weprotect Global Alliance

CPC Learning Network

Columbia | Mailman School of Public Health

Global Threat Assessment 2025

Preventing technology-facilitated child sexual exploitation and abuse: **From insights to action**

Contents

Content note and support resources 3

Executive summary 4

Prevention framework 8

Recommendations 13

Foreword 16

Introduction 17

The SafetyNet Manifesto: Youth voices for a safer digital future 19

The digital landscape 20

Legal and policy landscape 21

Scale and nature of technology-facilitated child sexual exploitation and abuse 22

- Data landscape 22
- Scale and patterns of harm 23
- Characteristics and vulnerabilities of victims and/or survivors 30
- Characteristics and behaviours of people at risk of offending and who have caused harm 31

Prevention 36

- Closing the funding gap 37
- Strengthening the evidence base for prevention 38
- Designing the prevention framework 39
- Putting prevention into practice: The Swiss cheese model 41
- Prevention action areas 43

Conclusion 73

Acknowledgements 74

Staying current with emerging evidence 77

Glossary of terms 79

References 82

Content note and support resources

This report discusses technology-facilitated child sexual exploitation and abuse, including survivor accounts that may be distressing. Some readers may find some sections of the report difficult to read. If this content raises concerns, please refer to the confidential global resources listed here.

You are not alone—support is available.

- Brave Movement, Get Help: Hub of national support helplines.
- Child Helpline International: Country-specific child helplines.
- INHOPE: Global network of hotlines to report child sexual abuse material in your country.
- MOORE | Preventing Child Sexual Abuse, Johns Hopkins Bloomberg School of Public Health: Guidance and resources for individuals seeking help for themselves or someone else to prevent child sexual abuse.
- ReDirection Self-Help Program: Confidential online resource that supports individuals concerned about their sexual thoughts or behaviours towards children.

Executive summary

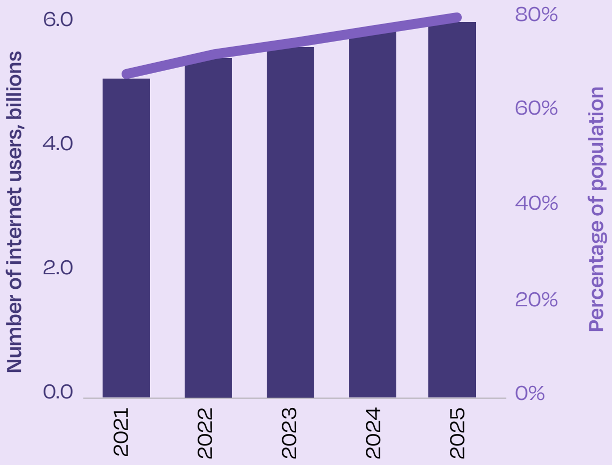
> “The future of our digital world doesn’t have to be scary—it can be exciting and enriching. But we have to approach it with care, responsibility, and transparency. As we step into this new era of AI, we need to make sure the younger generation is not only equipped to navigate these spaces but also empowered to shape them into something better.”

Youth advocate[1]

Technology-facilitated child sexual exploitation and abuse (CSEA) is a complex, global challenge that inflicts profound harm on children, families, and communities. This threat is **preventable, not inevitable.**[2] Tackling this issue requires coordinated, cross-sector action centred on children’s rights, and promising data and strategies are emerging globally. The Global Threat Assessment 2025 takes an action-oriented approach, assessing the current landscape while emphasising prevention and practical measures to keep children safe.

The digital landscape is transforming rapidly, creating new threats to children and challenges for detection and enforcement. Over 6.0 billion people now use the internet, and youth access outpaces the general population.[3,5] More than half of the world’s population now owns a smartphone.[4]

Figure 1. Trends in internet use over the past five years[5]



While digital technologies create opportunities for connection, learning, and expression, they also expose children to new risks. Technology is often an amplifier of harm that cuts across physical, social, and digital spaces. Existing and emerging technologies, such as generative artificial intelligence (AI), encryption, and extended reality, are reshaping children’s digital environments. In just a few years, generative AI, including AI chatbots, have moved from largely experimental, to fully embedded in social media, messaging platforms, and everyday tools that children use.[6] While these developments bring benefits, they also create substantial challenges for prevention, detection, and enforcement. Encrypted platforms enhance user privacy but can also lower barriers to offending against children. They also make it harder to detect, block, and remove child sexual abuse material (CSAM). Civil society experts highlight an ongoing trend in which some offenders initiate contact with children on open platforms before moving interactions to encrypted channels or offline environments with the intent to cause harm. In addition, growing evidence suggests that peer-perpetrated sexual exploitation and abuse appears to be increasing, and exposure to developmentally inappropriate sexual content online may be playing a role.[7–9] Harms caused by peers, classmates, and intimate partners often arise when weak digital safeguards, poor supervision, and limited education about appropriate online conduct and sexual behaviours intersect.[10,11]

Technology-facilitated CSEA continues to expand in scale and complexity, shaped by rapid technological change and systemic gaps. Since 2023, existing harms have largely persisted while new threats have emerged faster than laws, policies, and safeguards can adapt. CSAM is being detected, reported, and removed at record levels. Reliable global prevalence data remain elusive, and caution is needed when interpreting observed trends in reporting, as these often reflect reporting capacity and practices, rather than the true scale of harm. For example, reports to the National Center for Missing and Exploited Children (NCMEC) CyberTipline fell from 36.2 million in 2023 to 29.2 million incidents, associated with 20.5 million reports, in 2024. This decrease is largely attributed to 'bundling' practices, where related reports are grouped together, and end-to-end encryption, which limit detection and reporting.[12]

INHOPE received **2.5 million** suspected CSAM reports in 2024, more than double the previous year.[13]

NCMEC received **20.5 million** reports of suspected child sexual exploitation in 2024.[12]

Internet Watch Foundation (IWF) confirmed almost **300,000** instances of CSAM in 2024.[14]

Generative AI has been used to facilitate the creation and distribution of CSAM at scale, to conceal victim and offender identities, and to circumvent laws and safeguards, such as age verification methods. It has also fuelled new forms of CSEA, including financial sexual extortion and 'deepfake' images depicting real children in simulated sexualised situations. By late 2023, the first AI-generated child sexual abuse images were reported via internet hotlines and their prevalence has since increased exponentially.[15] NCMEC's **CyberTipline** recorded a 1,325% increase in reports linked to generative AI between 2023 and 2024, representing 67,000 reports.[12] This volume strains law enforcement agencies and content moderators.

In the first six months of 2025, more than **440,000** reports of generative AI related to child sexual exploitation were received by NCMEC.[12]

Grooming and online enticement remain prevalent. In 2024, NCMEC documented 546,000 reports, a 192% increase compared to 2023.[12] Experts are also noting alarming intersections between technology-facilitated CSEA and other harms, including suicidal ideation and self-harm, extremism, human trafficking, and financially motivated scams. This emerging phenomenon requires further investigation and remains poorly understood. Financial sexual extortion is a persistent trend that disproportionately impacts boys.

In 2024, NCMEC received approximately **100** reports of financial sexual extortion each day.[12]

Global momentum to address technology-facilitated CSEA is building.

Since 2023, several countries have proposed or passed new legislation addressing the issue. The **U.S. Report Act** of 2024 imposed additional obligations on technology companies, including mandatory reporting to NCMEC in cases that were previously voluntary, and up to USD one million penalties for violations.[16] The UK's 2023 **Online Safety Act** extends new requirements, including risk assessments and age assurance, to hundreds of thousands of online service providers globally that target UK users.[17] In Brazil, two landmark child protection measures in 2025 included a nationwide ban on non-educational smartphone use in schools and new legislation introducing safety by design and reporting obligations for online platforms.[19,20] Australia has adopted a social media age delay, restricting use for children under 16, which is currently being implemented.[18] In Singapore, the telecommunications regulator will soon require age checks to download certain apps on mobile devices—the first such legislation globally.[21] The full impact of this wave of legislation remains to be seen as policies move to regulation and implementation.The **UN Convention Against Cybercrime**, adopted in December 2024 and now moving towards ratification, marks a major milestone in global child protection. For the first time, it makes CSAM and online grooming crimes under international law.[22,23] The **Global Digital Compact**, implemented in 2025, provides a framework for international cooperation, guiding efforts to address online harms and strengthen digital safety.[24]

Notable progress has also been achieved through the adoption of the second edition of the **Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse** (abbreviated to the Terminology Guidelines), the launch of innovative cross-industry partnerships to improve detection and prevention, such as **Lantern**, and large-scale research studies aimed at closing evidence gaps.[25,26] The Safe Futures Hub's **Living Systematic Review** will provide updated evidence, while initiatives such as **Prevention Global** expand knowledge on perpetration prevention and global prevalence.[27,28]

Children's perspectives remain under-represented. Despite some promising approaches to integrate children's perspectives in policy and decision-making, children are often not provided opportunities to meaningfully participate in the policy decisions that affect them. Our review of literature published since 2023 relating to technology-facilitated CSEA found that a minority of publications included children's voices, and very few consulted children on their recommendations for action. The Global Threat Assessment 2025 involved consultations with children to help inform and shape the recommendations presented.

Technology-facilitated CSEA can be prevented, but there is no universal solution. Prevention requires whole-of-society action. The prevention framework presented in this report, complementing WeProtect Global Alliance's Model National Response, offers practical guidance across four interconnected action areas:[29]

- CHILD PARTICIPATION AND LEADERSHIP
- COMMUNITY EDUCATION AND SUPPORT
- DIGITAL SAFETY
- LAW, POLICY, AND JUSTICE

These action areas are mapped across three levels of prevention:

- primary (proactively protect),
- secondary (detect and disrupt harm), and
- tertiary (respond and support after harm has occurred, which can prevent re-victimisation and re-offending).

The framework synthesises emerging evidence, good practice, and expert guidance. It aims to provide an entry point for stakeholders to consider prevention actions relevant to their context and expertise. The action areas are organised to reflect the socio-ecological model, starting with children and progressing through communities, institutions, governments, and global actors.[30] It highlights the layered nature of prevention, where each level reinforces the others. Enablers such as financing and research provide the foundation for all actions and must be proactively addressed and sustained to make prevention possible.

Prevention framework

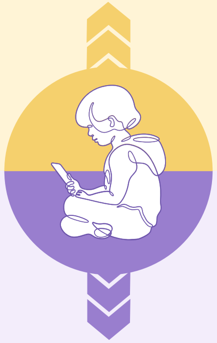
Guiding Principles

Every child has the right to be safe from harm, including sexual exploitation and abuse.
Efforts to prevent technology-facilitated child sexual exploitation and abuse should:

- Uphold children's and survivors' rights and dignity and avoid increasing risks or causing further harm;
- Recognise that children are both at risk of being harmed and of engaging in behaviours that can harm other children;
- Centre the perspectives, needs, and preferences of children and survivors;
- Account for differences in children's ages, development, and other characteristics - such as gender identity, sexual orientation, ethnicity, disability status, migrant status, economic and educational status – that can affect their needs and the risks they face.

Drivers of technology-facilitated child sexual exploitation and abuse

- Lack of protective mechanisms
- Financial motivations
- Weak governance and accountability
- Intersectional vulnerabilities
- Harmful social norms



Enablers of prevention

- Political will
- Strong digital governance and accountability at global, national, and local levels
- Harmonised terminology and data systems
- Global and cross-sector coordination
- Supportive social norms
- Trained child-facing professionals and providers
- Strong child protection systems

Research and Data

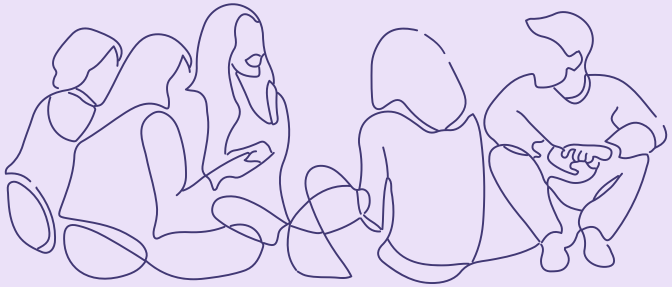
- Use a public health approach to define the problem and prevalence, identify risk and protective factors, design and test interventions, and scale up what works.
- Prioritise research informed or led by children, youth, survivors, and marginalised populations.
- Develop knowledge and good practices in low- and middle-income countries and under-represented contexts
- Share data, knowledge, and good practices across regions and sectors, adapting evidence sensitively to new contexts.
- Conduct cost-benefit analyses to strengthen the case for funding prevention

Sustainable Financing

- Dedicated budget lines in national strategies
- Industry commitments
- Participation of multilateral institutions
- Flexible financing mechanisms
- Cross-sector funding
- Sustainable support for community-based organisations
- Funding for innovation and evidence generation

CHILD PARTICIPATION AND LEADERSHIP

Meaningfully involve children in defining the problems and shaping policies, programmes, and services that affect them.



Primary Prevention **PROACTIVELY PROTECT**	Secondary Prevention **DETECT AND DISRUPT**	Tertiary Prevention **SUPPORT AND RESPOND**
Co-design contextually sensitive education and awareness-raising initiatives with children that reflect how they use technology, whom they trust, and where they turn for help if they are harmed or have concerns about their own thoughts and behaviours.	Partner with child-led and survivor-led organisations to co-design, implement, and evaluate accessible, easy-to-use, and trusted reporting channels, including non-formal channels, such as trained peers.	Use insights and data from both child and adult survivors to improve the accessibility and quality of support services, justice systems, and redress mechanisms. Explore survivors' own concepts of harm, justice, and accountability, including non-formal and restorative justice approaches.

Consult children only when trained staff, safety measures, and support services are in place. Otherwise, consult youth and adults who can represent children's perspectives, including adult survivors.

Create safe, welcoming spaces - both online and offline - for children to share their views, and influence policies, programmes, and services.

Engage children across age groups, genders, and backgrounds, and address barriers to inclusion. Seek input from children who have experienced harm, as well as children who have caused harm.

COMMUNITY EDUCATION AND SUPPORT

Equip children, caregivers, and communities with the knowledge, skills, and tools to keep children safe and appropriately respond to risks and harms. Provide early interventions for children and adults at risk of causing harm.

Primary Prevention **PROACTIVELY PROTECT**	Secondary Prevention **DETECT AND DISRUPT**	Tertiary Prevention **SUPPORT AND RESPOND**
Implement and evaluate evidence-based education and awareness raising initiatives that promote digital safety, reporting, and help-seeking. Ensure they are accessible, available in multiple languages, and delivered across schools, communities, and digital platforms that children use. Teach children how to keep themselves and others safe online and offline, where to seek help, safe adults they can turn to for help, and how to report concerns about their own or someone else's safety or behaviours.	Establish multiple accessible, child-friendly formal and non-formal reporting channels, including helplines, trained peers, and trusted adults who can provide early support and resources. Train peers, caregivers, educators, and service providers to help children stay safe online and offline, and respond appropriately to concerns or reports of harm. Deliver evidence-based early interventions for children and adults at risk of causing or experiencing harm.	Support survivors and ensure they know their rights, options, available services, and actions they can take to protect themselves from further harm, request image removal, and seek justice. Provide trauma-informed, survivor-centred services for both child and adult survivors that address both online and offline harms, promote safety and dignity, and prevent further harm. These should include legal, health, and mental health and psychosocial support services. Provide evidence-based, non-carceral responses for children who have caused harm to rehabilitate and prevent re-offending.

DIGITAL SAFETY

Protect children by prioritising their safety, well-being, and rights in industry culture and the design and development of digital products, services, and infrastructure.

Primary Prevention **PROACTIVELY PROTECT**	Secondary Prevention **DETECT AND DISRUPT**	Tertiary Prevention **SUPPORT AND RESPOND**
Prioritise children's safety, rights, and well-being across all levels of company culture, decision-making, and workforce training. Make Safety by Design the default, integrating child rights impact assessments and due diligence in development processes. Consult children and youth to inform design choices, and ensure safety features are functional, accessible, and equitably available across all locations and languages in which a product or service is offered. Harmonise terminology and transparency reporting metrics to improve comparability across products and services.	Detect and disrupt harmful content and behaviours using real-time tools that respect users' privacy and rights (e.g., hash matching, warning pop-ups, redirection to support services, detection of grooming behaviours and risky financial transactions). Fund and provide mental health and psychosocial support for digital frontline responders.	Provide child-friendly, accessible in-platform reporting channels. These should directly link users to helplines and support services and provide timely feedback. Ensure safe, stigma-free processes for survivors to request takedown of their images. Strengthen transparency and accountability, disclosing material child rights impact of digital products and services in every country where they are available. Collect and share anonymised, disaggregated safety data to strengthen industry-wide and cross-sectoral learning. Collaborate across industry to take down CSAM and other harmful content.

LAW, POLICY, & JUSTICE

Strengthen legal and regulatory systems to prevent abuse, secure justice, and hold duty-bearers accountable.

