KY-08-A-child) Two caregivers of children who had accessed the justice system call for the provision of lawyers *"to help the family and get legal justice for the family."* (RA4-KY-01-B caregiver, RA4-KY-05-B caregiver) Ideally, caregivers and child victims should be consulted before the allocation of a lawyer. There appears to be a preference for female lawyers, at least for female OCSEA victims.

> “The majority of the frontline workers that we surveyed rated the legal services for OCSEA cases as either ‘poor’ or ‘fair’.”

3.3.2 Compensation

Where compensation claims are addressed along with the criminal case, families do not need to take additional action, and children and families do not have to re-live their trauma again in a separate compensation case.

The law in Kenya provides for victims of OCSEA to be compensated by the offender upon conviction.[132] However, applying for compensation under criminal law is not yet an established practice. Of the OCSEA victims and caregivers in our access to justice interviews, only one child was aware of her right to compensation.

When informed of their rights during our interviews, six of the ten children and six of the ten caregivers expressed no interest in pursuing compensation. *"Even if they compensated me, they destroyed a life and it can't be refunded, so you just let some things go,"* said one caregiver. (RA4-KY-03-B-caregiver)

Nevertheless, most caregivers agreed it would have been useful to have known about their right to compensation earlier. One child saw compensation as another way of holding the offender accountable. (RA4-KY-10-A-child)

Other barriers to compensation include lack of awareness among justice professionals and the likelihood of the offender being unable to pay.

Although the Victim Protection Act establishes a Victim's Protection Trust Fund,[133] none of the justice professionals we interviewed knew of any victim that had been compensated by it or provided with support to attend court hearings. A senior coordinator of survivor services from the International

[132] Republic of Kenya. (2018). The Computer Misuse and Cybercrimes Act No. 5 of 2018. Section 45(1).
[133] Republic of Kenya. (2014). Victim Protection Act No. 17 of 2014. Part V.

Justice Mission confirmed that the fund was not yet operating, although the board was in place. (RA4-KY-05-A-justice).

Out-of-court settlements are undesirable as the offender is not held accountable before the law. There were no such settlements in the cases we explored through our interviews with child victims and caregivers who had accessed the justice system. One caregiver recalled that *"The white perpetrator promised my child that he would give her some money if she kept quiet. (...) The perpetrator later refused to give us the money stating that we had gotten him arrested, therefore breaking the agreement that if we did not report the case to the police he would give us money."* (RA4-KY-03-B-caregiver)

3.3.3 Social Support Services

Under the Victim Protection Act, it is the first duty of a person dealing with a victim to secure the victim from further harm.[134] In partnership with civil society organisations, the Department of Children's Services is tasked with providing rescue, shelter and reintegration services, referrals to medical care[135] and psychosocial support[136] to child victims of crime.

While children are best protected in a home environment, rescue or temporary shelter services are needed if the situation at home is unsafe or alternative family-based care is not immediately available. In practice, the availability of support services for children recovering from OCSEA is limited. The frontline workers who took part in our survey saw location as the main limitation – services are concentrated in urban areas – followed by the cost and low quality of the services.

Referrals: For those OCSEA victims whose cases are handled by the AHTCPU, the Department of Children's Services has appointed a children's officer to assist the Unit in supporting OCSEA victims. In our interviews with justice professionals, an official of the Department of Children's Services and two officials from the Unit confirmed that whenever a case is reported, the two agencies work together to ensure that the victim receives the support s/he needs even as the law enforcement officers undertake their investigations. However, for cases of OCSEA handled at regular police stations, there is need to create awareness and strengthen linkages with the Department of Children's Services so that support can be extended to victims.

Psychosocial support: Children have the right to free counselling under the law[137] but these services are not readily accessible everywhere. *"It's not that counsellors are not there,"* explained the representative of the Department of Children's Services whom we interviewed, *"There are professional counsellors all over in this country and you can access them if you are able to pay. So, you find victims are not able to afford it and for us, we work with child focused agencies who can provide for free. But you see we cannot depend on that, as there are those areas without those child-focused agencies. If there was a fund that could support victims to pay for counselling, it would ease this challenge."* (RA4-KY-11-A-justice)

A frontline worker from an organisation undertaking awareness raising and training activities argued that *"The support and counselling centres are not enough and it's costly. There are no such free services offered by the government, thus most people don't take their children for the same. Limited awareness has also made children and parents not to realise this as a violation."* (RA3-KY-37-A)

In fact, 68% of the frontline workers we surveyed – most of whom provide counselling services themselves – rated the availability of psychological services as either 'poor' or 'fair' and 62% rated the quality as either 'poor' or 'fair'.

Free services could be made more widely available by activating the Victim Protection Trust Fund, set up under the Victim Protection Act to assist the victims of crimes.[138]

One of the few child-focused organisations providing free counselling is Childline Kenya, which offers children on-location counselling services in Mombasa, Nairobi and Kisumu as well as telephone counselling country wide.

Medical services: Free medical support is widely

[134] *Ibid.*, Section 11(2).
[135] *Ibid.*, Section 11(2).
[136] *Ibid.*, Section 14(2).
[137] *Ibid.*, Sections 11(2) & 14(2).
[138] *Ibid.*, Section 28(2)(a).

available. A former legal officer of Childline Kenya explained that *"Mostly when you get cases of abuse, including OCSEA, you refer them to public facilities for medical attention where treatment is free."* (RA4-KY-04-A-justice)

Of the frontline workers we surveyed, around half thought the availability and quality of medical services for children subjected to OCSEA was either 'good' or 'excellent'. This is higher than for any of the other services the frontline workers were asked to rate (i.e., psychosocial, legal and reintegration services).

