DISRUPTING HARM

safeonline.global/disrupting-harm/

DATA INSIGHT 7

THE ROLE OF SOCIAL MEDIA IN FACILITATING ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE

unicef Office of Research-Innocenti

About the *Data Insights* series from *Disrupting Harm*

Disrupting Harm is a research project conceived and funded by Safe Online. The project is implemented by ECPAT, INTERPOL and UNICEF and generates national evidence on online child sexual exploitation and abuse. This publication is part of a series of thematic briefs that explores pressing issues emerging from the research and recommends ways for key entities and individuals to improve prevention and response.

So far, new evidence about online child sexual exploitation and abuse has been collected through *Disrupting Harm* in thirteen countries: seven in Eastern and Southern Africa (Ethiopia, Kenya, Mozambique, Namibia, South Africa, Tanzania, Uganda), and six in Southeast Asia (Cambodia, Indonesia, Malaysia, Thailand, the Philippines, Viet Nam). Up to nine primary research activities were undertaken in each country including surveys and interviews with more than 13,000 children, as well as caregivers, and other professionals with child protection mandates. Thirteen country reports were published in 2022, presenting the consolidated findings of all activities conducted within each country, along with targeted recommendations developed together with national stakeholders. Country reports can be found here.

Data collected by ECPAT, INTERPOL and UNICEF are used as the basis for the *Disrupting Harm* Data Insights series. Authorship is attributed to the organisation(s) that produced each brief. While the *Disrupting Harm* project is a close collaboration between ECPAT, INTERPOL and UNICEF, the findings, interpretations and conclusions expressed in this publication are those of the authors and do not necessarily reflect the views of the three organisations ECPAT, INTERPOL and UNICEF, individually or as a collaborative group.

Introduction

Along with the rapid rise in internet access and use in low- and middle-income countries, the use of social media and instant messaging apps has proliferated among children and adolescents. These apps allow children to socialise and stay in touch with friends, to gain access to information, and to express themselves creatively. However, these same platforms which benefit and are enjoyed by children are also being used to harm them.

Case studies of law enforcement cases conducted as part of *Disrupting Harm* in specific countries, highlight various ways in which abusers and facilitators[1] are using social media and instant messaging apps to gain access to children, to collaborate with other perpetrators, and to transmit child sexual abuse material.[2,3]

Abuse can occur directly on social media platforms, for example by coercing a child to share sexual images or to engage in sexual acts, but can also be used by perpetrators to contact children and convince them to meet in person, bypassing some of the safeguards usually provided by caregivers and teachers in non-virtual environments. As one *Disrupting Harm* research participant from the National Prosecuting Authority in South Africa said, "[Parents] are not aware that the children in their house are being groomed, with the house alarm on and the guard dog outside." (RA4-J-SA-08-A) Social media and instant messaging apps can also be used by people the child already knows as another avenue for perpetrating abuse.

Understanding how online child sexual exploitation and abuse occurs on social media and instant messaging platforms is a complex issue as these services can be used in different and fast-evolving ways to harm children.

Defining online child sexual exploitation and abuse

Situations involving *digital, internet* and *communication technologies* at some point during the continuum of abuse or exploitation. It can occur fully online or through a mix of online and in-person interactions between offenders and children.

[1] In addition to abusers who commit sexual offences against children directly, offenders of online child sexual exploitation and abuse also include individuals who facilitate the commission of sexual crimes against children. It is also possible for an offender to move across these categories or be operating simultaneously as both an abuser and a facilitating offender.

[2] ECPAT, INTERPOL, and UNICEF. (2022). Disrupting Harm in the Philippines: Evidence on online child sexual exploitation and abuse. Global Partnership to End Violence Against Children.

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

Funded by Safe Online

Understanding the nuances of how these platforms can be used to perpetrate or facilitate abuse requires gathering and analysing data from multiple perspectives, including from service providers themselves. Nationally representative data coming directly from children provide a robust understanding of where child sexual exploitation and abuse is happening on social media and who the perpetrators are. Some service providers publish transparency reports periodically and highlight the number (and nature) of policy violations on their platforms, as well as how those violations were actioned. While this is a good step towards greater transparency, data made publicly available by social media platforms remain scarce and are less comprehensive.[4] This remains a major gap in the understanding of online child sexual exploitation and abuse.[5]