Primary Prevention **PROACTIVELY PROTECT**	Secondary Prevention **DETECT AND DISRUPT**	Tertiary Prevention **SUPPORT AND RESPOND**
Strengthen, harmonise, and enforce laws and regulations using universal terminology and defining clear duties and sanctions. Consult with survivors, child rights groups, industry, and other stakeholders to align legislation with child rights laws, evidence, and good practice, and enable responsible industry innovation. Design laws that recognise developmental differences between children and adults, emphasise rehabilitation of children who cause harm, and avoid criminalising mutually desired behaviours between close-in age peers. Establish national/regional regulators with the power, resources, and technical expertise to set standards, monitor compliance, and ensure strong industry oversight and accountability.	Establish proactive systems to detect, investigate, and respond to technology-facilitated CSEA, rather than relying solely on survivor reports. Require financial institutions to actively detect and report transactions linked to sexual exploitation of children. Establish accessible, child-friendly, trauma-informed reporting channels linked to support services, and provide clear information about where people should make reports or seek help in their country.	Train law enforcement, judiciary, and prosecutors in child-friendly, trauma-informed, survivor-centred processes that uphold children's rights, dignity, and best interests. Establish anonymised national victim databases to inform prevention and response. Use evidence-based monitoring and rehabilitation to prevent re-offending. Treat children in conflict with the law in line with international child justice standards. Use rehabilitation, diversion, and alternative sentencing. Avoid detention, registration, and notification.

Recommendations

The recommendations emerging from the Global Threat Assessment 2025 underscore the need for coordinated global action to prevent technology-facilitated CSEA. Together, they outline a comprehensive, multi-sector approach to protect children both online and offline.

Cross-cutting recommendations for all stakeholders

1. **Address technology-facilitated CSEA as an urgent public health priority and invest in prevention strategies, including those to prevent perpetration and reduce the stigma associated with help-seeking and disclosure.** Recognise that children are at risk both of being harmed and of engaging in behaviours that cause harm to other children.
2. **Generate and use evidence to inform prevention.** Safely and ethically engage children and survivors to define the problem and identify barriers to the inclusion of marginalised populations.
3. **Collaborate across sectors to coordinate prevention efforts and share lessons learned.** Adopt harmonised terminology aligned with the Terminology Guidelines, standardise reporting metrics/systems, share timely data and evidence of what does and does not work, and establish sustainable systems.[26]

Civil society organisations, including international NGOs

1. **Create safe, inclusive spaces for children and survivors to share their views and influence prevention and advocacy efforts.** Make efforts to engage marginalised children, including children with disabilities, sexual and gender minority populations, rural and out-of-school children, children from ethnic minority or migrant backgrounds, and children who lack access to digital technologies.
2. **Advocate for rights-based prevention and response and robust accountability mechanisms to address technology-facilitated CSEA.**
3. **Strengthen community-based reporting and support services, including helplines and peer supporters.** Train caregivers, educators, and service providers to provide early, non-judgmental support and resources; and deliver survivor-centred, accessible services for child and adult survivors that address both online and offline harms, promote long-term well-being, and prevent re-victimisation.
4. **Deliver evidence-based early interventions for children and adults at risk of causing or experiencing harm**, and provide evidence-based, non-carceral responses for children who have caused harm.

Private sector, particularly technology companies

1. **Prioritise children's safety, rights, and well-being across all levels of company culture, decision-making, and workforce training.** Provide continuous education and training across the recruitment pipeline, invest in prevention research and survivor support services, and ensure frontline digital responders and Trust and Safety teams are well supported and resourced.
2. **Make safety by design the default, integrating child rights impact assessments and due diligence into development processes.** Safely consult children, youth, and survivors to inform design choices. Ensure safety features are functional, accessible, and equitably available across all geographic regions and languages where a product or service is offered.
3. **Strengthen transparency and accountability.** Disclose all material child rights impacts associated with digital products and services through existing corporate reporting frameworks in each country of operation.[31] Collect and share anonymised, disaggregated safety data with researchers, regulators, and across sectors to inform prevention. Embed independent accountability mechanisms within corporate governance.
4. **Proactively detect and disrupt harmful content and behaviours.** Use real-time, rights-respecting tools, such as hash matching, monitoring, warning pop-ups, redirection to support services, and detection of grooming behaviours and high-risk financial transactions. At the same time, provide child-friendly, accessible reporting channels. These should directly link users to helplines and support services and result in timely feedback and responses, including the rapid takedown of harmful content.

Academia and researchers

1. **Prioritise research on the prevalence, risk and protective factors, and systemic drivers of technology-facilitated CSEA.** Address critical research gaps, including intersectional vulnerabilities, online–offline escalation, and effective perpetration prevention strategies, including addressing the onset of harmful sexual behaviours amongst children and youth.
2. **Develop, adapt, and evaluate interventions across settings and populations.** Partner across sectors and conduct cost-effectiveness and implementation research to guide sustainable investments.
3. **Establish joint research partnerships, coordinate research agendas, and promote timely data sharing.**

Governments

1. **Review, strengthen, and harmonise global laws and regulations to address technology-facilitated CSEA.** Consult widely with stakeholders to align legislation with evidence, good practice, and child rights laws and standards. Use harmonised terminology and ensure legislation is technology-neutral, covering both existing and future technologies. Define clear duties, sanctions, and accountability mechanisms for duty-bearers, while enabling responsible industry innovation. Differentiate between adults' and adolescents' behaviours and avoid criminalising mutually desired behaviours between close-in-age peers.

2. **Resource and coordinate national child protection and justice systems to address harms to children both online and offline.** Establish multiple accessible, child-friendly, and trauma-informed reporting channels linked to comprehensive health, psychosocial, and legal services. Maintain secure, anonymised victim databases to guide prevention and response. Train law enforcement, judiciary, educators, and frontline workers in child-friendly, trauma-informed practice and provide ongoing support for their well-being.
3. **Use evidence-based monitoring and rehabilitation to prevent reoffending and prioritise support, diversion, and alternative sentencing for children in conflict with the law.**
4. **Establish independent national or regional regulators with the authority, resources, and technical expertise to address technology-facilitated CSEA**, including setting standards, monitoring compliance, and applying sanctions.
5. **Implement and evaluate evidence-based national education and awareness programmes that aim to promote digital safety, reporting, and help-seeking.** Integrate age-appropriate education into school curricula, and train teachers, caregivers, and service providers. Deliver accessible, multi-lingual education and awareness campaigns, collaborating with communities and other sectors to reach marginalised children.

Intergovernmental organisations

1. **Facilitate cross-border law enforcement cooperation and intelligence-sharing.**
2. **Provide technical assistance and mobilise resources to strengthen national capacity,** prioritising based on need and prevalence.
3. **Mobilise pooled and sustainable financing** to support national governments, community-based organisations, and innovative prevention initiatives.

Foreword

“My images have been traded online for over 20 years. I'm a victim of CSAM every day of my life. I was abused as a young child when my first offender created my CSAM. Every week since then, my lawyers get new notices that my material is found in another paedophile's collection. I went to the Supreme Court of the United States and back on this issue over a decade ago with my lawyers at the Marsh Law firm.

My CSAM series is so popular that I know the distribution will never end. But not all victims of CSAM need to be confined to this same fate. The technology to intervene, detect, and stop the spread of CSAM is out there. We must make big tech use it.

I was a teenager when I found out my CSAM was being traded worldwide. Back then, I was one of a handful of victims of this heinous crime. Today, there are...[hundreds of millions of] children victimised every year.

Now, I am raising a teenager in a world that is getting more and more dangerous every day. It's incredibly difficult navigating parenting young kids through this toxic tech era. How do I make sure my kids never encounter my CSAM when it's literally all over the internet? How do I keep my kids safe from predators when I know they're only ever two clicks from harm?

I'm incredibly proud to see victims like myself—and parents like myself—taking on big tech companies. But to be clear: we are going to need innovative research, cutting edge law enforcement tools, and endless support from dedicated advocates to stand a chance. I don't know how we are going to hack it but I know we owe it to all children to not give up.

I don't have any answers for how we keep kids safe online these days but I do know this: WeProtect [Global Alliance] has been a lifeline for survivors in this fight for our kids' lives. Because of this network of support, I finally see the light at the end of the tunnel. The CSAM problems online are getting worse every day and the accountability gap is getting larger. But, schools are banning phones, tech companies are waking up, age verification is on the rise, support systems are expanding, and survivors everywhere are bravely speaking out.

We are finally moving in the right direction.”

This statement was provided, with the support of Protect Children, by a survivor who, like many others, has chosen to remain anonymous. WeProtect Global Alliance invited this anonymous contributor to share their voice alongside many others with lived experience—whether of the children we seek to protect in the digital world or of survivors of technology-facilitated sexual abuse—because such voices are too often unheard. In this Global Threat Assessment, we weave these lived experiences throughout the evidence and research, grounding our work in people's reality. We recognise that these voices are complex, diverse, and sometimes in disagreement, but they must be heard.

Introduction

Aims

Technology-facilitated child sexual exploitation and abuse (CSEA) is a complex, global challenge that profoundly harms children, families, and societies. Preventing and responding to this harm requires urgent, coordinated action across sectors and borders.

The Global Threat Assessment 2025 has two aims:

1. To analyse global trends in technology-facilitated CSEA since 2023.
2. To co-design a prevention framework with expert stakeholders, youth advocates, and survivors, providing actionable recommendations aligned with WeProtect Global Alliance's Model National Response.

The Global Threat Assessment 2025 emphasises the need for context-sensitive approaches. Children's risks, their access to digital technologies and protective resources, and the strength of protection systems vary widely across regions. The report reveals important protection gaps, highlighting the urgent need for equity in global prevention efforts, particularly to protect children in underregulated or resource-limited settings.

A child rights framing

> “Youth should have the right to understand their rights online. Acknowledging these rights would already be a step forward to getting themselves out of dangerous situations.”

14-year-old female, Canada[32]

Prevention of technology-facilitated CSEA is a legal and ethical imperative grounded in international human rights law. The United Nations (UN) Convention on the Rights of the Child requires states to protect children from all forms of violence, exploitation, and abuse. General comment No. 25 confirms that these rights extend to digital spaces and requires governments to integrate children's rights into digital policy, ensure access to justice, and consult with children on decisions that affect them.[33,34] While the Convention on the Rights of the Child establishes obligations for states as duty-bearers, the UN Guiding Principles on Business and Human Rights, and Children's Rights and Business Principles set out the private sector's responsibility to respect children's rights and to prevent and respond to rights abuses.[35,36] These principles underpin this report's analysis of global trends and inform the prevention framework and recommendations that follow.

Note on terminology

In 2025, a global Interagency Working Group updated the Luxembourg Guidelines, releasing the second edition of the **Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse** (abbreviated to the Terminology Guidelines).[26] Consistent with these guidelines, this report uses the term 'technology-facilitated child sexual exploitation and abuse (CSEA)'. **Technology-facilitated CSEA** refers to the use of digital technologies at any stage to prepare, commit, or disseminate (in the case of child sexual abuse material, or CSAM) the sexual exploitation or sexual abuse of a child. It encompasses harms committed in both digital and non-digital (offline) environments – including, for example, exchanging information, coordinating actions, and contacting children to groom or coerce them. This term acknowledges that technology plays a role in facilitating abuse, and perpetuating the harms caused by abuse, in both physical and digital spaces.

A **child** refers to anyone under 18 years of age. Children, including adolescents, differ based on characteristics such as age, developmental stage, sexual orientation, gender identity, disability status, ethnicity, educational background, economic situation, and migration status. These intersecting factors may affect the risks and harms that children face, and their access to protective resources. A **survivor** is a person who has experienced sexual exploitation or abuse. Many survivors of technology-facilitated CSEA are now adults who should also be included in prevention and response efforts. Recognising that people with lived experience use different terms to describe themselves, this report uses **victim** and **survivor** interchangeably.

Methodology

This report draws on a wide range of data sources and expertise. It was guided by an Expert Steering Committee of 14 representatives from government, law enforcement, the private sector, civil society, academia, international organisations, and lived experience advocates.

Evidence was synthesised through:

- A scoping review of academic and grey literature related to the two report aims, published in English between January 2023 and October 2025.
- Semi-structured interviews with 32 stakeholders from across sectors and regions from June to July 2025, to triangulate perspectives and address gaps in the literature.
- An online survey with 77 experts in September 2025 to seek multi-sector perspectives on prioritising prevention actions.
- Insights from four youth and survivor workshops led by survivor- and youth-focused organisations. Survivors also reviewed the interview and focus group guides to ensure relevance and sensitivity.
- Case studies shared by organisations and WeProtect Global Alliance members, showcasing promising practices and innovative responses.

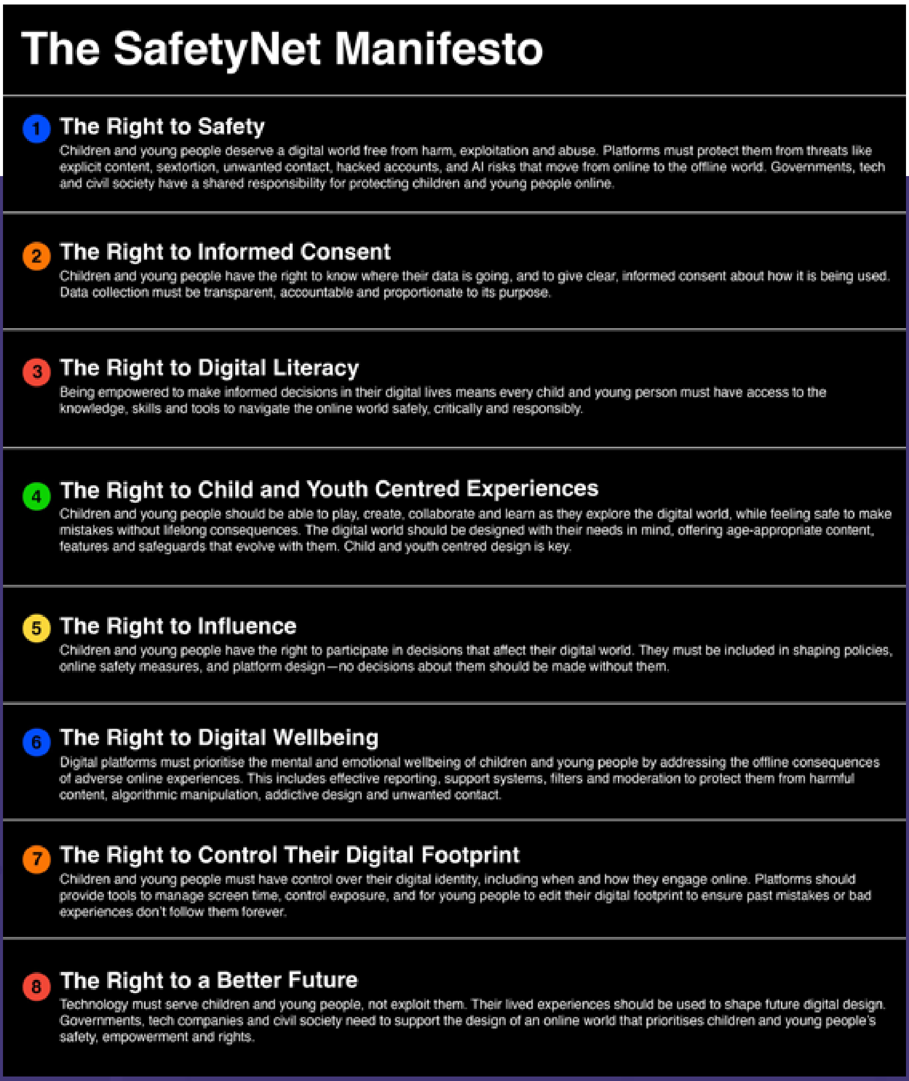
Geographic diversity was ensured through the selection of stakeholders, good practice examples, and case studies, with particular attention to under-represented regions and contexts. The prevention framework was co-created and reviewed through participatory processes that built on this diversity and representation.

Limitations include the restriction to English-language publications, which limits regional representation, the short timeframe for data collection, and potential selection bias in stakeholder and case study inclusion, despite efforts to ensure geographic and sectoral diversity.

The SafetyNet Manifesto: Youth voices for a safer digital future

To better understand how children and young people experience the digital world and imagine a safer online future, WeProtect Global Alliance led the second phase of the #MyVoice#MyFuture project. Through consultations with 109 young people aged 13–24 across 10 countries, and in collaboration with seven youth organisations, the initiative gathered insights on digital safety, rights, and technology-facilitated CSEA. The result is the **SafetyNet Manifesto,** a youth-led declaration of digital rights and a roadmap for building a safer, more equitable digital future. The Manifesto calls for stronger protections, inclusive design, and collective action to ensure that all children and young people can exist online without fear.[37]

Figure 2. SafetyNet Manifesto published on the Safe Futures Hub in June 2025[38]



The SafetyNet Manifesto

1 The Right to Safety

Children and young people deserve a digital world free from harm, exploitation and abuse. Platforms must protect them from threats like explicit content, sextortion, unwanted contact, hacked accounts, and AI risks that move from online to the offline world. Governments, tech and civil society have a shared responsibility for protecting children and young people online.

2 The Right to Informed Consent

Children and young people have the right to know where their data is going, and to give clear, informed consent about how it is being used. Data collection must be transparent, accountable and proportionate to its purpose.

3 The Right to Digital Literacy

Being empowered to make informed decisions in their digital lives means every child and young person must have access to the knowledge, skills and tools to navigate the online world safely, critically and responsibly.

4 The Right to Child and Youth Centred Experiences

Children and young people should be able to play, create, collaborate and learn as they explore the digital world, while feeling safe to make mistakes without lifelong consequences. The digital world should be designed with their needs in mind, offering age-appropriate content, features and safeguards that evolve with them. Child and youth centred design is key.

5 The Right to Influence

Children and young people have the right to participate in decisions that affect their digital world. They must be included in shaping policies, online safety measures, and platform design—no decisions about them should be made without them.

6 The Right to Digital Wellbeing

Digital platforms must prioritise the mental and emotional wellbeing of children and young people by addressing the offline consequences of adverse online experiences. This includes effective reporting, support systems, filters and moderation to protect them from harmful content, algorithmic manipulation, addictive design and unwanted contact.