Reintegration services: The Children Act recognises that a child who has been sexually abused or is prone to sexual abuse and exploitation, including CSAM-related conduct, needs care and protection.[139] Additionally, The Victim Protection Act outlines the role of the Victim Protection Board in advising the Cabinet Secretary on activities aimed at the implementation of rehabilitative programmes for victims of crimes.[140] The court before which such a child is brought may commit such child to a rehabilitation school suitable to their needs and attainments.[141]

"Around half of the frontline workers that we surveyed thought that medical services for OCSEA victims were either 'good' or 'excellent'."

The representative of the Department of Children's Services interviewed for *Disrupting Harm* confirmed that there are government shelters where victims of OCSEA may be placed if it is absolutely necessary to remove them from their current environments, and that partners of the Department offer this service in places where there is no government institution. However, in some counties the shelters are few and far between: *"Where we have vast counties, you'll find children have to travel so many kilometres before you can actually get to a place of safety for them as we move them from the perpetrator."* (RA4-KY-11-A-justice)

Protecting children

A number of respondents in Kenya spoke of 'rescuing' children living in particular harmful circumstances. This is also one of the prescribed duties of the Department of Children's Services under the law. While some emergency circumstances demand such action, the removal of a child from their family and community for protective reasons bears its own risks.

Fear of removal can also discourage children from disclosing abuse and seeking help, since they may view residential care negatively or even as a punishment.[142] Some emergency circumstances still demand removal actions, but where possible, removing the offender instead can protect the child while maintaining their attachment to their organic support systems.

Two other justice professionals interviewed spoke of the need to strengthen after-care services. (RA4-KY-05-A-justice, RA4-KY-11-A-justice) One of them proposed minimum standards: *"There is the issue of holistic survivor care, just having the minimum standards of care for every child victim of OCSEA, in order to know what must be given to every child for us to say that now they are ready for reintegration."* (RA4-KY-05-A-justice)

One child said that professionals who interact with children should contribute to the reintegration of children back to their homes and their families at the end of their cases: *"Stakeholders should follow up and help all children."* (RA4-KY-06-A-child)

[139] Republic of Kenya. (2001). Children Act No. 8 of 2001. Section 119(1)(n).
[140] Republic of Kenya. (2014). Victim Protection Act No. 17 of 2014. Section 32.
[141] Republic of Kenya. (2001). Children Act No. 8 of 2001. Section 125(2)(c).
[142] ECPAT International. (2017). Through the Eyes of the Child: Barriers to access to justice and remedies for child victims of sexual exploitation. Bangkok, ECPAT International. 54-55.

3.4 COORDINATION AND COLLABORATION

3.4.1 Policy and government

Promising developments and initiatives

At the policy and government level, our research has identified several promising developments and initiatives in addressing OCSEA in Kenya:

- **Acknowledgement of the threat:** In the 12 duty-bearer interviews, almost all the respondents perceived OCSEA as a growing threat. In the words of a Principal Children's Officer from the Child Online Protection Unit of the Department of Children's Services: *"As much as online child sexual exploitation and abuse has been there for some time, it was not as it is now. With the advancement in technology, we find that there is more online child sexual exploitation and abuse than what we used to know several years ago. For example, when I was in the field, we would hear of pornographic materials, children being put in a room and somebody trying to come up with some videos but that time it was 'a foreign issue'. It was something done by 'Wazungus' [white people] in secluded and affluent areas. It was not as big as it is now."* (RA1-KY-08-A)
- **Understanding of the need for collaboration:** The importance of a multi-stakeholder approach for addressing OCSEA was underlined in six of the twelve duty-bearer interviews. According to the Principal Children's Officer cited above, *"OCSEA is not just one department's problem. It cuts across government and state agencies"* and *"For the Department of Children's Services, we look at OCSEA from the broader perspective of child protection, maybe within sexual exploitation. We do not want it to be in a silo."* (RA1-KY-08-A) As an example, the health system also may play a role. For instance, as a gateway to support for victims.
- **Creation of the National Technical Working Group on Child Online Protection:** The group brings together mandated government agencies, civil society organisations, industry representatives and UN agencies.[143] Thanks to this working group, adequate coordination exists at the national level between government agencies with mandates related to OCSEA, according to most of the frontline workers we surveyed. A principal officer from the National Council of Children's Services described the group as vibrant, well-coordinated and the embodiment of a multi-sectoral approach, while at the same time admitting: *"All these agencies may not be fully conversant with it and the process and procedures to be followed, and we are still learning and putting measures in place to ensure we address such gaps so there is seamless flow."* (RA1-KY-02-A) A representative of the Communications Authority of Kenya still felt the need for more synergy: *"The agencies know their mandates but (...) for example, when it comes to reporting of cases and how cases should be handled, agencies tend to talk about their mechanisms yet there is need to find ways of working together with others."* (RA1-KY-03-A)

Awareness raising initiatives

- The Ministry of Education is currently integrating child online protection into the new school curriculum, which will help to standardise awareness raising in schools. A representative of the Kenya Institute of Curriculum Development said that OCSEA is not directly addressed but that relevant topics such as online offenders and how to avoid them are included. (RA1- KY-10-A)
- In partnership with Terre des Hommes Netherlands, the Ministry of Education recently launched the first children's and facilitators' manuals for training on online safety and security.[144] These are to be used to equip children and caregivers to identify, prevent and respond to abuse and exploitation. It is not clear if they will be rolled out nationally.
- The Communications Authority of Kenya runs awareness raising initiatives on child online protection. Child and adult consumers of information and communication technology services can visit the *Kikao Kikuu* county forums to discuss and explore solutions for communications challenges in the counties.[145]

[143] The National Technical Working Group on Child Online Protection is Comprised of: The Department of Children's Services, Directorate of Criminal Investigations-Anti Human Trafficking, Child Protection Unit, Directorate of Criminal Investigations HQs – Cyber-Crime Forensic Lab, Information and Communication Technology Authority, Department of Information, Kenya Institute of Curriculum Development , Judiciary, Kenya Film Classification Board, Communication Authority of Kenya, Ministry of Education, Kenya Police Service, Office of the Director of Public Prosecutions, Attorney General's office, Kenya Computer Incidence Response Team, UN agencies- UNICEF, UNODC, INGOs/ National NGO's- Terres de Hommes, Child Line – Kenya, African Institute of Child Studies, Watoto Watch and ECPAT.