Data and analysis

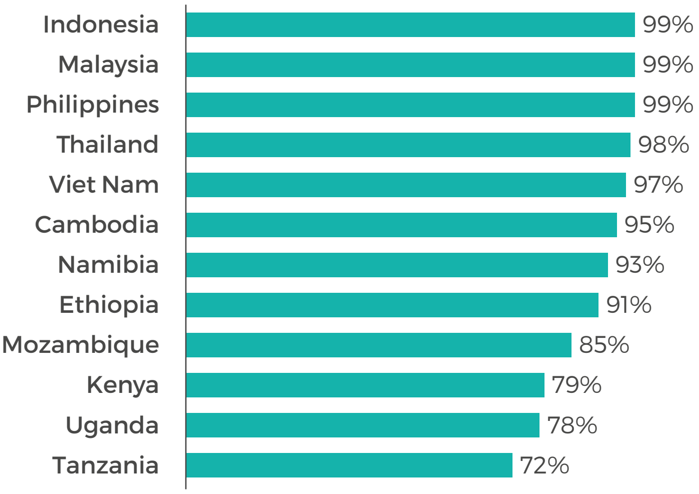
The first section of this Data Insight presents survey data on children's use of social media and instant messaging apps, and their self-reported experiences of sexual exploitation and abuse on social media platforms. The analysis is based on data from a sample of around 12,000 internet-using children living in 12 different countries, collected via nationally representative household surveys in each of the countries.[6]

The second part of this Data Insight includes data about reports of suspected child sexual exploitation made to the National Center for Missing and Exploited Children (NCMEC) (based in the United States of America) by electronic service providers. The *Disrupting Harm* research team analysed NCMEC reports from 2017 to 2019, which are included in the individual 13 *Disrupting Harm* country reports. However, for the purpose of this Data Insight only the most recent NCMEC data analysed by *Disrupting Harm* (for 2019) are presented.

Children's experiences of sexual exploitation and abuse on social media

Social media and messaging apps are a key part of children's internet use. Most 12–17 internet-using children in all 12 countries had used a social media or instant messaging app at least once in the month prior to the survey (Figure 1). While these platforms can be useful to children in many ways, they also come with a variety of risks, with online sexual abuse and exploitation being one of the most concerning.

Figure 1: Children who have used social media or instant messaging apps in the previous month.



Base: internet-using children aged 12–17 years.

The analysis in this portion of the Data Insight focuses on children who were subjected to the following forms of online sexual exploitation and abuse in the past year, prior to the survey:

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

[4] The Tech Coalition has developed a Framework to guide tech companies on metrics and data that could be provided in their transparency reporting. See: Tech Coalition. (2022). Trust: Voluntary Framework for Industry Transparency. Tech Coalition.

[5] For examples of current efforts being made by some online service providers to keep users safe, see: eSafety Commissioner. (2022). Basic Online Safety Expectations: Summary of industry responses to the first mandatory transparency notices. eSafety Commissioner.

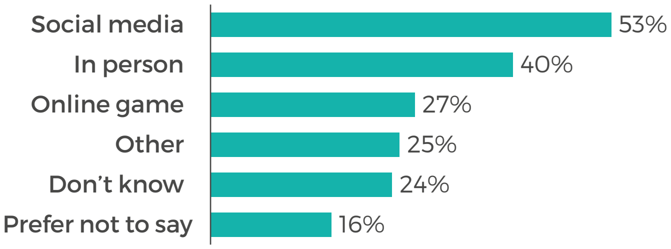
[6] Household survey data were collected from December 2020 to November 2021. The sample in each country was a stratified random cluster sample with random walk within clusters. Children were randomly selected at household level if they were between the ages of 12 and 17 years and had used the internet at least once in the three months prior to data collection. The sample size in each country was about 1,000 12–17-year-olds and 1,000 of their caregivers.

Funded by Safe Online

Each of the forms of violence listed above involve the use of technology in one way or another. For example, sending sexual images involves the use of digital technology to take the images and/or share them. Being offered money or gifts *online* to then meet *in person* or receiving threats online to engage in sexual activities also involve the use of digital technologies at some point in the continuum of sexual abuse or exploitation of a child.