7 The Right to Control Their Digital Footprint

Children and young people must have control over their digital identity, including when and how they engage online. Platforms should provide tools to manage screen time, control exposure, and for young people to edit their digital footprint to ensure past mistakes or bad experiences don't follow them forever.

8 The Right to a Better Future

Technology must serve children and young people, not exploit them. Their lived experiences should be used to shape future digital design. Governments, tech companies and civil society need to support the design of an online world that prioritises children and young people's safety, empowerment and rights.

The digital landscape

Children today are growing up in an age of rapid digital transformation. While the digital environment creates valuable opportunities for learning, connection, expression, and belonging, it can also expose children to significant risks and harms, both online and offline. These opportunities and risks have evolved quickly in recent years, accelerated by the rise of technologies including generative Artificial Intelligence (AI), extended reality (XR) environments, decentralisation, quantum computing, and end-to-end encryption, which have challenged the ability to prevent, detect, and respond to technology-facilitated CSEA.[39]

Children are more connected than ever, but digital inequities persist. [40] There are now 6.0 billion internet users – about three fourths of the world's population – up from 64% in 2021.[5] More than half of the global population now owns a smartphone.[4] In some countries in the Global Majority, most web traffic occurs on mobile devices, which are often shared within households or between friends.[41] For example, 88% of web traffic in the Philippines and 85% in Nigeria originated from a mobile device in February 2025.[41]

Youth internet use outpaces the rest of the population by 13%.[42] A global survey of over 380,000 children in 55 countries found that a majority began using a digital device before age 10.[43] In just a few years, AI technologies have moved from largely experimental, to fully embedded in social media, messaging platforms, and everyday tools that children use, such as AI chatbots.[6,44] While AI offers educational and social benefits, it is rapidly amplifying risks and harms to children, including technology-facilitated CSEA. Efforts to harness its potential to protect children lag behind. Findings from the 2025 **Digital Well-Being Index** reveal that 80% of surveyed Gen Z teens and young adults reported experiencing some form of online risk.[45] Potential grooming interactions were common, and sharing of intimate imagery was widespread. Additionally, approximately one in four respondents indicated they had encountered AI-generated sexual images, while 25% of participants were unaware that involvement with sexual images of minors is illegal. [45]

While more children worldwide are gaining access to digital technologies, access – and with it, exposure to risks – remains uneven. Nearly half of the six million schools worldwide lack internet access, most of them in Global Majority countries and remote rural areas.[46] Higher socio-economic status has been consistently linked to stronger digital literacy, and the digital divide acts as "an amplifier of broader social exclusions".[47] Children who lack access to digital devices remain at risk, as in-person sexual abuse is often recorded, stored, and disseminated via digital technologies, including shared devices.

Legal and policy landscape

In recent years, governments and international bodies have advanced legislative and policy responses, seeking to harmonise laws, strengthen regulations, and adapt to rapidly evolving technologies. The **UN Convention against Cybercrime** (2024) establishes the first universal standard against cybercrime, explicitly covering crimes against children such as CSAM and grooming, while strengthening international evidence-sharing.[23] The **First Global Ministerial Conference on Ending Violence Against Children** (2024) catalysed multi-sectoral coordination and national pledges to reinforce child protection frameworks including on the subject of online harms.[48] The **Universal Classification Schema Version 3** (2025) provides a harmonised framework for identifying, categorising, and responding to child sexual exploitation and abuse material, with machine-readable labels and globally aligned definitions across borders.[49] The second edition of the **Terminology Guidelines** (2025) provides a foundation of universal terminology to facilitate legal reform.[26] A 'third wave' of legislative reform has emerged across countries, marked by improved harmonisation, including on social media age restrictions, future-proofing, and efforts to close loopholes around emerging harms such as AI-generated child sexual abuse images and sexual extortion.[50] Yet many frameworks to protect children remain fragmented or outdated, with inconsistent regulatory authority and limited protections against first-person generated sexual content involving children or AI-facilitated abuse.[50,51] In some settings, children victimised through sexual extortion still risk criminalisation, reflecting gaps between law, policy, and children's lived realities.[52]

Persistent enforcement and regulatory challenges continue to undermine progress. Cross-border investigations are slowed by jurisdictional fragmentation, uneven resourcing, and weak data-sharing systems. Only 45% of WeProtect Global Alliance's 20 Global Taskforce countries have formal reporting obligations for technology companies.[53] Reliance on voluntary industry measures leaves major accountability gaps, particularly in countries in the Global Majority. Industry representatives argue that voluntary reporting systems can be more agile and responsive, but there is broad agreement among stakeholders that binding obligations are needed.

> “But as businesses, they often don't do it unless they have to.”
>
> *Industry[7]*

Rapid technological shifts are outpacing existing legal tools, and tensions between privacy protections and proactive detection remain unresolved.[39] Stronger international coordination and legislative harmonisation, empowered regulators, increased resourcing of child protection systems and law enforcement, and enforceable industry obligations are required to protect children in the rapidly evolving digital environment.

> “We can't arrest our way out of this problem.”
>
> *Government[54]*

Scale and nature of technology-facilitated child sexual exploitation and abuse

Since the last Global Threat Assessment, existing harms have continued, while new risks have emerged more quickly than legal, policy, and technological safeguards can respond. This chapter brings together available evidence on the scale of abuse, victim and/or survivor characteristics, perpetrator profiles, and emerging threats, recognising that global data remains fragmented, incomplete, and difficult to compare. A number of forthcoming perpetration prevalence studies aim to address existing data gaps (see Appendix). Despite these limitations, the findings provide an important picture of the threat environment from 2023 to 2025 and set the foundation for the recommendations advanced later in this report.

Data landscape

> "The truth is…it's really impossible to give an accurate scale of the issue."
>
> *Industry*[7]

Available data on technology-facilitated CSEA reflect collective progress in coordination, reporting, and monitoring, and are essential for understanding the threat and mobilising action. However, we begin by noting persistent constraints of the data environment, as these challenges frame both the interpretation of available figures and the analysis that follows. Currently available data are fragmented and partial. For example, efforts to measure global prevalence are limited by gaps in geographic coverage, inconsistent definitions, varying strength of detection and reporting systems, and variable study quality. Limited industry transparency also makes it hard to assess what companies are doing: for example, 60% of the top 50 global content-sharing platforms publish no information on how they address child sexual exploitation, and among those that do, data is fragmented and lacks comparability.[55] Available data can both overcount, due to duplication or incorrectly classified material, and undercount, due to encryption and hidden platforms.[7] Robust, representative data on victims and perpetrators remain limited, as discussed later in this chapter. In light of these challenges, we conducted interviews with expert stakeholders and survivor advocates to address evidence gaps and capture up-to-date, context-specific insights on emerging trends and operational challenges. While not a substitute for representative data, triangulating these perspectives with existing datasets and research provides a more comprehensive and nuanced picture.

Scale and patterns of harm

This section outlines key harms shaping the global threat landscape, including CSAM, grooming, livestreamed abuse, AI, violent online extremism, and technological developments such as end-to-end encryption, decentralisation, quantum computing, and XR.

Child Sexual Abuse Material

CSAM is being detected, reported, and removed at unprecedented levels. As previously discussed, reporting trends reflect reporting capacity more than actual prevalence, and most CSAM data originate from high-income platforms, offering a partial view of global harms. It is also important to recognise that upward trends can in part reflect positive developments, such as more children coming forward to report harm, companies improving detection systems, and greater industry transparency in sharing data. Data from various sources, including the National Center for Missing and Exploited Children's (NCMEC) mandatory industry reports, INHOPE's hotlines, and Internet Watch Foundation's (IWF) proactive detection and referrals, serve distinct purposes and use different methodologies, so their figures cannot be meaningfully combined.

Reported figures remain extraordinarily high.

INHOPE: received more than 2.5 million suspected CSAM reports in 2024, a 218% increase from 2023. Of these, 65% were confirmed illegal content. This surge was largely driven by SafeNet Bulgaria, which contributed 1.6 million reports.[13]

NCMEC **CyberTipline**: received 20.5 million reports corresponding to 29.2 million incidents in 2024, down from 36.2 million in 2023. This decrease was partly attributed to 'bundling' practices that group related reports and the impact of end-to-end encryption, which limits companies' ability to detect and report harmful material.[12]

IWF: assessed 424,047 reports, confirming 291,273 instances of CSAM or links to it in 2024—a 6% increase from 2023.[14]

The types of harmful content are diverse and increasingly video based.

NCMEC: nearly 63 million files were reported in 2024, including 33 million videos, 28 million images, and 1.8 million in other formats. Among these, over 51,000 involved children in imminent danger requiring urgent intervention.[12]

IWF: classified 734,048 unique files as CSAM, including 47,000+ videos and 4,000+ prohibited non-photographic images.[14]

Hosting and distribution remain geographically concentrated for content that can be traced. According to INHOPE, 59% of detected servers were located in the Netherlands and 13% in the United States, and these two countries have held the top positions for the past five years.[13] The IWF similarly found that over half of child sexual abuse URLs actioned in 2024 were hosted by European Union member states, with the Netherlands, Bulgaria, and Romania hosting 29%, 9%, and 7%, respectively.[14] Childlight's **Into the Light Index** highlights the high levels of global CSAM hosting traceable to the Netherlands, as well as 4.5 million reports coming just from India, Pakistan, and Bangladesh.[57] A combination of large-scale hosting infrastructure, high-speed connectivity, and regulations that prioritise freedom of speech creates conditions exploited by offenders for storing and distributing abusive content. The location of some content cannot be readily traced because it is hosted on anonymising networks such as Tor, which are designed to conceal the server's physical origin.[11] NCMEC noted that 11% of **CyberTipline** reports had unknown origin in 2024.[58]

Patterns of distribution shifted alongside detection efforts. SafeNet Bulgaria's contribution meant that forums accounted for 61% of reports received by INHOPE in 2024 – up from less than 9% in 2023 – while reports from image-hosting platforms and conventional websites sharply declined.[13] In parallel, the IWF primarily received URLs and confirmed 291,270 webpages containing CSAM in 2024, a 5% increase from 2023.[14]

Grooming and online enticement

Online enticement, often called grooming, is when perpetrators target children using the internet to identify and coerce them into illegal sexual acts. In 2024, NCMEC documented 546,000 reports of online enticement, a 192% increase from 2023, with numbers expected to rise as more companies comply with the **U.S. Report Act**.[16]

Generative artificial intelligence

AI-generated CSAM, flagged in earlier Global Threat Assessments and in key informant interviews, continues to grow at alarming speed.[54] Deepfake technologies (AI-generated images or videos that realistically depict people who never existed or alter real photos and footage), AI chatbots (automated conversational tools that can impersonate children or adults), and generative models (AI systems capable of producing new text, images, or video from learned patterns) are being weaponised to exploit children and disseminate CSAM at scale.[59]

> “If technology can now create images and videos that never actually happened, how will we know what is real in the future, and how will that change the way we trust each other online?”

15-year-old male, Ethiopia[60]

NCMEC: documented a 1,325% increase in AI-related CSAM reports between 2023 and 2024, representing 67,000 reports.[12] By June 2025, preliminary figures show 440,419 new reports involving AI-generated child sexual exploitation content, up from 6,835 during the same period in 2024.[61]

IWF: one forum alone shared over 3,500 digitally altered or synthetic sexually explicit images or videos of children in a single month.[63]

Thorn: 1 in 17 adolescents report being victims of deepfake sexual imagery.[62]

Emerging offender tactics include the use of predictive AI and recommender systems to identify and disseminate CSAM.[63–65] Some offenders share custom AI models trained on real abuse material to generate synthetic content, while others test grooming strategies on child-like chatbots.[8,63,66] At the same time, AI can be deployed to protect children and support detection and investigation.

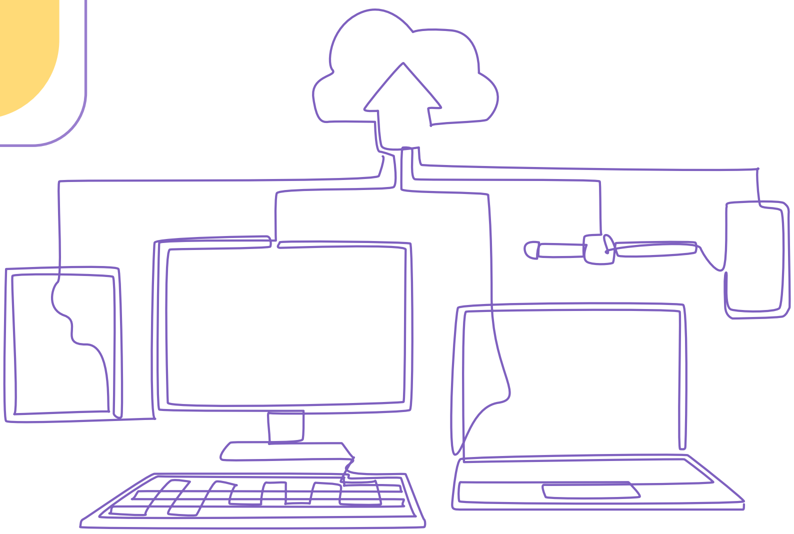


Figure 3. AI: Promise and pitfalls[6,67,68]

OPPORTUNITIES

Automate detection of harmful behaviours: interrupt high-risk interactions, grooming, and trafficking before harm occurs.

Automate detection of CSAM: rapidly identify, block, and remove harmful content.

Support law enforcement: Expedite investigations, review and triage CSAM, identify victims and offenders, and reduce human exposure to traumatic content.

Safety by design: develop and deploy safe generative AI systems and models.

THREATS

Amplify harm: re-victimise children by creating new images from existing CSAM, spread CSAM and guides for offending, bypass age verification systems, and boost harmful content via algorithms.

Generate CSAM: produce sexualised or explicit representations of children in whole or in part, including deepfakes of real children in simulated sexualised situations.

Complicate detection and enforcement: impede identification of victims and offenders, overwhelm detection and removal systems and law enforcement capacity.

Lower technical and social barriers to harm: enable easy creation of CSAM, facilitate online grooming, and normalise exploitation and sexualisation of children (e.g., ‘nudify’ apps).

> **“In my opinion, AI could be very helpful, but like any powerful tool, it needs safety rules, and instead of removing it, we should build strong protections and safety hacks, like filters, monitoring, and guidance to make sure it’s safe for children and everyone else.”**

15-year-old female, Ethiopia[60]

Violent online extremism

Since the 2023 Global Threat Assessment, online groups promoting violence have proliferated, with a 200% increase in NCMEC reports (over 1,300 total) from 2023 to 2024.[12] These groups encourage children to harm themselves or others, highlighting new intersections between sexual exploitation, online radicalisation, and offline harms. Emerging intersections with suicidal ideation, eating disorders, financially motivated scams, and human trafficking have been noted, though research remains limited. Perpetrators often target children in forums where they are seeking help.[7]

> **"We will continue to see this merging of risks together...I think [sexual extortion] is a great example where so many different threats have come together to create this new harm...when someone reaches out to you and says, 'hey, you're cute, you want to chat?'...then it turns into an exchange of imagery...then it might turn into actual production of child sexual abuse imagery. Then it might turn into bullying and harassment before it turns into actual blackmail before it could potentially lead to self-harm..."**

Industry[7]

From the frontlines of harm detection: Insights from PGI on 'Com' groups

PGI (Protection Group International) supports governments, NGOs, and companies in detecting and disrupting online harms—from child exploitation and disinformation to violent extremism—using human-led, technology-supported intelligence.

'Com' groups (also referred to as the 'Com') are an archipelago of online communities where children and young people are targeted and manipulated into producing CSAM, engaging in self-harm, or even recording violent acts. These groups are mostly transnational and are known under different and evolving names: 764, 676, Harm Nation, Leak Society, and CVLT fall under this umbrella. While perpetrators are often young themselves – predominantly male teenagers – there are overlaps with extremist and fringe subcultures, including groups with violent ideologies.

Tactics of the 'Com'
Perpetrators typically use mainstream platforms to identify vulnerable children and adolescents, often seeking those already struggling with mental health issues. For example:

- They infiltrate online self-harm or eating disorder communities and invite children into closed group chats.
- They exploit popular child-focused video games as spaces to meet potential victims, redirecting them into private messaging platforms.

Once isolated, young people may face threats, manipulation, or extortion. Victims may be pressured into recording or livestreaming harmful acts, including self-harm, CSAM, or drug use. This material is then compiled into so-called 'lorebooks', which also contain victims' personal information. These lorebooks circulate among community members, and perpetrators gain status based on the level of harm they inflict. Perpetrators regularly create new online identities to avoid detection.

Impact on victims

- Victims often face severe psychological harm, living under constant fear due to threats and blackmail. Exposure to coercion and violent demands can intensify existing vulnerabilities such as depression, anxiety, or suicidal ideation, sometimes escalating to forced acts of self-harm or suicide attempts.
- Constant exposure to extreme material can normalise harmful behaviours for victims, sometimes leading to ongoing participation. Some victims move from coerced participation to ongoing involvement with offender groups, in rare cases even creating their own channels and repeating patterns of abuse.

Livestreamed abuse

As highlighted in the 2023 Global Threat Assessment, the scale and nature of livestreamed sexual abuse of children – occurring across mainstream social media as well as dedicated livestreaming platforms – remains important and under-documented.[69] Surveys of offenders looking for CSAM on the dark web suggest that over one-third consume livestreamed material, with prevalence varying across regions.[70] Investigations show that livestreams are often prearranged, with small financial transactions linking consumers in higher-income regions to facilitators in high-risk jurisdictions.[71] Projects such as International Justice Mission's **Scale of Harm** study fill critical data gaps, but more systematic monitoring is needed. Financial tracking is a promising avenue for detection (see Prevention).