[144] KBC News. (2020). Education Ministry launches online safety manual.

[145] See: Communications Authority of Kenya: Kikao Kikuu.

- The Kenya Film Classification Board runs a media literacy programme entitled *You are what you consume*[146] intended for a wide national audience.

Training programmes

- In conjunction with Terre des Hommes Netherlands, the Department of Children's Services provided 76 children's officers, police officers, magistrates and prosecutors from Nairobi, Nakuru, Kisumu and Mombasa with two days of training on OCSEA prevention and response, since in the words of the principal children's officer from the Child Online Protection Unit of the Department of Children's Services, *"It's a negligible number of officers that have been trained on OCSEA."* (RA1-KY-08-A)
- According to the Ministry of Information Communication Technology, a five-day Child Online Protection Training programme has been developed by the Communications Authority of Kenya, African Advanced Level Telecommunications Institute and the International Telecommunications Union Centre of Excellence for professionals from both government agencies and non-governmental organisations. Two workshops[147] have been conducted face-to-face and others online.

Challenges

Nevertheless, much needs to be done. *"I do acknowledge that conversations have started but we have a long way to go in terms of awareness creation and setting up of appropriate response structures and also effective referral pathways,"* said one of the respondents to our frontline workers' survey. (RA3-KY-29-A) Pressing issues highlighted from our research activities included the following:

- **Lack of awareness at local level and among frontline workers.** At county level and lower levels, the existing child protection mechanisms – i.e., the Area Advisory Councils – coordinate OCSEA issues. However, according to the UNICEF Kenya's Head of Child Protection, *"The challenge is that there is still not much awareness at the county level in regard to OCSEA prevalence. Take a Children's Officer somewhere in West Pokot, they probably have low levels of awareness that this is an emerging issue and that it's something they need to consider in their broader work of violence against children."* (RA1-KY-01-B)
- **Insufficient training of professionals.** Eighty percent of the frontline workers we surveyed rated the government's training efforts as either 'poor' or 'fair'. As an example, the Head of the Children Division and Anti-Female Genital Mutilation Unit commented: *"Awareness and technical capacity is a challenge. (...) These cases are technical and there are forensic issues as well. (...) Except for the few prosecutors trained and working with the Directorate of Criminal Investigations Child Prosecution Unit, there is need for training not only for prosecutors but police and the bench [magistrates and judges] as well."* (RA1-KY-07-A)
- **Understaffing at the Department of Children's Services.** According to a Deputy Director of the Department of Children's Services, *"We have officers in 283 out of the 295 sub-counties. In those 283, you will find in a sub county it is only one officer without a driver, goes to the post office, goes to court (....) The Department of Children's Services is under-represented (....) Where a child is abused, we are not able to reach the child in good time. We have to refer to partners."* (RA1-KY-08-B) The Department's Online Child Protection unit currently has one officer. A representative from the Communications Authority of Kenya commented: *"Robustness on the role and mandate of Department of Children's Services needs to be strengthened. The Department for example on the ground works with volunteers which might not make it a strong approach in carrying out its mandate."* (RA1-KY-03-A)

> “Where a child is abused, we are not able to reach the child in good time. We have to refer to partners.”

[146] See: Kenya Film Classification Board: You are what you consume.
[147] AFRALTI. (2020). Child online protection training workshop 2020; & AFRALTI. (2019). November child online protection training workshop.