We asked children who were subjected to the various forms of online sexual exploitation and abuse above how they were targeted the last time it happened (i.e., in person, online through social media or online games, or both). As shown in Figure 2, among all the children who were subjected to any of the forms of violence listed above, 53% said this happened on a social media app. Yet, a substantial proportion of children (40%) said that they were targeted in person. This highlights the spillages between sexual violence that occurs through the virtual and the physical environments, which are sometimes seen as two mutually exclusive spaces. Other *Disrupting Harm* analysis shows that only a very small proportion of internet-using children experienced online sexual exploitation and abuse without also experiencing some form of sexual violence in person.[7] The overlaps between online and in-person sexual abuse against children suggest that efforts to prevent online child sexual exploitation and abuse should be integrated within the wider systems that prevent and respond to child sexual abuse.

Figure 2: Proportion of children subjected to online sexual exploitation and abuse in the following ways.



Base: Internet-using children aged 12–17 years who were subjected to online sexual exploitation and abuse in the past year prior to the survey. This was a multiple-choice question, so responses add up to more than 100%.

Figure 3 shows the most common platforms where children who experienced sexual exploitation and abuse on social media said that it happened to them. The results show that Meta-owned platforms were the most common apps where children experienced sexual exploitation and abuse. Facebook/Facebook Messenger were the most common in all countries analysed.[8] This was usually followed by WhatsApp. YouTube, Twitter (now called X) and TikTok also featured in children's responses, but much less frequently. While this is likely a reflection of the relative popularity of these platforms, it highlights that service providers – particularly those with a large user base – need to do more to protect children.

Figure 3: Percentage of children in each country who experienced online sexual exploitation and abuse on a given app (only the top three social media and instant messaging apps presented per country)

	Facebook	WhatsApp	YouTube	TikTok	Twitter	Instagram	Telegram	Snapchat
Ethiopia	75%				14%		26%	
Kenya	84%	64%	19%			19%		
Mozambique	95%	37%		9%				
Namibia	92%	46%				40%		
Uganda	91%	34%	13%					
Cambodia	96%		16%	29%				
Philippines	97%		8%	10%	10%			10%
Thailand	96%			74%	82%			

Base: Internet-using children aged 12–17 years who were subjected to sexual exploitation and abuse on social media.

[7] UNICEF Office of Research – Innocenti (2022). The Relationship Between Online and In-person Child Sexual Exploitation and Abuse. *Disrupting Harm Data Insight 6*. Global Partnership to End Violence Against Children.

[8] Countries where the sample size was too small were excluded for this analysis.

Funded by Safe Online

CyberTips submitted by social media platforms

Beyond data coming directly from children, CyberTipline reports concerning suspected child sexual exploitation and abuse – also known as CyberTips – that are made to the NCMEC can provide some insight into the volume and types of offences being committed and detected. Reports can be made by members of the public, although most reports come from electronic service providers (such as social media platforms). United States federal law requires 'electronic service providers' based in the United States (i.e., technology companies including social media platforms) to report instances of suspected child exploitation and abuse on their platforms to NCMEC's CyberTipline. NCMEC then triages the CyberTips and passes them to the relevant national law enforcement units for action. While NCMEC CyberTips can provide some indication of suspected cases of child sexual exploitation and abuse that occurs on social media, it is important not to view these reports as a full representation of the scope of violations in a given country.

Figure 4 shows the number of reports made by the top three electronic service providers in each country related to suspected child sexual exploitation and abuse in 2019. A common pattern across all *Disrupting Harm* study countries was that the possession, manufacture, and distribution of child sexual abuse material accounted for almost all of the CyberTips from 2019.

As shown in Figure 4, in all countries analysed, Facebook made the highest number of reports, normally followed by either Instagram, Google or Twitter. A high number of reports may reflect the level of content that is being circulated (or re-circulated) on a platform and could also be indicative of a service provider's content moderation capabilities and proactive detection of online child sexual exploitation and abuse. At the same time, it further stresses the responsibility of these social media platforms to ensure that proper safeguards are in place to protect children on their platforms. It is concerning that some electronic service providers do not submit any reports at all to NCMEC.

Figure 4: Top three electronic service providers that submitted CyberTips concerning suspected child sexual exploitation, by country (2019)

	Facebook	Instagram	Google	Twitter	Imgur
Kenya	11,592	770	349		
Ethiopia	14,829	79	133		
Mozambique	4,477	53	124		
Namibia	712	103	60		
Tanzania	5,394	1,050	308		
Uganda	4,662	105	172		
Indonesia	756,084	57,675	22,161		
Cambodia	90,596	132	467		
Malaysia	172,294	6,637	3,045		
The Philippines	795,913		2,627	1,064	
Thailand	34,124		7,280	3,067	
Viet Nam	370,401		7,060		764

Base: Internet-using children aged 12–17 years who were subjected to sexual exploitation and abuse on social media.