Evolving technologies: encryption, decentralisation, quantum computing, and extended reality

End-to-end encryption

Increasingly adopted as a privacy and safety feature, end-to-end encryption ensures that only senders and recipients can view message content. However, when introduced without additional child protection safeguards, it makes it virtually impossible to detect CSAM or grooming and severely limits law enforcement's ability to identify victims.[72] In December 2023, one of the main global messaging applications, Meta, enabled end-to-end encryption by default, with other platforms expected to follow. The growing adoption and use of end-to-end encryption likely contributed to a **7 million drop in incidents of child sexual exploitation online** reported to NCMEC.[12] Several major platforms also reduced reporting volumes by about 20% in 2024, raising concerns about transparency and accountability.[73]

Decentralisation

Decentralised computing distributes tasks across multiple devices or systems rather than relying on a central authority, enabling peer-to-peer connections and applications such as social networks, data storage, financial transactions, and machine learning.[39] While this architecture can improve privacy, it also poses unique challenges for preventing and addressing technology-facilitated CSEA. Decentralisation complicates suspect identification, content moderation, and removal of illegal material.[39] Looking ahead, the main challenge lies in the increasing adoption of decentralised technology without adequate safeguards for the risks already observed.[39]

Quantum computing

Quantum computing is an emerging field that enables information to be processed exponentially faster than classical computers. While no cases of its use in CSEA have been documented yet, future risks could include accelerating the generation of AI-generated CSAM or breaking encryption systems that currently safeguard children's data. Early policy and safety by design considerations are critical before applications mature.[39]

Extended reality

XR technologies (virtual, augmented, and mixed reality) are becoming more accessible and affordable, expanding risks of misuse and abuse.[75] Research highlights possible misuse, including immersive CSAM experiences and normalisation of harmful behaviours.[76] Pre-emptive action is essential before XR becomes mainstream. At the same time, XR shows promise for prevention and training, offering realistic simulations for law enforcement and therapeutic interventions. However, evidence of effectiveness remains limited.

> “...with virtual reality, you're going to have tactile touch and feel soon, and there's going to be pads on bodies and that's going to be a new way of perpetrators inflicting physical harm in the virtual space.”

Survivor[77]

Characteristics and vulnerabilities of victims and/or survivors

The following section summarises what is currently known about victims and/or survivors, while noting persistent data gaps. Information about victims depicted in CSAM remains scarce: only a fraction of the millions of children depicted in INTERPOL reports are ever identified, geographically located, or confirmed by age.[9] The scale of the problem exceeds law enforcement capacity, due to limited personnel, technical capacity, and financial resources to identify victims. Offenders deliberately hide identifying details or use encryption or anonymising technologies, making image analysis and source tracing extremely difficult.[78] Reported material disproportionately depicts pre-pubescent children, while adolescents are likely underrepresented due to the lack of research with this particular demographic and difficulty of distinguishing their images from those of young adults.[8,9] Stigma, inconsistent reporting practices, and a lack of data disaggregation in administrative data systems limits the ability to understand victim demographics and characteristics. Marginalised groups, including sexual and gender minority populations, children with disabilities, and those in institutional or unstable living conditions, remain largely absent from quantitative data despite facing increased risk.[8]

> “We don’t know what happens to victims.”

Law enforcement[79]

Age and gender

Consistent with the 2023 Global Threat Assessment, pre-pubescent girls remain the most frequently depicted victims in reported CSAM. In 2024, I See Child Abuse Material (ICCAM) data showed that 98.7% of reported cases involved girls, and 93.2% were pre-pubescent girls.[13] Boys are disproportionately represented among sexual extortion victims, accounting for 91% of reports received by the IWF in 2023.[14] Anecdotal evidence suggests that more boys may be subjected to financial sexual extortion because of boys’ image sharing habits, or offenders’ impressions of their willingness and ability to pay.[9]

> “We have heard that they do target girls [with financial sexual extortion], but it’s in a different way. They’re not targeting them for money. They’re targeting them for images to…blackmail. The boys are their target.”

Industry[7]

Age remains a critical factor in understanding risk. Data from a nationally representative study of 16 to 24-year-olds in Australia indicates that children typically first experience unwanted sharing of their own sexual images around age 15, though approximately 9% report first experiences before age 11.[80] ICCAM data shows a slight increase in the proportion of CSAM reports involving pre-pubescent children (rising from 90% in 2023 to 93.2% in 2024), while reports involving adolescents (14–17 years) and infants/toddlers (under 3 years) decreased slightly.[13] INHOPE has also documented a growing volume of CSAM depicting children under 10.[81]

Vulnerabilities

In line with previous Global Threat Assessment findings, children who are marginalised – whether due to poverty, minority status, neglect, unstable living conditions, or rural residence – are disproportionately at risk.[80,82–84] Additional risk factors include family dynamics that normalise controlling behaviours, lack of parental digital literacy or supervision, lack of social support, and prior exposure to violence, CSAM and violent pornography.[54, 84–86] Children with disabilities also face compounded risks of sexual exploitation: for example, increased negative impacts on mental health and sexual risk behaviours, and significant barriers to disclosure, including fear of parental blame, judgment, and loss of autonomy.[87–89] Research shows that adolescents facing multiple forms of abuse are more likely to experience both offline and online sexual victimisation, with lasting educational and mental health impacts.[90–93]

Characteristics and behaviours of people at risk of offending and who have caused harm

Emerging evidence from law enforcement, research, and offender communities is deepening our understanding of who offends, how they operate, and what drives their behaviour. While most perpetrators are adult men, patterns are increasingly complex, with variation across age, gender, geography, motivations, and methods. Recognition of children and youth at risk of offending and who have caused harm is increasing, as well as the need for targeted research, prevention, and support focusing on this age group. Until recently, research focused mainly on adult offenders identified by justice systems or seeking help, limiting insights into perpetration pathways and opportunities for early intervention. Innovative approaches—such as studies directly surveying offenders on the dark web and prevalence estimates among representative male samples—are expanding the evidence base, though robust, representative data remain scarce.[57,94] Reporting biases and definitional inconsistencies also limit the data.[95] Despite these gaps, research continues to illuminate the vulnerabilities, technologies, social environments, and systemic failures that enable perpetration.

> **“We do our best to mitigate risk and to reduce harm. But as long as people continue to have a sexual interest in children, as long as people want to exploit others for their own financial gain or otherwise, we're going to continue to have these problems. They're what we call whole-of-society issues.”**
>
> *Industry*[7]

Adult offender profiles and patterns of perpetration

Available evidence indicates that offenders buying and exchanging content are predominantly male.[96,97] Surveys of dark web CSAM users show that 68% identify as male and 17% declined to report their gender.[94] In the case of livestreamed abuse, findings suggest consumers are mostly males, predominantly based in Asia, Europe, and North America, while those producing can be both men and women.[95] Age patterns vary by type of offending and by population studied. Of the 4,549 respondents who reported consuming CSAM on the dark web, 43% were aged 18-24.[91] Another study shows that consumers of livestreamed abuse tend to be older.[94,98]

Perpetration also extends beyond individuals acting alone. It often involves interconnected actors across borders: an initial abuser produces images or videos; others upload or distribute the material; and consumers and buyers fuel demand that drives its circulation. Online networks exchange, normalise, and amplify this abuse internationally, making it extremely difficult to identify perpetrators, despite specialised investigations.[79,99]

A global chain of abuse

In Operation Vibora (March–May 2025), led by the Spanish National Police with INTERPOL and Europol, 20 people were arrested and 68 additional suspects identified across 12 countries in connection to CSAM.[100] In Operation Cumberland (February 2025), Europol dismantled a Danish-run platform distributing AI-generated CSAM, leading to 25 arrests, 273 suspects identified, and the seizure of 173 devices in 19 countries.[101]

While many victims and perpetrators remain unidentified, available data on known cases suggest a significant proportion of CSAM and other forms of technology-facilitated abuse are produced by people known to the child.[102] A Thorn report drawing on NCMEC data indicates that, among the small number of children who are identified from CSAM, two in three are abused by someone in their offline communities.[10,103] A 2023 review of 66 studies of parental CSAM production highlights that family members are a significant but underacknowledged group at risk of offending, typically producing material involving pre-pubescent children.[104]

> **“There is a digital aspect [to abuse]…it is intra-family child sexual abuse…the offenders…even the grandfathers are using digital services like WhatsApp…private chat and taking pictures.”**
>
> *Civil society*[11]

Children displaying harmful sexual behaviours

Harmful sexual behaviours among children are recognised as a growing issue, though true prevalence remains unclear. Before the age of 18, one in five children experience sexual harm, both online and offline, and more than half of these instances occur between peers.[105,106] Such behaviours may begin as peer-related exploration, but can sometimes escalate into more serious offending. For example, a child may initially view sexual images of peers their own age and continue seeking similar material as they grow older.[9,11] Children displaying harmful sexual behaviours often share overlapping vulnerabilities such as prior victimisation or exposure to sexual content, trauma, neglect, social inequality and neurodiversity.[107] These vulnerabilities are often compounded by a lack of awareness, inadequate education, and weak prevention and support systems.[108] Without timely support, these behaviours can disrupt healthy development, damage relationships, and cause significant psychological distress. Stigma and exclusion can cause further harm, particularly when children are labelled as offenders rather than recognised as children with specific protection and developmental needs.[107] Existing prevention and intervention efforts have largely focused on adult perpetration. Child-focused interventions are often embedded within broader violence prevention programs, leaving gaps in understanding and response.[107] Most interventions begin too late, after harm has already occurred, missing a critical window for prevention.[108] By overlooking that exploration, boundary-testing, and risk-taking are developmentally typical, prevention and response efforts often fail to meet these children's needs.[108]

Recent data also highlights children who have caused harm online, particularly through sharing other children's sexual images.[80,99,109] Many do not act with the intent to cause harm, but rather due to boredom, attempts at humour, or expectations about masculinity.[7,99,108] Girls are more likely to face pressure to produce sexual content, while boys are more likely to share it.[99] Sexual and gender minority youth face heightened risks of blackmail and bullying.[110] Victim-blaming remains common, with surveys showing that nearly half of children and two-thirds of caregivers in Cambodia and the Philippines blame victims when their images are shared against their will.[111] As one adolescent boy shared, "He was quite popular. It didn't really have an effect on his popularity…I think it's more about what the girl sent and the boy doesn't really have any repercussions."[99]

Motivations and pathways to perpetration

Research highlights multiple pathways to perpetration of technology-facilitated CSEA. High sexual drive, sexual interest in children, neurodiversity, and emotional dysregulation are documented as risk factors.[94,108] In helpline data, some offenders reported that their own childhood victimisation contributed to later abusive behaviour, with trauma acting as both a motivator and rationalisation.[52,112]

New survey evidence deepens understanding of these motivations. A 2024 study of 4,549 dark web offenders found that:

- 30% were motivated by sexual interest in children,
- 15% were trying to regulate emotions such as loneliness or depression,
- 10.6% had a desire to understand their own experience of abuse, and
- 6.3% were searching for material that depicted their own abuse.

Notably, nearly 40% of offenders reported heavy consumption of adult pornography before progressing to CSAM.[94] This is consistent with other studies that show offenders often begin by consuming adult pornography but then start seeking novelty and 'variety'.[95,113] Consumption of increasingly violent or extreme pornography may stem from and interact with other problematic drivers of harmful sexual behaviours, reflecting a pattern of desensitisation. Further research is needed to understand these complex interactions and pathways to escalation and perpetration.

Financial motivations are important: there is evidence of CSAM being used to drive internet traffic, while crimes such as sexual extortion, livestreaming, and trafficking—often facilitated by generative AI—are highly profitable.[2,115] Perpetrators of financial sexual extortion of children are often based in low- and middle-income countries such as Nigeria, the Philippines, and Côte d'Ivoire, while victims are typically located in high-income countries.[116] In 2024, NCMEC reported around 100 reports of financial sexual extortion of children each day, with boys being disproportionately targeted.[117] The IWF also reported that 91% of sexual extortion victims were male.[117]

> “People often think offenders are motivated only by sexual gratification, but increasingly the motivation is financial.”
>
> *Industry[7]*

Methods and technologies used for offending

Methods of perpetration are dynamic and shaped by evolving technologies. Offenders exploit anonymity, encryption, and platform loopholes to share CSAM across the open and dark web.[118] They conceal content through link manipulation, content delivery networks, doppelgänger (masked) websites, and encrypted social media exchanges to avoid detection and takedowns.[11,119] Algorithms can also surface harmful material or connect children with offenders. At the same time, AI tools, deepfake technology, and 'nudify' apps (software that creates fake nude or sexually explicit images based on photos of real people) enable the production of synthetic child sexual imagery, which may be used to coerce victims into producing real CSAM.[13,118,121] This pattern typically involves first contact and grooming on mainstream social media, gaming, and messaging platforms, followed by a move into encrypted or anonymous environments to escalate the abuse.[120]

> “It used to only be in dark forums or the dark web...but in the last couple of years there's just a huge increase of [CSAM] being readily available.”
>
> *Industry[7]*

> “There is no safe platform, the offenders are using every platform… when we ask the offenders where do you contact children, they say, of course it’s in the open web and the social media and the gaming platforms, where the children are. Children [small children] are not in the dark web.”

Civil society[11]

Prevention

We use a broad definition of prevention, encompassing all actions that aim to:

1 prevent children from being subjected to exploitation and abuse or from causing harm to other children,

2 prevent re-victimisation and re-offending, and

3 reduce the harmful consequences for children who have already experienced abuse and ensure rehabilitation of those who have caused harm.

This definition includes actions that may occur after harm has taken place, often described as tertiary prevention or response. While these efforts often receive more focus and resources, greater attention is needed to address root causes, strengthen protective factors, and prevent harm before it occurs. Prevention efforts must span every level of a child's environment, including their peers, families, communities, institutions, and wider society, and adapt to an evolving technological landscape.[30] Creative cross-sector responses are demonstrating that prevention is possible, with several led or informed by children and survivors themselves. Emerging technologies have introduced new risks, but they also offer opportunities for protection.

Effective prevention begins with addressing the social, structural, and financial drivers of harm. It must consider how factors such as age, sexual orientation and gender identity, disability, neurodiversity, ethnicity, indigenous or migrant status, socio-economic conditions, and educational status intersect to shape children's risks of harm or harmful behaviour. Power imbalances, poverty, low digital literacy, and limited parental supervision can increase children's risks.[123,124] Harmful social norms, stigma, shame, and victim-blaming keep may deter disclosure and help seeking, while weak laws and governance allow abuse to thrive.[85,91,121] Economic drivers, including financial sexual extortion and revenue from online traffic and advertising, must also be addressed. Preventing technology-facilitated CSEA also requires political commitment and sustained investment in the systems, resources, and processes that protect children. Key enablers include:

- sustained political commitment and dedicated funding to prioritise children's safety and well-being,
- robust digital governance and accountability across all levels of government,
- research and data to inform prevention and prioritise resources,

- strong child protection systems with trained professionals who can detect risks early and respond with child-friendly, knowledgeable, and trauma-informed support,[121]
- supportive social norms that recognise technology-facilitated CSEA is preventable, encourage reporting, and promote help-seeking for individuals with harmful sexual thoughts or behaviours,[125] and
- global and cross-sector collaboration to coordinate prevention, strengthen accountability, and harmonise terminology, data standards, and monitoring systems.

> **"If you give the device and the mobile phone or the internet access to your child...you will be opening the door to the social environment which is full of adults. So, would you do that in your home? You just opened the door and said 'welcome, everybody!'"**
>
> *Civil society[11]*

Closing the funding gap

> **"I see missed opportunities because the funding is very tight right now, especially [with] what is happening in the world...Everybody is fighting [for] the funding, so it doesn't make the collaboration very easy... We should do more joint work to prevent these crimes."**
>
> *Civil society[11]*

Despite the increasing scale and complexity of technology-facilitated CSEA, there is a "significant – and worsening – global funding gap" for prevention, response, and research. Safe Online identifies chronic underfunding as "the single greatest barrier to achieving a safe, inclusive, and ethical digital future for children".[126] The mismatch between investments in prevention and the costs of harm is stark. Violence against children can cost countries up to 11% of GDP, in some cases exceeding national health expenditure sixfold.[126] In the United States, more than $5 billion is spent annually on incarcerating adults convicted of sex crimes against children – more than 3,000 times the budget for child abuse prevention research.[127] Low- and middle-income countries are especially underfunded, often relying on short-term, project-based funding rather than sustained national responses.[128] Closing the funding gap requires innovative approaches, including catalytic funding from philanthropic sources, co-financing from governments, sustained investment from international financial institutions and other multilateral agencies, and stronger mechanisms for long-term financing. Funding is also needed to strengthen national systems that are essential for prevention, including health, education, child protection, social services, and legal systems. Recognising the reality of a constrained funding environment, it is essential to use available resources more efficiently, by better coordinating prevention efforts across sectors, using evidence and data to prioritise investments, and adapting and testing evidence-based interventions, including from the Violence Against Children agenda.[9,129] Robust cost-benefit analyses are also needed to demonstrate that prevention is more cost-effective than reactive responses to technology-facilitated CSEA.

> “There's a lot of interesting elements to...bring the North-South conversation more aligned, to bring the academic world into the practitioner sphere... [but] I unfortunately think the funding landscape is not conducive to improving that.”

Civil society[11]

Strengthening the evidence base for prevention

> “It's kind of an automatic sentence to say...we need more data, but at some point we have to take stock of the fact that...If you have more than 500 [studies on sexual exploitation of boys], it's unfair to say that there's just no data. It's just that the quality of data is weak oftentimes.”