- **Limited government funding:** Funding is a challenge for many agencies. An interviewee from the Department of Children's services explained that their work is funded by partners such as UNICEF or civil society organisations: *"When it comes to the financial resources for children's services, it's minimal (...) but when we flag out our programmes properly, then we can get some funding from partners, not from mainstream government. The [children's officer heading the child online protection unit] is funded by partners (...) Last year, we did not have any resources from the government for that work (...) all our activities were supported by partners, OCSEA being a part [of this]."* (RA1-KY-08-B) A principal officer from the National Council of Children's Services added: *"We find that the children's sector is inadequately funded so that whatever you are given is not adequate (...) We have other government agencies with a mandate on children and more often than not, in case of any emergency or something, some components are more prioritised – health and education but they ignore child protection. There is, therefore, need for a balance in the distribution of resources for child protection services."* (RA1-KY-02-A) The chair of the Special Task Force on Children Matters noted that budgetary resources to safeguard the rights of children within the criminal justice system is a challenge for the judiciary and other law enforcement agencies alike: *"We don't have any budget that is designated for children. We just use what is given for other court operations. We know children have their own needs even when they come to court, they require lunch, we require to set up the place where they stay, we need a caretaker for them, we need toys and games (...). The police deal with children every day, they have a child protection unit yet there is no budget for children"* (RA1-KY-04-A) In our survey of frontline workers, 96% of respondents rated funding as 'poor' or 'fair'. Funding and training (rated as 'poor' or 'fair' by 80%) were most frequently selected as the major obstacles to adequate services for victims of OCSEA.
- **Lack of public awareness:** *"Awareness is a big problem because I don't think we even know there is a crime like that,"* said the Court of Appeal judge who also heads the Special Task Force on Children Matters, *"Awareness should be wide including also the communities themselves because if they don't report, then there is a problem. That is where we need to begin."* (RA1-KY-04-A) Respondents questioned whether awareness raising activities were reaching all regions and segments of society. *"So far I would say they are (...) only reaching the rich. (...) If there is a programme on TV and you are sensitising parents on how to keep their children safe online, there are so many other parents out there who may not have that TV,"* said a Principal Children's Officer at the National Council of Children's Services. (RA1-KY-02-A) *"How many people will sit to watch TV?"* added a principal children's officer from the Child Online Protection Unit. *"We should look at the medium we use when we try to sensitise people in the grassroots (...) We should use different approaches."* (RA1-KY-08-A) The Department of Children's Services confirmed that awareness activities have been conducted in a limited number of counties, not including rural counties. Watoto Watch Network confirmed that their awareness raising activities under the project implemented by UNICEF with funding from the Global Partnership to End Violence against Children, through its Safe Online initiative, targeted only Mombasa, Machakos, Nairobi and Nakuru. *"We need to train more stakeholders like 'training of trainers' and have them in every county, and then now they are able to train others,"* remarked a Principal Children's Officer. (RA1-KY-08-A) A representative of the Communications Authority of Kenya also acknowledged that *"It needs to go a level deeper in content including talking about the underlying issues as technology is only an enabler and also to broaden the scope."* (RA1-KY-03-A) Of our frontline workers' sample, two thirds rated the government's awareness raising activities and efforts on *"speaking publicly about child sexual exploitation"* as either 'poor' or 'fair'.

> **"Awareness should be wide including also the communities themselves because if they don't report, then there is a problem. That is where we need to begin."**

3.4.2 Civil society

Civil society organisations in Kenya play a major part in responding to OCSEA. They refer cases to the police and the courts and cooperate with the Department of Children's Services in the provision of services like shelter, counselling and legal aid. They are also involved in awareness raising activities and in training the child protection workforce. *"OCSEA requires a multi-sectoral approach and it's not for the government to work alone without the civil society organisations,"* says a UNICEF child protection officer at the UNICEF country office. (RA1-KY-01-A)

The local and international civil society organisations and UN agencies working on OCSEA in Kenya include Childline Kenya, Watoto Watch Network, Mtoto News, Terre des Hommes Netherlands, ECPAT International, Arigatou, UNICEF and the United Nations Office on Drugs and Crime.

While these organisations provide crucial services, their efforts and resources alone are not enough. According to one frontline worker, *"The support systems for helping survivors of OCSEA are extremely limited due to the small number of NGOs dealing in OCSEA. This is also due to insufficient awareness by most service providers from the government on what OCSEA is and how it happens."* (RA3-KY-01-A) Another frontline worker commented: *"The government must not take for granted the issues that surround the children especially on the internet. They give less support to organisations that try to deal with online issues. Governments should be supportive."* (RA3-KY-26-A)

When asked to assess the collaboration on OCSEA among non-government organisations, 52% of frontline workers said it was 'good' or 'excellent' and 48% 'fair', 'poor' or 'non-existent'

3.4.3 Internet service providers and platforms

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

Domestic Internet Service Providers

Evidence gathering: When the law enforcement authorities need evidence from a domestic Internet service provider – for example, to identify who was using a particular IP address or phone number at the time an offence was committed – they serve a court order to the service provider demanding this information. They can then use the subscriber information to locate and apprehend the suspect and to submit as evidence in court.[148]

Article 50 of the Computer Misuse and Cybercrimes Act provides that investigating agencies can apply for court orders when they have reasonable grounds to believe that subscriber information in the possession or control of a service provider is needed for the purpose of an investigation.[149] Moreover, service providers[150] can be compelled to collect, record or cooperate in the collection or recording – by the police or other authorised person – of traffic and content data.[151]

According to an investigator from the AHTCPU interviewed for *Disrupting Harm*, the Computer Misuse and Cybercrimes Act *"has helped us to bring on board the internet service providers on what we need to prove OCSEA cases. (...) We can go to internet service providers and they are more compliant because we have the Act as a reference."* (RA4-KY-08-A-justice)

Nevertheless, according to the same source, it is sometimes difficult to obtain the information requested due to:

- lack of a policy that regulates the length of time for which internet service providers must store data: *"You find that the internet service providers store data for some time. It is not regulated so at times you don't get it because they have done away with the data as they have their own policy to control the data, what to store and for how long. If it is data that has overstayed, we don't get it. When they have it, they comply."* (RA4-KY-08-A-justice)
- slow response to the court orders, leading to delays in prosecutions: *"When we request for IP address*

[148] This approach however ignores challenges posed by carrier grade Network Address Translation, a process by which rapidly exhausting IPv4 addresses have been assigned by ISPs to multiple users at the same time, thereby precluding definitive identification of the device and user behind an IP address in certain cases.
[149] Republic of Kenya. (2018). The Computer Misuse and Cybercrimes Act No. 5 of 2018. Section 50(1)(b) and (2)(b).
[150] *Ibid.*, Section 2.
[151] *Ibid.*, Section 52(1)(b) & 53(1)(b).