Recommended actions

Preventing and responding to online child sexual exploitation and abuse is a shared responsibility among government, industry, caregivers and the wider community. The findings of this Data Insight emphasise that social media platforms – and particularly those most frequently used by children – have more work to do to ensure that children stay safe while using their services, are aware of the risks they may encounter while using social media platforms, and know when and how to seek help. While social media companies are already taking action to prevent and respond to online child sexual exploitation and abuse,[9] the fact that a significant number of children still experience these violations on their platforms shows that more work remains.

Below are some recommendations for government, social media service providers and law enforcement based on the *Disrupting Harm* findings above. However, these are not fully comprehensive and further collaboration among sectors is needed to find effective solutions.

[9] eSafety Commissioner. (2022). Basic Online Safety Expectations: Summary of industry responses to the first mandatory transparency notices. eSafety Commissioner.

Funded by Safe Online

Recommendations for governments:

1. **Embed responses to online sexual exploitation and abuse into existing child protection and violence prevention systems.** The overlap between online and in-person sexual violence suggests these harms should be addressed together.
2. **Make it mandatory for online platforms to have clear, accessible, child-friendly mechanisms for children to report concerns.** These mechanisms should be developed in close consultation with children and young people across all markets to ensure that a wide range of views and needs are considered. In addition, these platforms should detail in child-friendly terms what the process looks like *after* children make a report, and platforms should be mandated to act expediently in cooperation with key actors such as law enforcement officials.
3. **Develop campaigns that teach children and caregivers about possible harms they may encounter on social media and how to identify inappropriate behaviours.** This should include ways to mitigate against those harms and how to seek help directly on the social media platform and through trusted adults. It should be noted that campaigns alone are not sufficient. They should be just one part of a multi-pronged approach towards prevention that accounts for the various social and behavioural drivers of child sexual exploitation and abuse.
4. **Law enforcement should liaise more closely with global technology platforms and build on existing collaborative mechanisms** to ensure that the digital evidence needed in cases related to online sexual exploitation and abuse can be gathered rapidly and efficiently, including in response to data requests, and illegal content is promptly removed.

Recommendations for social media service providers:

5. **Engage in consultations with children and their families** to understand their needs and what would make them feel safe when using social media services, including reporting functions in case of harm. These consultations should be age and culturally appropriate, in addition to being meaningful and safe for children. Use these insights when developing safety mechanisms and when introducing new features on a given service.
6. **Have monitoring and evaluation frameworks in place** to ensure that safety measures used to keep children safe from harm are working effectively and as intended. Metrics should aim to go beyond measuring engagement with certain campaigns but should also focus on lasting behaviour change.
7. **Make formal reporting mechanisms within social media and instant messaging platforms clear and accessible to children.** These mechanisms should be developed in consultation with children and young people and should detail in age-appropriate and child-friendly terms what happens after children submit a report. Platforms and internet service providers must respond rapidly to reports made by children and demonstrate transparency and accountability.
8. All platforms should work towards **strengthening their prevention measures, detection mechanisms and reporting of online child sexual exploitation and abuse.**
9. **Social media platforms and service providers should publish periodic transparency reports.** These should provide information about a company's policies, practices, and processes related to combatting online child sexual exploitation and abuse. It should also include the number of policy violations on their platforms related to suspected cases of child sexual exploitation and abuse, as well as how those violations were actioned.

[10] As per the United Nations Convention on the Rights of the Child, General Comment No. 12, meaningful participation of children and young people must also be: transparent and informative, voluntary, respectful, relevant, child-friendly, inclusive, supported by training, safe and sensitive to risk, and accountable. See more guidance here: Baron, J.G & Friscia, F. Child Consultation and Responsible Business Conduct in the Digital Environment: Rights, Risks, and Opportunities.

Suggested citation:

UNICEF Innocenti – Global Office of Research and Foresight (2023). The Role of Social Media in Facilitating Online Child Sexual Exploitation and Abuse. Disrupting Harm Data Insight 7. Safe Online.© End Violence Partnership, UNICEF, 2023.

Use of this publication is permitted provided that the source is acknowledged and the publication is not used for commercial purposes. Funding from Safe Online does not constitute endorsement.

Funded by Safe Online