Academic[8]

Robust evidence is essential to understand emerging risks, evaluate prevention strategies, and guide investments. A public health approach can guide this process: (1) defining and monitoring the problem and its prevalence; (2) identifying risk and protective factors; (3) designing, testing, and evaluating prevention strategies; and (4) sharing lessons and scaling up what works.[123] Translating research into more effective prevention requires coordinated research and data sharing across sectors and countries. The **Data for Change initiative**, launched in 2022 and now involving 120 organisations, aims to map good practices, reduce barriers to data sharing, and prioritise data from Global Majority countries.[130] The initiative emphasises adapting approaches to specific contexts and involving young researchers in low- and middle-income countries, to make global evidence more inclusive and actionable. UNICEF's data brief on **Measuring Technology-facilitated Violence against Children in line with the International Classification of Violence against Children**, advances efforts to enhance the quality and comparability of global data.[131]

To stay informed about emerging trends and the latest global evidence on effective prevention strategies, refer to the living resources in the Appendix.

Turning evidence into action to end childhood sexual violence: The Safe Futures Hub global Living Systematic Review and Practice-based Knowledge framework

Launched in September 2023, the Safe Futures Hub is co-led by the Sexual Violence Research Initiative (SVRI), Together for Girls, and WeProtect Global Alliance.[132–135] Its mission is to end childhood sexual violence by promoting solutions informed by data, evidence, practitioner knowledge, and community-led approaches.

In early 2026, the Safe Futures Hub, together with Oxford University, will launch the global **Living Systematic Review**, an updated resource that synthesises evidence on what works to prevent childhood sexual violence. The **Living Systematic Review** applies rigorous, transparent methods to identify, appraise, and summarise emerging intervention studies, ensuring policymakers, practitioners, and researchers have access to the most current evidence. Unlike static reviews, it will evolve in real time, bridging the gap between research and practice. Building on the **Building Safe Futures** 2024 evidence report and its call for stronger, evidence-driven action, this resource will guide investments in effective, contextually relevant strategies. By spotlighting interventions that work, the Safe Futures Hub **Living Systematic Review** will empower stakeholders to scale-up and adapt solutions that protect children from sexual violence.

In December 2025, the Safe Futures Hub will launch two new resources to strengthen how practice-based knowledge (PbK) is recognised and used in childhood sexual violence prevention and response.

- The background paper explains what PbK is and why it matters for preventing and responding to CSV, showing how it brings in under-represented voices, strengthens practice, and values both practitioner and lived expertise.
- The guidance framework offers actionable tools and processes to support practitioners in gathering, using, and sharing PbK in safe, ethical, and practical ways.

In the context of childhood sexual violence prevention and response, PbK refers to the insights generated through lived expertise and direct engagement in programmes, services, or advocacy efforts.

While research shows *what* works, PbK explains *how* it works, *why* it works, and how to keep it working in complex, changing contexts. Together, PbK and research can make strategies more effective, relevant, and grounded in real-world contexts.

Designing the prevention framework

Across consultations, a unifying message has emerged: we need to act now. Understanding the scale and the nature of technology-facilitated CSEA is necessary, but not sufficient. The central challenge that many in this field continue to face – "where do we start?" – was the impetus for this prevention framework.

The prevention framework was developed to complement WeProtect Global Alliance's Model National Response, which provides a structure for action at national and system levels. Together, they guide global action to address technology-facilitated CSEA.[29] The framework also builds on other well-established models:

- the Socio-Ecological Model, which highlights that risks and protections exist at multiple levels of a child's environment;[30] and
- the public health prevention approach, which defines prevention at different levels, from whole population approaches to targeted measures for individuals at risk of experiencing or causing harm.[123]

The framework is also anchored in international and regional child rights standards, including the UN Convention on the Rights of the Child and General Comments No. 16, 24, and 25, and the Global Digital Compact.[24,33,136] It was co-created through a participatory process involving youth, survivors, and an Expert Steering Committee representing governments, civil society, industry, and intergovernmental agencies. Stakeholders contributed through workshops and written feedback.

> **"When we are making prevention efforts, I believe we should involve every stakeholder... survivors, those with deep experience, tech industries, faith institutions, community leaders, teachers, parents, youth mentors, NGOs, civil society, and even regionals like the African Union, like the UN, INTERPOL."**
>
> *Civil society*[11]

The prevention framework is organised around four interconnected action areas:

- Child participation and leadership
- Community education and support
- Digital safety
- Law, policy, and justice

The order in which they are presented reflects a socio-ecological approach, starting with children and progressing to community, institutions, governments, and global actors. The action areas are mapped across three levels of prevention: primary (proactively protect), secondary (detect and disrupt harm), and tertiary (respond and support after abuse). Enablers such as research and financing are crucial and must be addressed continuously to ensure all actions are effective and sustainable.

Instead of ranking interventions by strength of evidence, which is not yet possible, this framework presents recommendations thematically to help stakeholders identify prevention actions relevant to their context and expertise. The framework highlights evidence-based approaches where available, and points to expert recommendations, good practice, and innovative practices needing further evaluation.

> **"A public health approach is now required, with the establishment of a system to prevent perpetration, detect and address crime, but also to support victims and their families."**
>
> *Academic*[8]

Expert insights on prevention priorities from the Global Threat Assessment 2025

Our online survey of 77 professionals working to combat technology-facilitated CSEA (61% non-profit, 19% government, 16% industry, and 3% independent statutory bodies) confirmed strong support for the four action areas. Respondents called for deeper understanding of perpetrator behaviour, motivations, and profiles (47%); root causes and systemic drivers of harm (45%); and children's perspectives on technology use (39%). The top priorities identified for scaling up prevention efforts were long-term, flexible funding (87%), training and technical support for staff (58%), and access to open-source, child-centred tools and guidance (50%).

Although based on a small sample of experts, these insights reflect broad agreement on prevention priorities and the urgent need for investment, capacity-building, and collaboration.

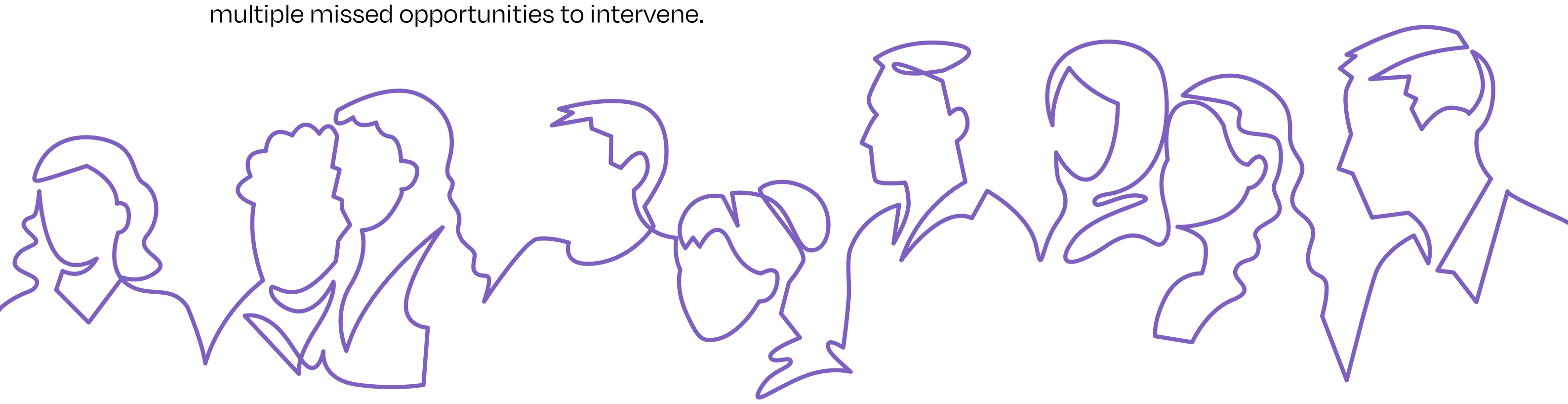
Putting prevention into practice: The Swiss cheese model

The Swiss cheese model offers a powerful lens to understand how this prevention framework can be applied in practice.[137] Widely used in safety-critical fields such as aviation, medicine, and engineering, the model emphasises that serious harm rarely results from a single point of failure. Instead, harm occurs when multiple weaknesses in protective systems align. Each 'slice' of Swiss cheese represents a layer of protection – for example, digital safety measures, or laws, policies, and justice mechanisms. Each slice has 'holes' that represent points of weakness. A single hole may not cause harm because other layers act as a barrier, but when the holes in multiple layers line up, severe harm can occur.

Applied to technology-facilitated CSEA, the Swiss cheese model underscores three important insights:

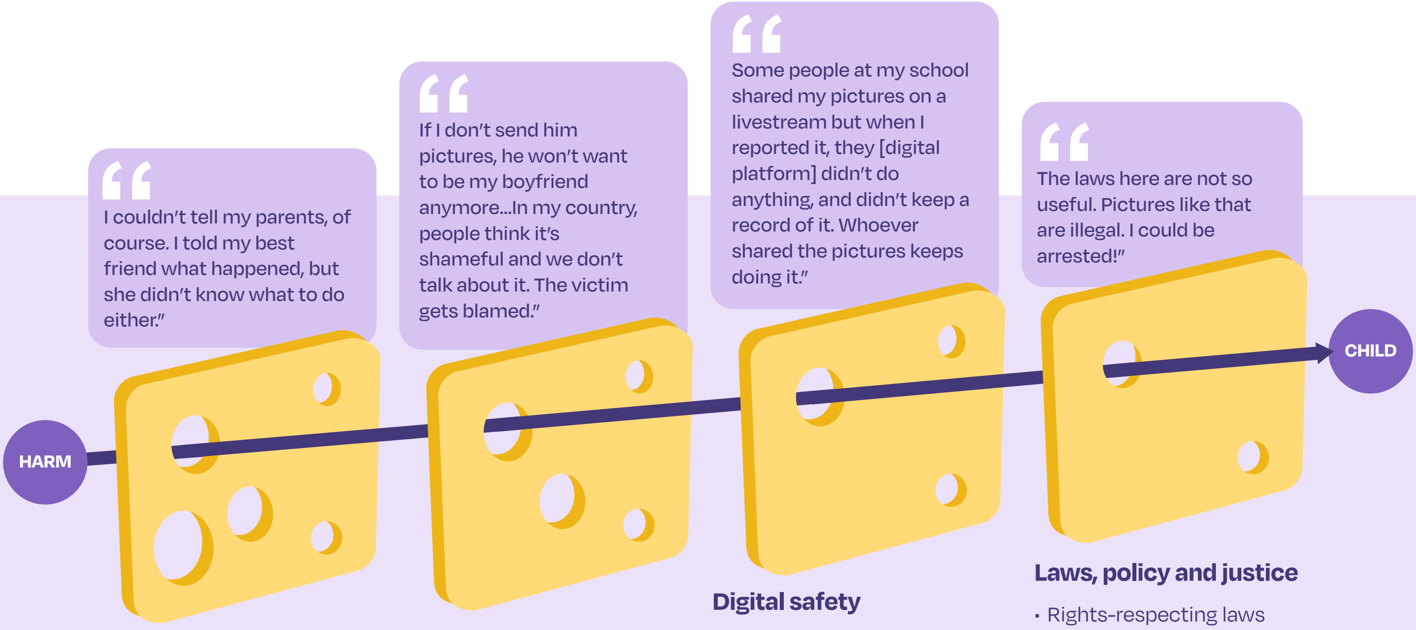
- Every time a child is harmed by technology-facilitated CSEA, it reflects a system failure and multiple missed opportunities to intervene.
- No single actor or sector has all the solutions. Multiple layers of prevention must work together.
- Prevention requires continuous learning and adaptation to identify where weaknesses in protection exist, how severe and urgent the potential consequences are, and what resources are available to address gaps, or to strengthen other layers of protection.

Used together, the prevention framework and Swiss cheese model provide structure and method. While the prevention framework encompasses all forms of technology-facilitated CSEA, the Swiss cheese model can help stakeholders to prioritise actions, assess risks, and identify weaknesses that contribute to a particular incident or type of harm. Together, they shift the focus from isolated fixes to building resilient systems with multiple layered protections to keep children safe.



Scenario: Amal is in high school. She recently broke up with her partner, who is the same age as her. To get back at her, her partner posted intimate pictures of Amal online, and then other people spread them around her school. What happened to Amal resulted from failures at multiple levels. This is how it went from her perspective.

Figure 4. Visualising the Swiss cheese model: Understanding risks in first-person generated sexual content involving children



"I couldn't tell my parents, of course. I told my best friend what happened, but she didn't know what to do either."

Child participation & Leadership

- Trained peer supporters to receive complaints and connect children to support services.
- Child- and survivor-led design of education and awareness raising materials, reporting channels, and digital safety features.

"If I don't send him pictures, he won't want to be my boyfriend anymore...In my country, people think it's shameful and we don't talk about it. The victim gets blamed."

Community education & support

- School-based programs on healthy relationships, sexuality, and digital safety.
- Early support for children at risk of harm or causing harm.
- Educator training and clear school policies for prevention and response.
- Community awareness campaigns to shift norms, reduce victim blaming, and encourage reporting.

"Some people at my school shared my pictures on a livestream but when I reported it, they [digital platform] didn't do anything, and didn't keep a record of it. Whoever shared the pictures keeps doing it."

Digital safety

- Child rights impact assessments and Safety by Design features during platform development (e.g., nudity detection, content-warning pop-ups that interrupt risky sharing and prompt help-seeking).
- Accessible reporting options that provide timely feedback, link to support, and remove harmful content or accounts quickly.

"The laws here are not so useful. Pictures like that are illegal. I could be arrested!"

Laws, policy and justice

- Rights-respecting laws that protect victims and avoid criminalising consensual behaviours between close-in-age peers.
- Regulators empowered to oversee industry compliance, investigate abuse, and impose sanctions.
- Child-friendly justice and access to redress through trained police, judiciary, and prosecutors.

Prevention action areas

Child participation and leadership

> Children's voices must be heard at every stage of prevention, detection, and response.

Survivor, Philippines[138]

Children and survivors have the right to share their views and influence the policies, programmes, and services that affect them through safe, meaningful participation.

Partnerships with child-led and child-focused organisations can promote safe participation, detect early risks and harms, and inform effective, child-centred, interventions.

Efforts must be made to involve all children, particularly those from marginalised backgrounds, recognising that children are at risk both of being harmed and of causing harm to other children.

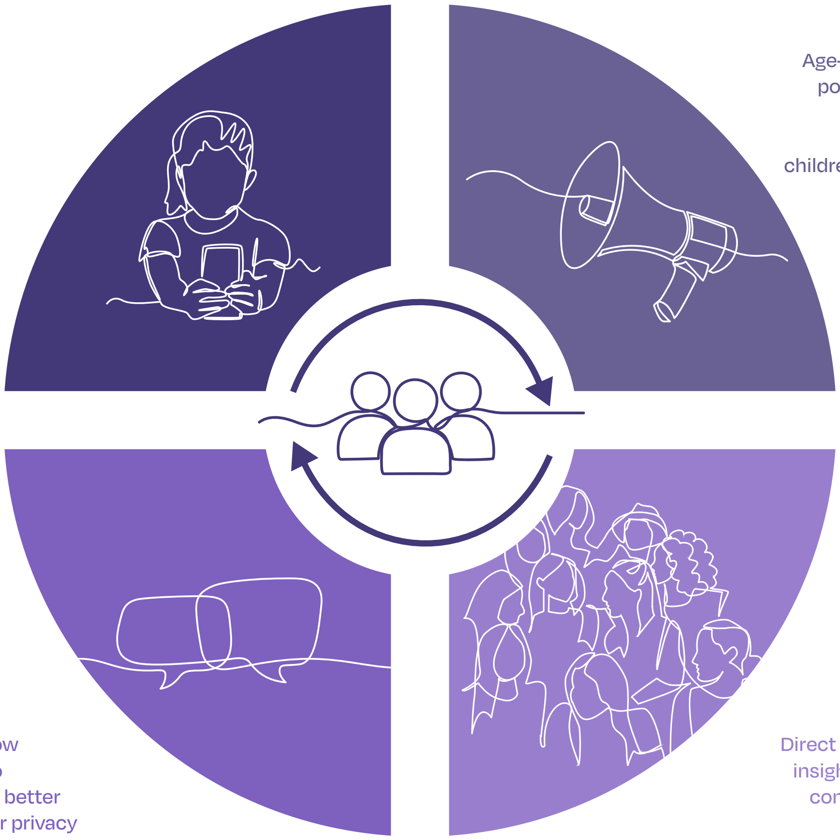
Principles for safe and meaningful participation

> They [children] are the most vulnerable and the most needed people to solve the problem.

Survivor, Philippines[138]

Article 12 of the UN Convention on the Rights of the Child affirms every child's right to be informed, express their views, and participate in decisions affecting all aspects of their lives.[33] The **Lundy Model** (see Figure 5) provides a practical framework for applying Article 12 to support children's meaningful participation.[139] Children and youth can help to identify emerging risks and inform proactive prevention strategies. As part of a campaign implemented in Indonesia, Nepal, and the Philippines, child rights organisation Kindernothilfe developed a **Global Program Guide** and **Toolkit** to support meaningful child and youth participation in advocacy for prevention and protection from online violence.[140,141] UNICEF has developed **Spotlight Guidance** sharing best practices for engaging with children in Digital Child Rights Impact Assessments.[142]

Figure 5. Features of meaningful participation applied online[143]



SPACE
Safe, accessible, and child-friendly forums where children can discuss digital risks.