> *data, you find they take time to respond or they don't even respond at all. Because we are relying on that to even reach the victim and the offender, at times, it is a challenge."* (RA4-KY-08-A-justice)

Safaricom, the largest mobile telecommunications operator in Kenya with a market share of about two-thirds, has reportedly taken steps to process requests for information for the prosecution of OCSEA cases faster. The officer-in-charge of the AHTCPU explained: *"Safaricom identified a specific liaison officer for this unit. An officer of the Directorate of Criminal Investigations who is attached there to deal specifically with the Unit's requests. We are yet to have the same with other internet service providers."* (RA4-KY-08-B-justice)

Removing/reporting CSAM: Kenyan laws do not impose legal duties on internet service providers to filter and/or block and/or take down CSAM and to report companies and/or individuals disseminating, trading or distributing the material. However, the National Kenya Computer Incident Response Team Coordination Centre may request internet service providers to remove content from their platforms, and compliance with requests is reportedly high.

As a representative of the Team explained: *"If there are gross materials, we in our own volition, can make a move to request the service providers (...) to have some content removed. (...) Other government agencies and also private organisations can flag some content and share with us and we will be in a position to analyse, see if it meets the criteria, and if it does, we will occasion the removal (...) We compel internet service providers to remove when the material in question is of a serious criminal nature – for example, child sexual abuse [material]. And you find that there is a way it's structured, that when it [the notice] reaches their servers, they know this is a demand and not a request. A demand is actioned within one hour. We have that arrangement and there is no instance where we have had to penalise."* (RA1-KY-11-A) However, the team was unable to provide us with specific statistics on child-related reports.

If internet service providers were obliged to *report* companies and/or individuals disseminating or distributing CSAM, an investigator from the AHTCU pointed out, *"It will assist in that immediately they detect OCSEA material from their side, it will be controlled and the materials will not be widely distributed."* (RA4-KY-08-A-justice) However, even if domestic internet service providers were required by law to filter/ block/take down CSAM, this would only apply to material hosted in Kenya – and the Internet Watch Foundation as well as INHOPE data indicate that relatively little material is currently hosted in Kenya.

In a promising development, in the first quarter of 2020, the Department of Children's Services indicated that it had initiated discussions with internet service providers to discuss their role in addressing OCSEA and other child online protection issues. "*They did not even know about these OCSEA cases. When we had that meeting with them and we educated them, we told them they can innovate and prevent these abuses even from being uploaded on their platforms,"* explained the principal children's officer from the Child Online Protection Unit of the Department of Children's Services. (RA1-KY-08-A)

Global platforms

Evidence gathering: If a report is made to the Kenyan police about OCSEA on a global platform, such as Facebook, a request is made to the platform to obtain subscriber information and IP data. Once the IP is known, the police then follow the domestic internet service provider request process to resolve the IP data and confirm the identity, location and other details of the suspect.

The wording of Article 50 of the Computer Misuse and Cybercrimes Act, which refers broadly to *"service provider offering [...] services in Kenya"*,[152] opens the door to obtain court orders directed to non-local service providers. The Act also enables the Office of the Attorney General and Department of Justice to request (or receive requests for) assistance from another State in any investigation related to a crime under the Act.[153]

[152] *Ibid.*, Section 50 (2)(b).
[153] *Ibid.*, Section 57(2).

In addition, the Mutual Legal Assistance Act outlines procedures for cases where Kenya has to seek legal assistance from another state with which it has a mutual legal assistance arrangement, or vice versa.[154]

Global platforms cannot be compelled to disclose information by Kenyan court orders, since they are governed by the domestic laws in their home countries – in the case of the USA, the Stored Communications Act and Electronic Communication Privacy Act. US law expressly prohibits the disclosure of communications content such as messages and images directly to non-US law enforcement authorities.

However, US tech platforms may voluntarily disclose non-content data, which includes subscriber data and IP logs, to such authorities. The largest US technology companies have dedicated Law Enforcement Response Teams (LERT) to respond to data requests from non-US law enforcement agencies. Facebook now has a dedicated Law Enforcement outreach manager for Sub-Saharan Africa.

Interviews held as part of the analysis of non-law enforcement data for *Disrupting Harm* indicated that there are informal working arrangements between the Kenyan law enforcement authorities and companies like Facebook and Google in relation to the voluntary disclosure of non-content data.

If the Kenyan police need to obtain information on content hosted outside of Kenya but not on a US tech platform (e.g.: on a website), the request would rely on the existence of a mutual legal assistance arrangement with the government in question.

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

Within this context, the normal procedure would be for the National Kenya Computer Incident Response Team (KE-CIRT) to send an informal email rather than a court order demanding removal. KE-CIRT was unable to provide statistics on its use of procedures or the quantity of CSAM removed as a result.

Transparency data

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

- 14 requests to Facebook for content restriction, related to violations of hate speech and election laws, and a private case of defamation;
- 20 requests to Facebook for user data;
- 19 requests to Google for content removal, mostly related to defamation;
- 9 requests for Google user data;
- 5 requests to Apple;
- 1 request to Twitter for user data, and 1 for content removal;

While none of the major platforms publish data specific to OCSEA or fully disaggregated by the type of crime, the diversity of platforms addressed suggests that Kenya engages with US technology companies more than some of the other African countries studied for *Disrupting Harm.*[155]

[154] Republic of Kenya. (2011). Mutual Legal Assistance Act No. 36 of 2011.
[155] Platforms were selected on the bases of high volumes of reports to NCMEC (10,000+), availability of transparency reporting, and known popularity in *Disrupting Harm* focus countries. In addition to US-based companies, transparency reports for Line and TikTok were also reviewed.

4. HOW TO DISRUPT HARM IN KENYA

Disrupting harm from online child sexual exploitation and abuse requires comprehensive and sustained actions from us all – families, communities, government duty-bearers, law enforcement agencies, justice and social support service professionals, and the 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 too much of the responsibility on children.