VOICE
Age-appropriate tools—like polls, avatars, anonymous surveys, and creative media—to learn about children's online experiences.

INFLUENCE
Visible links showing how children's input leads to improvements, such as better reporting tools, stronger privacy features, or school-based prevention programs.

AUDIENCE
Direct pathways for children's insights to reach technology companies, regulators, law enforcement, and policymakers.

Safety, quality, and children's best interests should always be prioritised when engaging with children. Children's participation should only proceed when adequate staffing, safeguarding measures, and trauma-informed support services are in place to protect them from harm. If this is not possible, draw on insights from youth, adults, and organisations that can represent children's views, as well as from existing evidence, research, and good practice.

Engaging children and survivors in prevention

> “I think NGOs made by the youth and for the youth will be really helpful. These organisations could raise awareness in a more comfortable way as the advice would be coming from fellow youth.”

17-year-old male, Pakistan[60]

Initiatives engaging children and youth to inform prevention include:

- **Mtoto News**, a digital and media platform based in Kenya that facilitates child-led advocacy and enables over 100,000 children to directly engage with their leaders on issues including child sexual abuse online and offline.[144]
- Snap Foundation's **Digital Well-Being Index**, which engages young people across six countries to share insights about their psychological well-being and experiences across online platforms, revealing important insights for prevention.[45]
- **BeSmartOnline**, the Malta government's official Safer Internet Centre, which is guided by a youth panel that helps to identify new online risks and co-design effective awareness raising strategies.[145,146]

Youth leadership in online safety: Insights from VoiceBox

VoiceBox is a UK-based, youth-led social enterprise and content platform that helps young creators aged 13–25 years thrive and shape safer digital environments that centre their lived experiences.[147] With a global network spanning more than 50 countries, VoiceBox amplifies diverse perspectives and can often identify emerging online risks faster than traditional research, serving as an 'early warning system' for policymakers and industry leaders. This ensures that decision-makers are equipped with real-time, youth-informed insights about evolving threats.

VoiceBox gathers honest, unfiltered insights from young people on complex online safety challenges, including media literacy, online harms, and emerging digital risks. Its approach combines leadership opportunities for youth with strong safeguarding and trauma-informed support. VoiceBox uses peer-led focus groups, interviews, and creative insight-gathering methods (such as art, videos, and poetry) to enable young people to share experiences in ways that feel safe and authentic. This approach has shed light on issues such as AI companions and subscription-based platforms.[44]

Children experiencing intersectional discrimination—such as sexual and gender minority populations and children with disabilities — face unique risks and harms online, but they are often excluded from policies and programming.[11]

> “If they're not adequately factored in the way the interactions and the policies are being designed, then we risk missing out on this underrepresented population.”

Civil society [11]

It is important to consult marginalised children and those with specific needs who may navigate digital technologies differently from their peers.[8] For example, deaf children, who often rely on video communication, face unique online risks and may have fewer opportunities to recognise or report potential exploitation.[11] Ensuring accessible, tailored and inclusive communication strategies is critical to support their safety online. Examples of survivor-led and survivor-informed initiatives are highlighted below:

- **Disrupting Harm** generates high-quality evidence on digital harms to children and young people in 25 countries across 6 regions. The project uses trauma-informed participatory processes following strict ethical guidelines and child safeguarding procedures. The first phase found nearly one in three children did not disclose harms, with almost half reporting they did not know who to tell or where to seek help.[10] A second round of in-depth interviews with more than 100 young survivors across Latin America, Eastern Europe, and the Middle East was completed in 2025, with results forthcoming.
- **Global Boys Initiative** documents the experiences of boys subjected to sexual exploitation and abuse across ten countries, highlighting barriers to disclosure, reporting, and access to services.[148]
- **Our Voice Male Survivors** study provides one of the largest datasets on boys who have been subjected to sexual abuse. It shows distinct patterns such as earlier onset, different offender profiles, and longer delays before disclosure, underscoring the need for gender-sensitive research and services.[114]
- **Secrets Worth Sharing** is a platform providing trauma-informed resources that recognise the diversity of survivor experiences. It features survivor-centred workshops, podcasts, and videos covering topics such as child sexual abuse, intersectionality in trauma, and children displaying harmful sexual behaviours.[149] As the founder shared:

> “One thing we do differently as an organisation is producing online resources which are specific to different identity factors, such as being a Black Man, or Queer, or speaking another language. My highest engagement with teens and young people is over suggestions for these [podcast and video] episodes. I think this is because children and young people don't want to just see themselves as a survivor or victim but are interested in how their experiences are unique based on their own identities.”

Civil society[150]

Community education and support

> “To promote digital education and collaboration, focus not only on safety tools, but also on empowering children and teens with the knowledge and skills to navigate safely and responsibly. Involve parents, educators, and young people themselves in creating safer, more positive digital environments.”

18-year-old male, Nicaragua[60]

Education and awareness raising efforts should seek to change behaviours and promote reporting and help-seeking. They should be based on evidence, adapted to context, accessible for all children, and coordinated across sectors to ensure clear roles and consistent, effective messaging.

Children need multiple, trusted ways to report concerns, seek help, and access survivor-centred support services, including helplines, formal reporting channels, trained peer supporters, and safe adults.

Early, evidence-based interventions should be available for children at risk of being harmed, as well as children and adults at risk of causing harm.

Deterrence messaging and warnings should be tailored to different individuals at risk of causing harm and paired with immediate pathways to support for harmful sexual thoughts and behaviours.

Education and awareness campaigns

> “We need to educate both the children as well as the parents on online safety...I feel like most people think that they don’t have anywhere to go [for help] because it’s online...Parents also need to be more educated on how to handle these situations. And the laws could be stricter, especially in my country, I’ve never heard of much about this stuff.”

14-year-old female, Ethiopia[60]

Education and awareness raising initiatives are key for prevention. These efforts must move beyond simply raising awareness to driving real behaviour change and ensuring access to help.[9]

Experts across sectors, as well as youth advocates and survivors, stressed that effective education and awareness raising efforts should:

- Be informed by or co-developed with children and survivors, trauma-informed, and contextually sensitive.
- Avoid fear-based messaging or stigma that deters reporting and help-seeking.
- Be inclusive and accessible. They should be delivered in multiple languages, formats, and locations, including in schools and other physical and digital spaces where children learn and connect. Efforts should be made to reach marginalised groups, including children with disabilities, out-of-school children, and those in rural areas or fragile education contexts.
- Equip both children and adults – including caregivers, educators, and service providers – with the knowledge and skills to prevent, recognise, and respond to sexual exploitation and abuse both online and offline. This should include information about relevant laws, how to report concerns, where to seek help, and how to support children and peers, and avoid causing harm.
- Be coordinated and sustained, with clear roles across schools, families, communities, industry, and government to ensure consistent, effective messaging.
- Be appropriate for children's age and developmental stage and strategically timed (e.g., before a child receives their first phone or starts to go online unsupervised).

Some survivors and youth advocates expressed concerns that education may struggle to keep pace with the risks associated with rapidly evolving technologies (e.g., XR), and that formal education settings may feel intimidating or unsafe for children to discuss sensitive issues. This highlights the need to involve children in identifying risks and shaping education and awareness initiatives.

> **“There's going to be a lot of children who are not going to want to participate in something like that [school-based education] because it's... still [a] taboo topic and you're going to have different children who are afraid to say anything and afraid to speak out.”**
>
> *Survivor*[77]

> “Parents, especially newcomers, may not have the language skills or technological knowledge to keep up [with risks associated with new technologies]. Resources…should teach social media safety, or schools should send materials in multiple languages to educate parents.”

Child advocate, Canada[38]

Prevention programmes for child sexual abuse are well supported by evidence, though evidence for programmes addressing technology-related risks is still limited and developing.

- **Tackling Online Child Sexual Exploitation (TOCSE)** addresses online violence at individual, community, industry, and systemic levels in Vietnam. It engages children in participatory consultations, child-informed design of materials, and child-led initiatives in schools.[153,154] TOCSE has provided education and skills training for over 18,000 children 12 years and older, and 11,000 parents and teachers, alongside strengthening child helplines and support services.[153,154]
- UNICEF’s report on parenting programmes draws on a rapid evidence synthesis and consultations with over 50 experts across multiple sectors to identify key considerations for designing interventions that support parents and caregivers in preventing and responding to technology-facilitated CSEA.[155]

> “I think there should be more lessons and workshops in schools regarding child exploitation or sexual abuse online…think I could easily have become a victim to it. But now that I’ve done a few workshops, I’ve become more knowledgeable as to how traffickers victimise people, and how they choose the victims…And so, I feel like educating students on… how victims are chosen by traffickers would really prevent them from becoming trafficked.”

Child advocate, Canada[38]

> More education [is needed] on what to avoid and why to avoid it. Children will not listen when they are only told not to do something. It is better to give children a step-by-step education and hear the uncomfortable parts of why something is wrong so that they know not to do it.

Child advocate, Kenya[38]

Effective public awareness campaigns can change behaviours and reinforce that CSEA is preventable. They can also reduce the stigma around reporting, seeking justice, and seeking help for harmful sexual thoughts and behaviours. For example, following the UK National Crime Agency's awareness raising campaign on sexual extortion, the proportion of respondents who said they would share explicit images in an extortion scenario decreased significantly.[156] Similarly, data from the IWF show that after a campaign on non-consensual intimate image distribution, use of the **Report Remove** tool rose, even though the campaign did not specifically promote the tool.[157] However, campaign content, quality, and effectiveness vary, and few initiatives are formally evaluated. Recent examples of awareness raising campaigns include:

- **Help Children be Children** in Uganda and Zambia, which combined awareness raising campaigns with strengthening capacity of hotlines and law enforcement. The campaigns led to more reports and improved hotline staff knowledge.[157]
- **UNODC's Beware the Share**, interactive local-language campaigns, informed the public about grooming, sexting, and image-based abuse across five South-East Asian countries.[158]
- In response to a research finding that 70% of parents in Nepal were unaware of the risks and harms of online CSEA, ChildSafeNet partnered with TikTok to deliver digital safety training for children, parents, and educators across seven districts of Nepal.[159]

> I think everybody should be given awareness at a very early age regarding their [digital technologies] use and misuse and if such problems are coming then how can they tackle it. And in both ways, family, friends and every person should be aware.

19-year-old female, Nepal[38]

Responsible Behavior with Youth and Children (RBYC): Promoting healthy sexual norm development and addressing abuse by close-in-age peers

Developed by child sexual abuse and school-based violence prevention experts at MOORE | Preventing Child Sexual Abuse, Johns Hopkins Bloomberg School of Public Health.

RBYC is an evidence-based school curriculum for 11–14-year-olds that aims to prevent problematic sexual behaviour and help young adolescents develop safe, appropriate interactions – with younger children, their peers, and adults – both online and offline.[74] The programme consists of five interactive sessions supported by animated videos and classroom discussions.[74]

A high proportion of child sexual abuse is perpetrated by other children and adolescents. Early adolescence is a critical developmental stage, when young people are forming identities and sexual norms and may lack the skills or knowledge to navigate emerging relationships safely.[160,161] **RBYC** addresses these gaps through a trauma-informed, strengths-based approach. The curriculum can be delivered as a stand-alone program or integrated into existing health, sexuality education, or violence prevention curricula. Sessions cover:

- Healthy relationships and decision-making
- Personal boundaries and consent
- Developmental differences between teens and younger children
- Responsible and irresponsible behaviours in both online and offline contexts
- Identifying and preventing problematic sexual behaviours
- Safe adults and safe friends

RBYC includes take-home materials for families and adult-focused components for educators and parents/caregivers to encourage open communication and reinforce prevention messages at home and in school.

A randomised controlled trial of 160 students in the U.S. found that children who participated in **RBYC** demonstrated significant increases in self-efficacy to prevent sexual harm and improved knowledge about developmental differences, consent, and problematic sexual behaviours compared to those who did not receive the curriculum.

Beyond its U.S. trial, **RBYC** is being scaled and adapted globally. The curriculum has been adapted for use in Germany (with a 24-school randomised controlled trial underway) and in the Philippines (reaching 250 students as part of blended prevention programs).[162] In collaboration with the Kennedy Krieger Institute, **RBYC** has also been adapted for neurodiverse teens and enhanced with educational videos to increase accessibility and engagement.[8]

First-person generated sexual content involving children

> “Kids are going to be doing this [sexting] in the context of relationships, and how do we get them to do it in a way that isn’t going to come back to haunt them?”

Civil society[11]

Sharing of intimate images can be a normal part of adolescent relationships. However, the distribution and criminalisation of such content can cause harm, particularly when laws and policies fail to distinguish between adult-produced CSAM and first-person generated images involving children.

Evidence shows that fear-based or abstinence-only approaches are often ineffective and can discourage reporting and help-seeking.[163]

> “There was a social worker and a police officer there that were talking to us about it and saying that… if you send your own nude that’s still distributing child pornography so…I’m pretty sure half the people there sent nudes themselves…they were probably like ‘oh, there’s a police officer right there and they’re gonna arrest me in the middle of the gym.’”

17-year-old female[164]

Leaked: Insights on first-person generated sexual content in Thailand

- Young people commonly share and encounter sexual content online and primarily describe harm as occurring when they lose control over content.
- Approaches based in sexuality education may be more effective than stern warnings and threats against any sharing of sexual content.

Leaked is a 3-year partnership between the HUG Project, an NGO based in Chiang Mai and Bangkok-based research firm Evident, supported by World Childhood Foundation.[165,166,167] This initiative set out to better understand how young people in Thailand engage with – and make sense of – first-person generated sexual content. It includes a population-representative survey with 1,916 young people 9-17 years old in schools across Northern Thailand, and in-depth interviews with expert stakeholders. Insights from the data will inform new, tailored educational curricula in the final year of the project.[110]

More than one in three young people (36%) reported receiving or being shown sexual images of someone believed to be under 18. Motivations for sharing sexual content were varied. Many believed content was shared to gain likes and followers (46%), to earn money, gifts, or credit (45%), to feel good about themselves (40%), or to show trust in a relationship (27%).[110] One young person explained:

> **“Some of my friends and younger acquaintances have also shared nude images. When I asked about their motivations, they said they were seeking acceptance. They felt confident in their bodies but had not fully considered the potential consequences. These individuals are talented, yet they lack sufficient space and opportunities for self-expression. As a result, they engaged in this behaviour as a way to attract attention.”**

18-year-old key informant[110]

A notable proportion of respondents (34%) believed that young people share sexual content because they are pressured, tricked, or coerced. Young people also described how technology makes it too easy to share explicit sexual pictures impulsively, while at the same time offering little support when problems arise.[110]

Crucially, the **Leaked** project emphasises that the harms identified by young people do not stem from sharing intimate content itself, but from losing control over it. Unwanted sharing of first-person generated sexual images emerged as the top concern reported by young people (81%), following by regret (76%), bullying (70%), and emotional distress (68%).[110] This evidence challenges traditional fear-based approaches, which rely on stern warnings and legal threats to discourage sharing of any sexual content. Such messages fail to reflect the realities of young people's lives and may actually worsen stigma or discourage them from seeking help. Instead, the **Leaked** data supports an approach that calls for:

- Rights-based, comprehensive sexuality education that recognises the realities of technology in modern sexual interactions
- Stronger platform safety features to protect children from sexualised, sensational, or harmful content
- Cultural shifts – from punishment to support – in responding to issues arising from first-person generated sexual content
- Judgement-free spaces for open dialogue with young people about navigating online decisions

> **“I think we should just try to understand their situation and not victim blame. As this is prevalent in my country...People just hop on a bandwagon of insulting the person who was actually the victim.”**

17-year-old male, Pakistan[60]

Support for adults and children at risk of causing harm

> "It was the hardest thing I have ever done calling the helpline for the first time, but I am so glad I did. [It was the] first time in years I recognised my addiction to adult porn which led me to viewing other [CSAM] images. I have had great support and have never felt judged."
>
> *Anonymous caller to* **Stop It Now!**[112]

Perpetration prevention programs are an important prevention strategy supported by growing evidence.[28] They can provide early help for people concerned about their own sexual thoughts or behaviours towards children, interrupt pathways to offending, and prevent harm before it occurs. Harmful sexual thoughts and behaviours often begin in childhood, underscoring the need for early, tailored interventions for both adults and children at risk of causing harm.[168] Barriers to help-seeking can be reduced by providing multiple accessible options that prioritise anonymity and set clear confidentiality limits.[168] Examples of perpetration prevention initiatives are listed below:

- The **ReDirection** project surveys anonymous individuals searching for CSAM on the dark web and redirects them to support services, while generating data to inform effective prevention strategies.[169] With over 26,000 responses collected in multiple languages, the project has provided important insights into offending pathways and offenders' help-seeking behaviours. The **ReDirection Self-Help** programme has been assessed for scalability and is undergoing further evaluation.
- **Help Wanted,** an online course providing help to adolescents and young adults attracted to younger children, was developed in the U.S., and is now being adapted for Mexico and evaluated.[170]
- The **Stop It Now!** helpline provides confidential advice and support for people worried about their own or others' sexual thoughts or behaviours towards children. Support is available in over 200 languages. In 2023-24, nearly half of the 4,000 clients who called the helpline were adults seeking help for their own thoughts and behaviours, including those who had already harmed children.[112] Around 12% of those seeking help were unknown to authorities at the time of first contact, suggesting that helplines can reach at-risk individuals before law enforcement becomes involved.[112]
- **Prevention Global** is a knowledge platform and ambitious research initiative evaluating seven programs developed to prevent child sexual abuse perpetration, including individual and group therapy, remote counselling, self-guided materials, and school-based curricula. **Prevention Global** also publishes a knowledge product series and the **Scalability** release explores barriers to and opportunities for scaling prevention programs, including an assessment of programs with a particular focus on providing help-seeker services.[125]

> “We can see that for some offenders, they can be diverted from their offending behaviour. And if we focused on that more, then we would be doing a better job. But it’s really difficult for people to understand…It’s a very complicated narrative politically, socially, to accept…which makes it not very popular to talk about, not very popular to fund. But there is a growing evidence base that for some [people], you can intervene and divert [them] from the road that they’re on.”

Civil society[11]

Deterring searches for CSAM: Insights from Lucy Faithfull Foundation

Lucy Faithfull Foundation works to prevent child sexual abuse through professional services for individuals at risk of causing harm, families affected by abuse, and tools and resources for professionals to create safer environments for children.

- Offender typologies and pathways vary significantly, requiring tailored tactics and diverse, multi-channel messaging to reach different offender profiles.
- Warnings must be delivered at every point where someone might attempt to access illegal content.
- Messaging should be non-judgemental and carefully designed. Deterrence messaging alone cannot deter offending, but pairing messages with accessible, anonymous support can encourage people to seek help to address their sexual thoughts and behaviours.

> “The majority of the public would prefer to ‘other’ sexual offending. It’s something that happens to other people. Other people are offenders. Other people are victims….It does nothing for child protection. It does nothing for keeping kids safe…you’re not going to notice if your child is abusing your other child… you’re not going to notice if you’re only looking for monsters and predators.”

Civil society[11]

Lucy Faithfull Foundation has pioneered deterrence messaging through campaigns across online and offline channels, including conventional news media, social media, paid digital advertising, short films, and partnerships with law enforcement and other statutory and voluntary organisations.[171]

Over eleven years of deterrence messaging and campaigning, the Lucy Faithfull Foundation identified four core messages that effectively warn those searching for CSAM:

- Accessing sexual images of children is a crime.
- It causes harm to children.
- It carries consequences for you and your family.
- Anonymous help is available if you want to stop.

Lucy Faithfull Foundation, in partnership with IWF and Aylo (an adult content platform), tested whether anonymous chatbot-based deterrence messages could disrupt and reduce searches for CSAM on Pornhub UK. Aylo maintains a dynamic list of thousands of terms banned due to their association with sexual images of children. When a user searches for one of these terms on Pornhub UK, a static warning message appears. Additionally, a chatbot pops up, resembling a standard customer-service box commonly seen on other websites. Based on user responses, the chatbot may direct individuals to anonymous support services, including the **Stop It Now!** helpline, email or live-chat support, online self-help resources, the National Suicide Prevention Lifeline, or the National Health Service urgent mental health services.[171]

An evaluation of the intervention found that:[171]

- 82% of sessions searching for illegal content were interrupted. Some users ended their session entirely, while others switched to legal content or left the site.
- The combination of the warning message and chatbot effectively encouraged people to seek support from **Stop It Now!** services.
- When the chatbot was disabled for a month, searches for CSAM increased.

Impact of the project by numbers

- There was a statistically significant reduction in searches for sexual images of under-18s over the 18-month project.
- The chatbot and warning message were shown 2.8 million times.
- 99.8% of searches during the 18-month project did not trigger the chatbot or warning message.
- 1,656 people requested information about helpline services after seeing the chatbot or warning message.
- 490 people visited the **Stop It Now!** website after seeing a warning message or chatbot.
- 68 **Stop It Now!** helpline callers were identified as having interacted with the chatbot.

Accessible, trusted reporting options and survivor-centred support

> "The governments, tech companies and educational institutions should… ensure children can report anywhere and anytime…And then the necessary actions can be taken in order to help reduce it."

24-year-old female, Uganda[38]

A range of accessible, trusted reporting mechanisms are needed to link children who have experienced harm to comprehensive, child-friendly, survivor-centred support services. Evidence consistently shows that children rarely use formal reporting channels. For example, **Disrupting Harm** found that only around 3% of children subjected to sexual exploitation or abuse online reported to a helpline or police, compared to 40% who told friends and 24% who told siblings.[60]

> "I prefer talking to adults because I feel they'll have more ideas…the adults that I talk to listen to me well, especially my sister."

17-year-old female, Nigeria[60]

> "I usually don't talk to adults. I usually talk to people my own age, because they're going through similar things and can relate more easily, and I know adults mean well, but sometimes it feels like they might not fully get it, or might see it differently, and…it's better to talk to my own age people."

15-year-old female, Ethiopia[60]

> "I think that a lot of people might not [talk to parents] because they feel that they'll be restricted from their phone if they tell…maybe a lot of children might feel guilty, especially with sexual abuse. They might feel guilty and that it's also their fault."

15-year-old female, UK[60]

Youth advocates emphasise that reporting must be easy to access and use, stigma-free, and trustworthy.[60] Some youth suggest peer-led models, such as trained adolescents who can respond effectively and direct their peers to appropriate support services.[60] Other examples in practice include:

- **Meri Trustline**, a helpline in India that supports children, women, and people from marginalised identities who are at risk of online harm.[172] Reports submitted through WhatsApp, email, or phone are received by trained counsellors. The platform also integrates the IWF's **Report Remove** tool which enables children to report online content and seek to have it removed.[173]
- Child-centred multidisciplinary service models for child victims of sexual abuse and exploitation, such as **Barnahus** (Children's House), which provides co-located child-friendly, trauma-informed services including forensic interviews, medical examinations, therapeutic services, and victim/family support. **One Stop Centres** are another example: they provide immediate crisis response and support services for women and children subjected to gender-based violence, particularly in low- and middle-income countries. Their comprehensive, co-located services include legal services, social services, and counselling.[174] UNICEF is examining how these models of care can support children subjected to technology-facilitated CSEA.[174] Documented experiences from the Philippines, South Africa, Nigeria and Bulgaria will be forthcoming soon.[174]
- Prevention Global's **Serving Youth** knowledge products include a **Practical desk guide for leaders** of youth organisations that highlights eight systematic practices to prevent and address child sexual abuse.[175, 176] Research shows a decrease in victimisation prevalence of more than 20% in youth serving organisations that implemented child sexual abuse prevention strategies.[180]

> **“In my opinion, the best way would be listening to them without judging, believing what they say, give access to counselling or help, and making sure they know they are not alone, because it would mean a lot... feeling safe, being heard, having support to recover, and also making sure the people who did it are held accountable.”**

15-year-old female, Ethiopia[38]

Digital safety

> “As we continue to build these digital worlds, we have to make sure we're building them with safety in mind. It's not just about giving young people access to cool new tech - it's about giving us the tools to protect ourselves, teaching us how to recognise when something feels off, and creating spaces where we can enjoy all the benefits of these innovations without the lurking dangers.”

Youth advocate[1]

Children's safety, rights, and well-being should be prioritised across all levels of company culture, governance, and workforce training.

Companies should integrate child rights impact assessments, child safety due diligence and child-centred design features throughout development processes.

Companies must proactively detect and disrupt harmful content and behaviours, in addition to reactive moderation.

Transparency, accountability, and cross-sector collaboration are essential to strengthen global defences against technology-facilitated CSEA.

Promote an industry culture of child safety

Creating a safer digital ecosystem for children requires an industry culture that prioritises children's rights, safety, and well-being across all levels of company culture, governance, decision-making, and workforce training. Child safety should be emphasised as a professional responsibility from the pipeline stage, including computer science curricula and industry hiring pathways.[32] Staff involved in the design, development, and delivery of digital products and services should receive ongoing training to recognise and mitigate risks to children. Child safety should also be integrated into company safeguarding policies and codes of conduct. In 2024, the Cambodian government trained 48 digital technology companies on industry guidelines for child online protection – four of these trained companies subsequently integrated child protection into their internal policies and developed a child protection code of conduct for their staff.[159]

Frontline content moderators and digital safety workers, described as the 'essential safety workers of the internet', perform vital, difficult work, but often face precarious conditions and risks to their own health and well-being. They should be supported with fair employment conditions, professional development, access to mental health and psychosocial support services, and post-employment support.[181] Such measures can improve workforce retention, enhance expertise, and improve the quality and effectiveness of frontline digital safety responses.

Make safety by design the default

A safety by design approach requires all stakeholders involved in designing and developing digital products and services to ask: "what would we do differently if we knew the end user was a child?"[182] It shifts the responsibility to companies to ensure that their products do not cause harm to children. Importantly, these safety measures should apply across all digital technologies, since children often access products and services that were not specifically created for them.[183] Several civil society experts noted a perception that commercial interests take precedence over child rights and safety considerations.[184] Industry representatives maintain that a safety by design approach need not conflict with commercial interests.[7]

Key features of safety by design include:[31]

- Integrating child rights impact assessments and due diligence into design and development processes. Child rights impact assessments are processes that enable companies to assess how their operations, products, and services affect children's rights, as defined in the UN Convention on the Rights of the Child and other human rights instruments.[185]
- Privacy and data protection, including strict privacy defaults, age-appropriate user experiences, and safeguards against the misuse of children's personal data.
- Child-centred design and education, such as engaging children and youth in designing and testing products, providing clear and accessible information, and building in educational features that increase children's agency and awareness.
- Built-in protections such as parental controls, contact limits, financial safeguards to prevent children transferring money online, and limited functionality modes or devices.
- Accountability through clear transparency reporting obligations, robust moderation, and accessible reporting and redress mechanisms.

Child safety features should be functional, accessible, and equitably available across all geographic regions and languages in which a product or service is offered.

> **“If you open an [social media] account here in Latin America and the Global South, the question was will they have the same kind of protections and safeguards that people that have an account in US and UK [have], and the answer was, absolutely no!...People here in Latin America are less safe than children in other countries. And why must that be?”**
>
> *Civil society*[11]

A complementary framework, child rights by design, recognises that digital technologies should support the realisation of children's rights, including their right to safety.[186] Applying these approaches requires leadership commitment, dedicated resources, and trained staff. Smaller companies and start-ups often lack this capacity, though guidance is available to help companies evaluate the child rights impacts of digital technologies, including generative AI.[36,184,187–189] Effective implementation of safety by design principles should be guided by evidence and requires industry transparency and independent accountability mechanisms.

Table 1. Examples of safety by design and child rights by design in practice

Design element	Action	Examples in practice
Product safeguards	Integrate safety risk assessments into product development.	UNICEF's **D-CRIA ToolBox** guides businesses on conducting robust child rights impact assessments and due diligence related to the digital environment. It includes a D-CRIA template, quick start guide, and spotlight guidance for child participation and engagement.[185] Thorn's **Responsible AI Framework** and **Safety by Design Checklist** for technology platforms aims to decrease risks associated with generative AI.[188]
Product safeguards	Design child-safe devices or modes with limited functionality or access. Enhanced features may be unlocked by a parent or caregiver.	**HMD Fuse** is a child-safe smartphone with a built-in AI content filter which blocks nude content from being viewed, recorded, or stored. It begins in a restricted mode with no apps or social media access unless caregivers enable additional features.[190] Apple **Communication Safety** is enabled by default for child accounts. It scans images and videos on-device to detect and automatically blur nudity, warns the child, and provides age-appropriate safety guidance and resources, and allows parental control via Screen Time settings.[191]
Privacy and data protection	Apply strict privacy defaults and safeguards, and collect minimal data from child accounts, or when user age is uncertain.	Social media teen accounts, such as **Snapchat Teen mode**, may make accounts private, restrict direct messaging, filter harmful content, and disable location sharing by default.[192] **YouTube Kids,** for children under 13, filters content, disables comments, location sharing, and personalised ads by default.
Child-friendly communication, education, and reporting mechanisms	Provide age-appropriate, child-friendly information, education, and reporting/complaint mechanisms.	Google's **Be Internet Awesome** digital safety curriculum includes interactive games on online safety, privacy, and respectful sharing.[193] LEGO developed a child-friendly code of conduct. The now defunct LEGO Life app's **Captain Safety** tool incorporated a safety pledge, in-app safety reminders, and child-friendly explanations of LEGO's privacy and moderation policies.[194] Instagram's **School Partnership** programme offers digital safety resources and prioritises reports of harmful content and accounts submitted by students and educators, ensuring review within 48 hours.[195]

> “When she was a teenager, she was looking for a reason to say no. And he kept pressuring her [to send more sexual images], and she couldn't fight...She couldn't say no...But, 'my phone won't let me take nudes' seems like a really powerful way of giving that power back to those victims to say they can't. 'Yeah. Not me – the device won't let me.'”

Civil society[11]

Proactively detect and disrupt harm

Technology companies should proactively detect and block harmful content, accounts, and behaviours in real-time using tools such as hash matching systems and content monitoring filters, while respecting users' rights.[73] Efforts to harness AI and machine learning for proactive content detection are emerging, including a grooming detection service that uses machine learning and a proposed CSAM detection intelligence system shown to accurately distinguish between CSAM and non-CSAM posts on the dark web while generating actionable insights about creators and victims.[196,197] Thorn's **Safer** product is a suite of AI-powered tools companies can use to detect, identify, and report CSAM. **Safer** was integrated into OpenAI's DALL-E2 generative AI web app.[198]

The Tech Coalition is testing a proof of concept for detecting and responding to technology-facilitated CSEA in livestreaming environments.[199] This pilot will use metadata signals, such as session characteristics and the use of anonymisation services, to generate a risk score that indicates the likelihood of CSEA online occurring within a given livestream session for further investigation by child safety teams. Testing and evaluation will take place in 2026 to assess feasibility for broader industry adoption.

Children must be able to immediately report their concerns and harmful content and behaviours they encounter online —including CSAM, sexual extortion, grooming, or unwanted image distribution—through simple, trusted, in-platform channels.[60] Reporting should trigger timely responses to remove content and block harmful accounts, as well as connect users to support services and follow-up.

Many digital products do not offer accessible reporting mechanisms, and even when they are available, children often do not use them. A global study on sexual extortion found that **only 4% of children reported incidents to the platform where they occurred**.[52] Youth advocates emphasised that the experience of reporting and requesting takedown of sexual images is as important as the function itself: it must be easy, safe, and free from stigma. As a positive example, NCMEC's **Take It Down** service reassures children with non-stigmatising messaging ('having nudes online is scary, but there is hope to get it taken down'), multilingual support, explainer videos, and FAQs.[200] OECD (Organisation for Economic Co-operation and Development) guidance stresses that redress systems must be designed with children's input and adapted to platform-specific risks.[182]

> “I think that [some digital platforms]…they're sort of focused more on their profit than the [children's] safety. Something that could definitely help is improving reporting mechanisms on the platform, because I think a lot of the time it's very tricky to actually find where to report, and there's not much on how it actually works. And a lot of the time, you don't really hear back from them. So, you kind of feel like it's hopeless and like there's no point in doing that reporting anyway.”

15-year-old female, UK[60]

Transparency and accountability

Stronger commitments to transparency and accountability are essential. Companies should conduct mandatory child rights impact assessments and publish timely transparency reports that capture risks, harms, and user behaviours that can inform prevention strategies. These may include, for example, victim and perpetrator demographics, and rates of session abandonment or click-throughs to support services triggered by warning popups. Standardising child safety metrics and reporting processes across industry can address current challenges with data comparability. The Tech Coalition's **Lantern** programme highlights the need for an ecosystem where data, insights, and responsibilities are shared across sectors to strengthen child protection online.

Lantern – coordinated industry action against CSEA online: Insights from the Tech Coalition

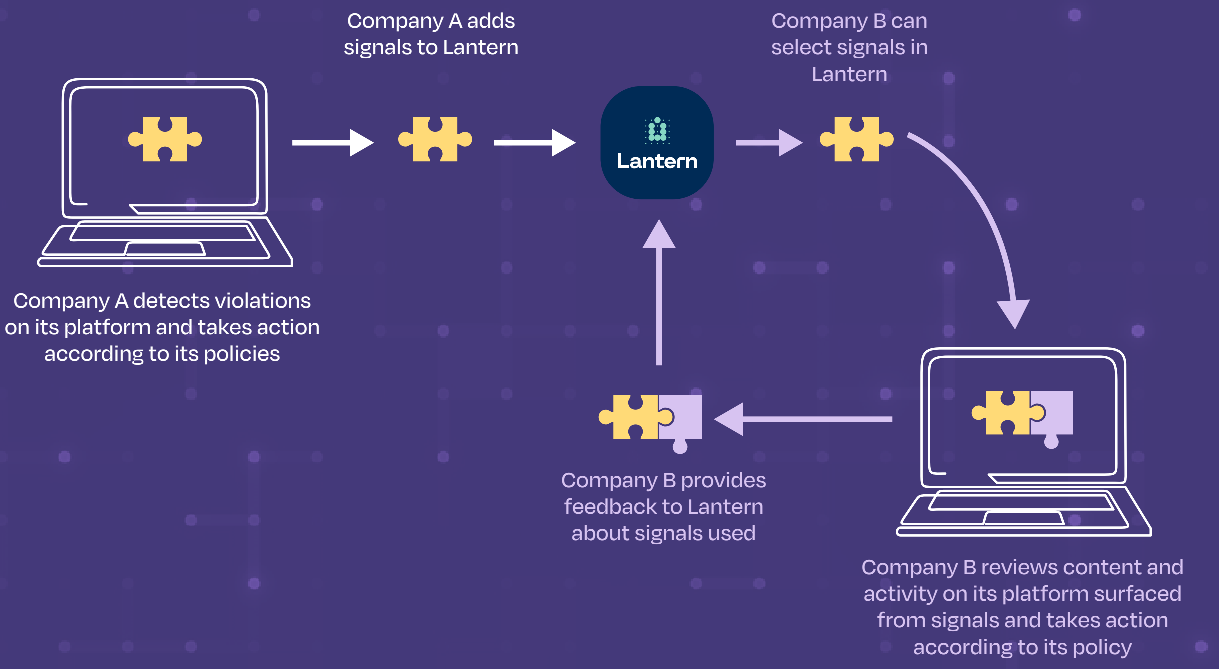
The Tech Coalition is a global alliance of over 55 technology companies committed to protecting children from sexual exploitation and abuse online by sharing knowledge, identifying threats, and developing collaborative solutions.