A detailed set of actions needed in Kenya are clustered under five key insights from the *Disrupting Harm* data and sign-posted for different stakeholder groups. However, all these recommendations are interlinked and are most effective if implemented together.

INSIGHT 1

Internet-using children in Kenya are subjected to OCSEA. According to children who were subjected to OCSEA and frontline workers, most offenders are someone the child already knows. These crimes can happen while children spend time online, or in person but involving technology.

Government

1.1. Adapt and deliver national-scale awareness and education programmes about the sexual exploitation and abuse of children – including how technology might play a role. These programmes must be evidence-based and not shy away from difficult and sensitive messages about sex, or the finding that offenders 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, the Ministry of Education and Kenya Institute of Curriculum Development have a leading role to play. For reaching wider communities across the country the Communications Authority of Kenya and the Department of Children's Services, with its presence at the local level, are important institutions. The Ministry of Information Communication and Technology, the Anti Human Trafficking and Child Protection Unit of the Department of Criminal Investigations, the Kenya Film Classification Board and National Government Administration Officers (NGAO) can all support these efforts with their own expertise and in their respective sectors.

Liaising with churches, child rights clubs and peer mechanisms can also be important to create awareness about OCSEA (including reporting mechanisms – see Insight 2). Information on OCSEA should be included in parenting education programmes. Special care should be taken to ensure that information is communicated to children with disabilities.

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 (see *Start the chat*[156] for an example).
- 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 children are using (see *Be Connected*[157] for an example).
- 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 know about sex, it enables offenders to 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.

1.3. Adjust education and awareness raising approaches to reach children. Pamphlets may not reach the intended audience. It is essential to employ child-friendly language and engage through social media and messaging platforms that children are using. Campaigns should be designed and run by people who understand the approaches and messages; they must receive experiential training and support to be able to design and share this type

[156] See: eSafety Commissioner's programme: 'Start the Chat'.
[157] See: eSafety Commissioner's programme: 'Be Connected'

of material. Better still are campaigns and messaging that involve young people in their design and delivery.

Existing tools like the Ministry of Education's online safety and security manuals may serve as one avenue for delivering the messages identified in the *Disrupting Harm* research. However, ensuring that these issues are explored with the necessary depth and sensitivities also requires training and support for those required to deliver such complex material.

Caregivers, teachers, medical staff and social support services

1.4. Improve understanding of digital platforms and technologies. Around half of the caregivers of internet-using children in Kenya have never used the internet themselves. Being involved and supportive of a child's internet use will help them understand the risk and benefits of being online and lead to a more open dialogue between children and adults when children face dangers or harm online.

1.5. Inform children about their right to be protected from all forms of physical, sexual, and emotional abuse and exploitation, 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.

1.6. Caregivers and duty bearers should learn about what children are doing online and offline, and be vigilant about the people that 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.

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, Kenya 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 recommendations 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 Kenya. The evidence from Kenya shows that even though many of the capabilities in the Model National Response exist, they are not functioning optimally.

Our recommendations primarily address legislation,[158] dedicated law enforcement,[159] judiciary and prosecutors,[160] and education programmes.[161] 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, or caregivers, the community and teachers.

The recommendations are organised under five key insights from the *Disrupting Harm* evidence, and signposted for different stakeholder groups.

[158] Model National Response #3.
[159] Model National Response #4.
[160] Model National Response #5.
[161] Model National Response #13.

INSIGHT 2

Many children in Kenya did not tell anyone the last time they were subjected to OCSEA. Children tend to disclose to people they know rather than reporting to a helpline or the police.

Government

2.1. Provide public financial support to Childline Kenya in order to ensure its sustainability and improve its ability both to receive reports and to provide psychosocial support to children. Allocations should be made for this purpose in the budget of the Ministry of Labour and Social Protection. The Ministry of Health, the Communication Authority of Kenya and internet service providers (Safaricom, Airtel) could also contribute. However, voluntary contributions should only be complementary. In return, Childline Kenya could be requested to assess their efficiency and hold extensive consultations with children on how to best provide support for OCSEA.

2.2. Increase awareness raising efforts about hotlines and helplines as a reporting and help-seeking mechanism for OCSEA. An important prerequisite is that helplines should be adequately resourced and providing good quality care and support. Even if children are made aware of helplines, if initial responses to disclosure and help-seeking are poor, the child – and others observing the case – will be much less likely to seek help again.

2.3. Diversify mechanisms for children to disclose concerns, seek help and formally make reports (including simple child-friendly, online methods), bearing in mind that most children first prefer to seek help from friends, then within their own family or community.

A further consideration from the data

Children abused by an offender of the same sex may have difficulty disclosing instances of exploitation or abuse or seeking help due to the stigma associated with being viewed as homosexual which involves strong societal taboos, and is criminalised. Children may fear legal consequences if they report. Although our survey results show that boys and girls are both subjected to OCSEA, no male victims could be identified for interview during the research for *Disrupting Harm in Kenya.*

Law enforcement

2.4. Establish a clear reporting process for cases of OCSEA and facilitate widespread training for all police and other duty-bearers to ensure full implementation, so that children and families are comfortable about reporting instances of abuse. Ensure that child-friendly procedures are implemented whenever children are involved as victims so as to make the justice process a more positive experience. Ensure that the Justice for Children strategy being developed by the National Council on the Administration of Justice includes OCSEA-related issues and child-friendly reporting procedures.

2.5. Create formal mechanisms for the sharing of evidence from OCSEA cases between civil society organisations and the police. This will ensure that frontline workers are not forced to develop workarounds which may be problematic or illegal.

Caregivers, teachers, medical staff and social support services

2.6. 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.

2.7. 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. Our 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.

2.8. Try not to restrict children's internet access as a response to potential harm. Restricting access to technology is seen as a punishment. It only protects 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.

2.9. 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/pastoral care staff in schools as well as health workers, additional to all those providing psychosocial support (see insight 4).

2.10. Help 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 initially 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.

INSIGHT 3

Among children who were subjected to OCSEA through social media, Facebook and WhatsApp were the most common platforms where this occurred.

Law enforcement

3.1. Improve law enforcement officers' abilities to flag/refer cases of OCSEA to global technology companies.

3.2. Improve officers' ability to report content hosted outside of the country – e.g., on a website. This is most often achieved by an effective hotline having access to hotlines in other countries (e.g., via the INHOPE network), which can then serve a take-down notice on their domestic internet service providers.

Government

3.3. 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 CSAM 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 CSAM.

3.4. Impose legal duties on social media platforms to ensure that there is a strategic and well-funded effort to minimise children's experiences of OCSEA on their platforms. Hold social media platforms legally responsible for facilitating cases of harm against children.

Industry

3.5. Make formal reporting mechanisms within platforms clear and accessible to children and detail 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. Platforms should also work proactively to prevent sexual content from appearing on children's feeds and where relevant adhere to government regulations on how to do so.

3.6. Internet service providers should comply with regulations to filter and remove CSAM. Enforcing this action is vital in keeping children safe online.

INSIGHT 4

The law enforcement, justice and social support systems have inadequate awareness, capacity and resources to respond to cases of OCSEA.

Government

4.1. 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. Address child protection issues including OCSEA in basic training and provide specialist training more widely. Provide both initial and refresher training.

4.2. Provide adequate and sustainable funding for all agencies involved in tackling OCSEA such as the Department of Children's Services, Anti-Human Trafficking and Child Protection Unit, and Childline Kenya.

4.3. Support the National Police Service in establishing 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. Increase the expertise, resources and staff of the AHTCPU to ensure a presence in more counties/within the 11 regions. Strengthen the links between the AHTCPU and the police stations at the county level for guidance. Make sure that officers trained in handling OCSEA cases are not transferred to other units without a suitable replacement.

4.4. Provide psychological support to all those working with victims of OCSEA, including probation officers, Department of Children's Services workers, prosecutors, magistrates, lawyers, social workers, mental health professionals and personnel of the AHTCPU.

4.5. Ensure that the arrangements for child-friendly justice envisaged in the Children Act are implemented consistently in all cases of child sexual exploitation and abuse crimes, including those with online elements. This will require financial resources, operating procedures and training.

4.6. Operationalise the Victim Protection Trust Fund to provide victim support services (including counselling and medical care) where there are no pro bono services available, and to meet victims' logistical expenses during the criminal justice process.

4.7. Expand access to legal aid to ensure more child victims go through the justice system with a lawyer. The Children Act entitles every child to legal support at the expense of the State. To achieve this, however, both funding and the awareness of victims of their right to legal aid need to be increased. The Department of Children Services may coordinate.

Law enforcement

4.8. Improve data collection and monitoring of OCSEA cases both in the AHTCPU and all police stations in Kenya. It is advised to identify and record OCSEA indicators (i.e. was there a technology element involved) in all case records related to child sexual exploitation and abuse at both the AHTCPU and police stations in Kenya with breakdowns of victim's and offender's characteristics.

4.9. Train all police officers and prosecutors, especially at the county and sub-county 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.

4.10. Guidelines for police officers should be adapted to incorporate best practice on interviewing children during the criminal justice process. This will prevent children from being interviewed repeatedly, which can feel like a form of secondary victimisation. As in the AHTCPU, investigators could record the interviews and share a copy of the interview with the prosecutor and the court instead of arranging multiple interviews.

4.11. Ensure that police officers/prosecutors/courts have a standard information package to provide to all victims and their caregivers related to child sexual exploitation and abuse (including OCSEA) to ensure that all the relevant procedures and rights, including their right to compensation, are clearly explained. The National Council of Children's Services could be mandated to develop such a package. This will enable child victims to make informed decisions as well as familiarise them with the upcoming procedures.

4.12. Maintain the connection to INTERPOL's Child Sexual Exploitation (ICSE) database. Improve the availability and speed of the internet connections at the Nairobi Anti Human Trafficking and Child Protection Unit (AHTCPU) and connect the Mombasa AHTCPU to the internet and the ICSE database. Ensure the units have the necessary Triage tools to deal with CSAM. Mobilise resources with the Ministry of Interior in conjunction with the Treasury to sustain the AHTCPU project.

4.13. 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.

4.14. Law enforcement to strengthen collaboration with social services. Law enforcement should seek to collaborate with social services whenever possible, to ensure a victim-centered justice process.

Justice professionals

4.15. Train all justice actors, including prosecutors and judges, on how to handle OCSEA cases and deliver child-friendly justice as dictated by the Children Act.

4.16. Limit the duration of criminal court cases that include child victims. OCSEA cases must be processed and adjudicated without undue delays to secure digital evidence and protect the child's wellbeing. Courts could grant priority to cases involving children when scheduling hearings, or the Children Act could be amended to limit the duration of cases.

4.17. Develop and implement programmes preparing the child victim to engage with the court system and legal actors.

4.18. Ensure that child victims do not have to face the offender – for example, by employing video-link technology so that evidence may be given from another room. The court methods used in the Barnahus model[162] 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).

4.19. 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.

Social support services

4.20. Train all staff on the frontline of social support services (not just specialist services) to recognise the unique risks and harms of OCSEA, and provide them with evidence-based best practices for responding. When children are brave enough to seek help, those they seek help from must be equipped to provide it.

4.21. 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 not sufficient. Other social support services need online means of access, and support from young, trained staff who understand the way children engage in their online lives.

Industry

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

A further consideration from the data

During the *Disrupting Harm* research activities, respondents expressed concern that requests for informal payments and corrupt influences on judicial processes constitute serious barriers to formal reporting and obstruct access to justice in some instances.

[162] See: Child-friendly centres for abuse victims: Barnahus.

INSIGHT 5

Important OCSEA-related legislation, policies and standards are not yet enacted in Kenya.

Government

5.1. Integrate OCSEA in other policies addressing violence against children.

5.2. Prioritise the ratification of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography and amend legislation to bring it fully into line with the standards set by the Protocol. This Protocol is relevant to combating CSAM and other crimes related to the sexual exploitation of children. Kenya signed the Protocol in 2000 but is yet to indicate its consent to be bound by its provisions by ratifying it. The Office of the Attorney General, the Kenya Law Reform Commission and the National Council for the Administration of Justice need to be engaged with respect to the amendment of legislation, including all legislation mentioned below.

5.3. 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 CSAM.

5.4. Consider amending legislation to conform to other international conventions which offer good guidance for addressing OCSEA, such as the Council of Europe's Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) and Convention on Cybercrime (Budapest Convention). These conventions provide useful measures of national legal frameworks related to OCSEA and are open for accession by states which are not members of the Council of Europe.

5.5. Ensure data retention and preservation policies are in place to support law enforcement authorities in criminal investigations.

5.6. Adopt and enforce the upcoming Children Bill 2021 to properly define and criminalise OCSEA in law.

5.7. 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 CSAM and share it with the offender).[163]

5.8. Amend legislation to explicitly criminalise the live-streaming of child sexual abuse and sexual extortion committed in the online environment. The Computer Misuse and Cybercrimes Act is a milestone in Kenya's fight against OCSEA, as it provides the procedural rules needed to assist law enforcement officers in the investigation of OCSEA cases. However, it does not explicitly criminalise knowingly obtaining access to CSAM or any forms of OCSEA other than conduct related to CSAM.

5.9. Take the necessary steps to support the effective implementation of the National Plan of Action Against Sexual Exploitation of Children in Kenya, 2018-2022 and the National Information, Communications and Technology Policy (2019). The National Council of Children's Services and Department of Children's Services can take the lead on this. These steps should include the dissemination of these policies to relevant implementing agencies and the allocation of the budgets needed for implementation and regular monitoring of progress.

5.10. Ensure that the programmes and solutions foreseen by the National Plan of Action on online child sexual exploitation and abuse and the National Strategy on Child Online Protection complement each other.

[163] The Lanzarote Committee recommended 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, INTERPOL, and UNICEF Office of Research – Innocenti have greatly appreciated the unique opportunity to work shoulder-to-shoulder to assess OCSEA in Kenya. This comprehensive report is the result of a two-year collaborative effort to design research, gather data and produce extraordinary evidence. These efforts would not have been successful without the engagement of so many individuals and partners in Kenya. The project partners would like to express their appreciation to everyone who engaged with *Disrupting Harm* by:

Contextualising the findings: The African Union, Child Fund Kenya, Childline Kenya, the Communication Authority (KE-CIRT and Consumer Affairs Division), CRADLE, the Department of Children's Services of the Ministry of Labour and Social Protection, the Directorate of Criminal Investigation – Anti-Human Trafficking and Child Protection Unit (AHTCPU), Eveminet Communications Solutions Limited, HAART Kenya, Hope in Life, the Kenya Alliance for Advancement of Children (KAACR), the Kenya Films Classification Board, the Kenya Institute of Curriculum Development under the Ministry of Education, the Kenya Law Reform Commission, Ladder of Hope Kenya, Love Justice International, the Ministry of ICT, Information and Youth Affairs, Missing Child Kenya, Mtoto News, the National Council for the Administration of Justice – Special Taskforce on Children Matters, the National Council for Children's Services, the Office of the Director of Public Prosecutions, the Judiciary, Plan International Kenya, Save the Children Kenya, Solidarity with Girls in Distress, Terre des Hommes, Trace Kenya, UNICEF Eastern and Southern Africa Regional Office, UNICEF Kenya, Watoto Watch Network.

Supporting data collection: Child Helpline International, Directorate of Criminal Investigation – Anti-Human Trafficking and Child Protection Unit (AHTCPU), the Kenya Alliance for Advancement of Children (KAACR), the International Association for Internet Hotlines (INHOPE), the Internet Watch Foundation (IWF), INTERPOL National Central Bureau (NCB) Nairobi, Ipsos Kenya, Ipsos MORI, Missing Child Kenya, Awareness Against Human Trafficking (HAART), UNICEF Eastern and Southern Africa Regional Office, UNICEF Kenya.

Sharing expertise and experiences through interviews and survey responses: African Network for Prevention and Protection of Child Abuse and Neglect, Childline Kenya, the Child Rights Network, Child's Life, the Coalition on Violence Against Women, community volunteer officers, CRADLE, Department of Children's Services, Directorate of Criminal Investigations, Eveminet Communications Solutions Limited, Facebook, Hope in Life, the Kenyan Police – Child Protection Units, Kesho Kenya, Ladder of Hope Kenya, Love Justice International, members of the Judiciary, International Justice Mission, Missing Child Kenya, Mtoto News, Solidarity with Girls in Distress, Stop the Traffik Kenya, teachers of the Ministry of Education, Terre Des Hommes Netherlands, Trace Kenya, UNICEF Kenya, Watoto Watch Network,

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.

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