Perpetrators often use multiple platforms to share abusive content and exploit children online. Historically, there was no universal framework to coordinate across industry efforts to detect exploitation and abuse, leaving gaps in detection and response. **Lantern** was created to close this gap by enabling participating companies to share actionable signals of abuse, allowing for the detection and response to harms that might otherwise go unnoticed.[201]

Operating on the principle that sharing threat intelligence enhances industry response to CSEA online, Lantern facilitates collaboration to strengthen collective defences against emerging threats. Signals – such as hashes, URLs, or usernames – represent potentially harmful content or behaviour relevant to CSEA online. When one platform flags a signal, others can independently review related activity on their own services.[25]

When a company identifies CSEA on its platform, it takes appropriate action to uphold its child safety policies and shares the associated signals through **Lantern**. This allows other platforms to proactively detect and remove related content or accounts, strengthening the overall online safety ecosystem.

Figure 6. **Lantern's** signal sharing framework and process[25]


Company A adds signals to Lantern
Company B can select signals in Lantern
Lantern
Company A detects violations on its platform and takes action according to its policies
Company B provides feedback to Lantern about signals used
Company B reviews content and activity on its platform surfaced from signals and takes action according to its policy

Collaboration through **Lantern** is already demonstrating impact, with participating companies noting steady improvements in their ability to mitigate child safety risks.[201] In 2024:

- Nearly 300,000 new CSEA online-related signals were shared — bringing the total to over 1 million total **Lantern** signals to date.
- 100,000+ accounts were enforced against for violations related to child sexual exploitation and abuse.
- 135,000+ URLs hosting or transmitting CSEA were blocked or removed.
- 7,000+ pieces of CSAM were removed.
- High-risk cases, including 81 incidents of contact sexual offenses and 45 trafficking-related cases, were flagged.

Most incident-based signals involved perpetrators seeking to distribute or obtain CSAM, sometimes as precursors to grooming or contact abuse.[201] **Lantern's** taxonomy of signals allows for more precise categorisation of threats, supporting multiple approaches to detection and response.[201]

Figure 7. Uploaded signals by type in 2024

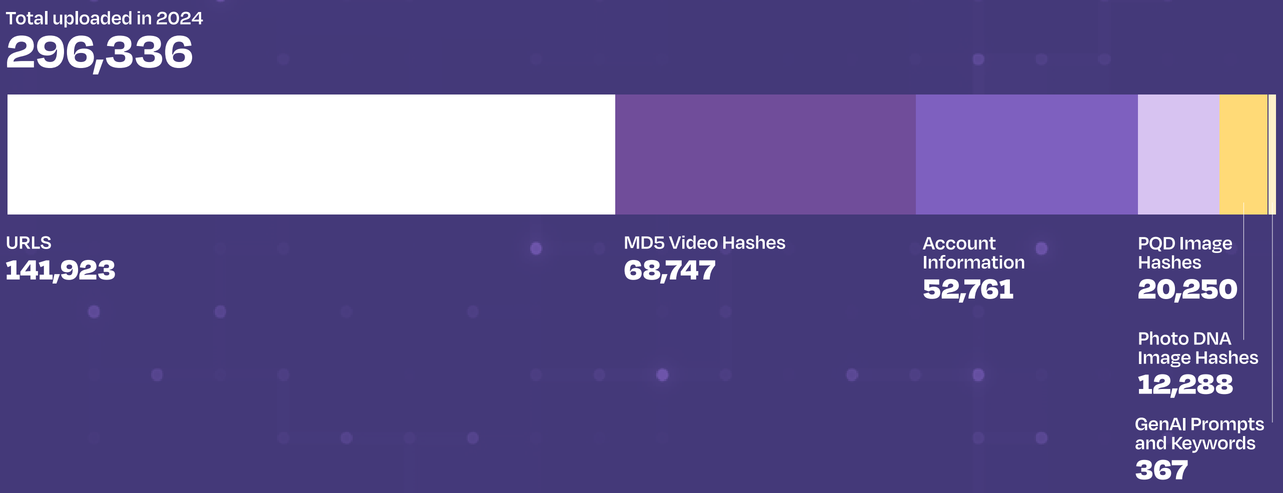
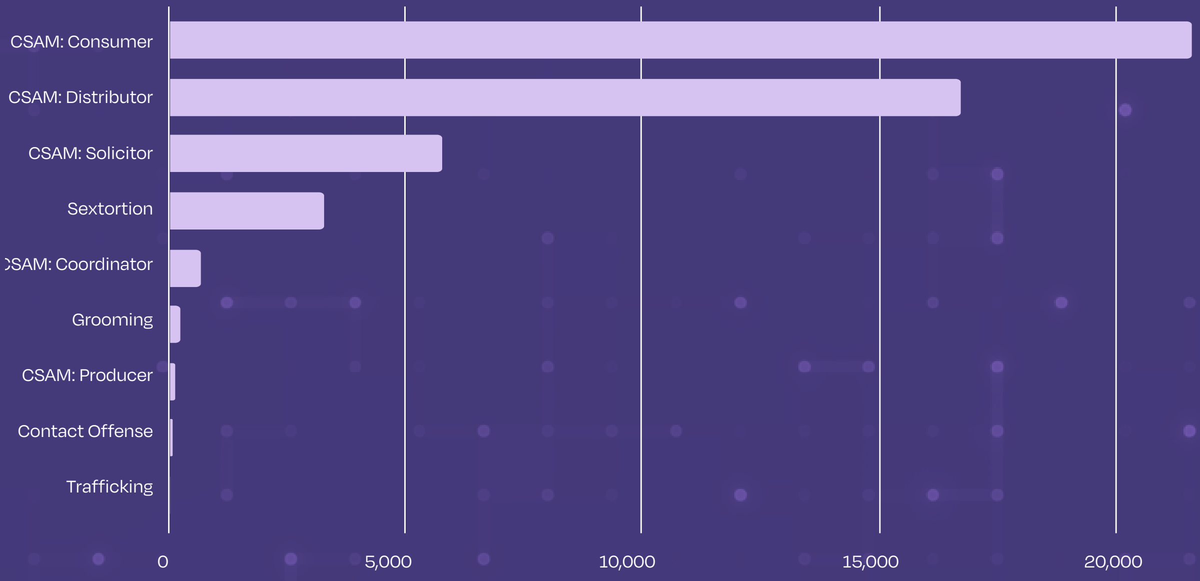


Figure 8. Categories of incident-based signals reported in 2024



Lantern demonstrates the power of cross-industry collaboration in tackling child exploitation and abuse online. By breaking down silos between platforms, the program has improved detection, perpetrator accountability, and speed of response. Importantly, it also demonstrates how sharing signals related to content and behaviour can strengthen defences against broader threats like grooming, extortion, and trafficking in addition to the distribution of CSAM.

> **"What really resonated with me was the importance of it takes a village…everybody needs to be involved in prevention."**

Industry[7]

Law, policy, and justice

> “I think we need more regulation, legislation. And I think that’s the same with smoking, with substance abuse. We don’t let children smoke. We don’t let children drink. We have legislation. So, it has taken too long for us to regulate the internet.”

Civil society[11]

Harmonising legislation is essential to close legal loopholes, ensure cross-border cooperation, and keep pace with emerging digital threats.

Effective implementation of laws depends on well-resourced, trauma-informed, and survivor-centred justice systems that protect children and do not re-traumatise them.

Addressing technology-facilitated CSEA requires collaborative action across government, regulators, industry, and civil society to hold duty-bearers accountable.

Harmonising legislation globally in line with child rights standards

Efforts to harmonise national legislation addressing technology-facilitated CSEA are gaining momentum globally. The **UN Convention Against Cybercrime** is a landmark multilateral anti-crime treaty that advances efforts to standardise global child protection laws, including by criminalising CSAM and grooming for the first time globally.[23] Comprehensive laws such as the **UK Online Safety Act** help to minimise inconsistencies that naturally exist when legislating across government ministries and issue areas.[8,202] Fiji’s recent comprehensive Child Safeguarding Policy, enacted in 2025, aligned the previous **Care and Protection Act 2024** and the **Child Justice Act 2024.** It also sought to minimise loopholes and improve coordination across sectors.[203] However, globally, inconsistencies remain in legislative efforts both within and between governments. The lack of a centralised system for monitoring legislative developments and sharing developments further compounds the global challenge of legislative inconsistency. Comparative tools like the Brave Movement’s **#BeBrave G7 Country Scorecard** and the **Online Safety Regulatory Index** highlight progress and gaps.[204,205]

> “So much [sexual extortion] comes from foreign countries... but everyone’s got their own jurisdictions and laws, and no one wants to work together [so] that it becomes so hard for us to say, ‘don’t do this to kids’.”

Survivor[77]

Brazil's 2025 advances in child protection online

In 2025, Brazil marked a milestone in digital child protection through policy actions that reflect growing leadership from countries in the Global Majority in shaping safer online environments. In September, Brazil enacted a comprehensive law that sets clear obligations for companies and platforms to prevent, detect, and respond to CSEA online.[19] The law introduces a duty of prevention, requires the prompt removal of illegal content without court orders, and mandates reporting to national authorities. The law also embeds safety- and privacy-by-design principles, prohibits targeted advertising to children, and establishes strict age assurance rules, including parental account linkage for users under 16. Platforms must provide parental control tools in Portuguese, publish transparency reports, and enable research access to data on children's digital well-being. Enforcement will be led by Brazil's National Data Protection Agency.[19]

Multi-sector consultations, including with industry and child rights organisations, are essential to ensure that laws keep pace with emerging technological threats and align with child rights standards, while also enabling innovation that enhances child safety. Views on how to best protect children through legislation remain mixed: one industry expert advocated for legislative safe harbours (with strict safeguards) to pilot and pressure-test detection tools, while a civil society representative cautioned that some mandatory reporting laws can inadvertently restrict voluntary, timely reporting.[7,11]

Age assurance in the digital age: Balancing protection and participation

- Age assurance describes the methods used to verify or estimate an online user's age to ensure access to age-appropriate content. Methods involves trade-offs between accuracy, privacy, and equity.
- Recent laws requiring age verification have drawn public attention to online child safety risks and surfaced a range of ethical, practical, and policy challenges. They may lead to unintended consequences, such as users circumventing restrictions or exclusion of marginalised groups.
- Age assurance can enhance children's safety online, but without meaningful consultation with children and young people, implementation risks undermining their rights.
- Age restrictions must not reduce the importance of family, school, and community-based interventions, nor minimise the importance of company responsibility and child rights impact assessments in relation to digital environments.

Global legislative trends

Since the last Global Threat Assessment, many countries have introduced age-assurance and online-safety laws:[206]

- Brazil: approved legislation including comprehensive age-verification obligations in September 2025.[19]
- United Kingdom: required platforms to prevent young people from encountering harmful content, including use of 'highly effective' age assurance (e.g., ID or facial estimation) on pornography sites and large social media platforms, as of July 2025.[202]
- Australia: will restrict children under 16 years old from social media from December 2025.[207]
- Singapore: requires app-store age verification for downloads from Google Play, Apple, and Huawei stores.[21]

Additional localities that considered or recently adopted similar legislation include Denmark, Malaysia, Mongolia, New Zealand, South Korea, Türkiye, the European Union, and Uzbekistan.[50,51]

> **“A lot of laws developed for young people are not [really] developed for young people. For example, the current bans on social media for under 16s – young people were not consulted enough. Young people should be in the room while the laws are being drafted and developed, not just at the consultation stage.”**

22-year-old female, Australia[38]

Children’s perspectives

Children and youth acknowledge the value of online safety laws, while emphasising the need for nuance in their design and implementation. A nationally representative survey of children aged 8–17 years in Australia found that nearly 90% supported age checks to access websites, while 56% of surveyed US teens supported requirements for age verification on social media.[208,209] Yet, young people also highlight concerns about privacy, security, and digital inclusion.

> **“If you want protection, there needs to be some sacrifice of freedom. But as a young person, I also have the right to explore and discover things [in the digital world].”**

Young person[38]

Critics of blanket bans warn that restricting access can exclude or isolate marginalised youth, such as sexual and gender minority populations, or undocumented children, and push them toward unregulated digital spaces.[210] Evidence from the UK shows that VPN use spiked after restrictions, highlighting the challenges of enforcement in a digitally connected world.[211]

> **“When a child needs access to streaming platforms but does not have an account, they use illegal sites which bring up inappropriate pop-up ads with explicit content.”**

Child advocate, Kenya[38]

> “Alt [alternative] accounts is a big issue. If anyone gets banned, they can set up a new account. [There are] so many different ways to get around bans or moderations.”

13-year-old female, Australia[38]

Balancing safety, privacy, and rights

Advocates argue that “age assurance should not be about keeping children out; it should be about letting them in – safely”.[186] The African Union’s **Child Online Safety and Empowerment Policy** (2024) adopts this rights-based approach, promoting access alongside prevention.[212]

> “Age assurance is a tool, not an end in itself, for positive online youth experiences. At its best, it protects; at its worst, it bars young people from essential information, expression and connection.”

Regulator[206]

2. Age assurance methods[213]

Method	Description	Key concerns
Self-declaration	User enters a birth date or checks a box.	Easy to implement, but unreliable.[214]
Age estimation	Predicts age via algorithms or biometrics.	Convenient but prone to bias and errors—studies show up to 34–73% error rates among teens and racial biases.[207,215]
Age verification	Requires official ID or verified signal.	Most accurate, but raises privacy, security, and exclusion concerns, especially for those without formal ID.[216]

No global standard for age assurance yet exists. Meta has proposed on-device or app-store-based checks, while Google explores zero-knowledge proofs that confirm eligibility without revealing identity. Policymakers and companies must ensure systems are transparent, rights- respecting, privacy-preserving, equitable, and co-designed with children.

Capacity building, child-friendly response, and survivor-centred justice

Laws to protect children must be backed by investments in training, capacity building, and dedicated regulators. Governments should ensure that law enforcement, prosecutors, and the judiciary receive ongoing training in child-friendly, trauma-informed approaches and have the resources to apply them effectively. Survivors across regions report that existing legislative protections are either insufficient or poorly enforced and call for survivor-centred justice.[60]

> If you report to the police... they will laugh at you. That's why we need cybercrime units.

Survivor advocate[60]

In Kenya, the National Council on the Administration of Justice launched a specialised training handbook for justice sector actors on investigating and prosecuting technology-facilitated CSEA .[217] This initiative reflects recognition of the need for tailored child-friendly and trauma-informed practice within the justice system, moving beyond legislation to supporting effective survivor-centred responses.

> Legal systems should make it easy for them to report abuse without fear, and online platforms should work quickly to remove any harmful content.

15-year-old male, Ethiopia[60]

Proactive detection, independent of survivor complaints, is crucial. Tools like Thorn's CSAM classifier (via INTERPOL) and Rigr AI's AI-powered video summariser enhance timely response to livestreamed CSEA.[218,219]

Law enforcement consistently notes that more resources are needed to handle the growing number of reports received by hotlines, as reports exponentially increase, in part due to generative AI. Additional capacity is also required to support hotline staff and first responders' well-being, and to finance proactive investigations that can cut off production and consumption of CSAM.[79] Cambodia's police training on technology-facilitated CSEA illustrates how to build inclusive, child-centred systems.[220] Similarly, the Canadian Association of Chiefs of Police has adopted a framework for trauma-informed policing, built around six steps, the **Six 'R' Model**: Realize, Recognize, Rethink, Respond, Reduce, Review.[221] When systems are trauma-informed and child-friendly, they reduce the harm of victim-blaming, which discourages reporting, worsens long-term impacts, and weakens detection and response.

> Especially in my country, I've never seen them blame the person who's grooming. It's always, 'Why would you? It's your own phone, why would you let this happen?'

14-year-old female, Ethiopia[60]

Global cross-sector coordination to address financial sexual extortion

Global coordination across sectors, including law enforcement, government, industry, and service providers is essential for effective prevention, particularly in cases of sexual financial extortion. ECPAT recommends further strengthening cross-sector measures by:[222]

- Mandating financial institutions to actively detect and report transactions linked to sexual exploitation of children.
- Adapting surveillance tools for emerging trends including digital wallets and cryptocurrencies.
- Reforming bank secrecy laws to enable collaboration with police services beyond financial police.

Preventing sexual extortion of children online: Insights from the Australian Federal Police-led Australian Centre to Counter Child Exploitation

Data released by the Australian Centre to Counter Child Exploitation (ACCCE) in 2023 identified an emerging trend: overseas offenders primarily targeting teenage boys for financial sexual extortion.[223] More than 90% of reports relating to financial sexual extortion involved young male victims. Reports of online financial sexual extortion targeting Australian children increased by nearly 60% between December 2022 and the start of the 2023 school year, suggesting a surge during school holidays.[223]

Since January 2024, the ACCCE has recorded a decline in reports of financial sexual extortion, likely due to coordinated law enforcement activity, prevention messaging, and educational efforts. However, many incidents are believed to go unreported, and sexual extortion of children remains a significant concern and priority.

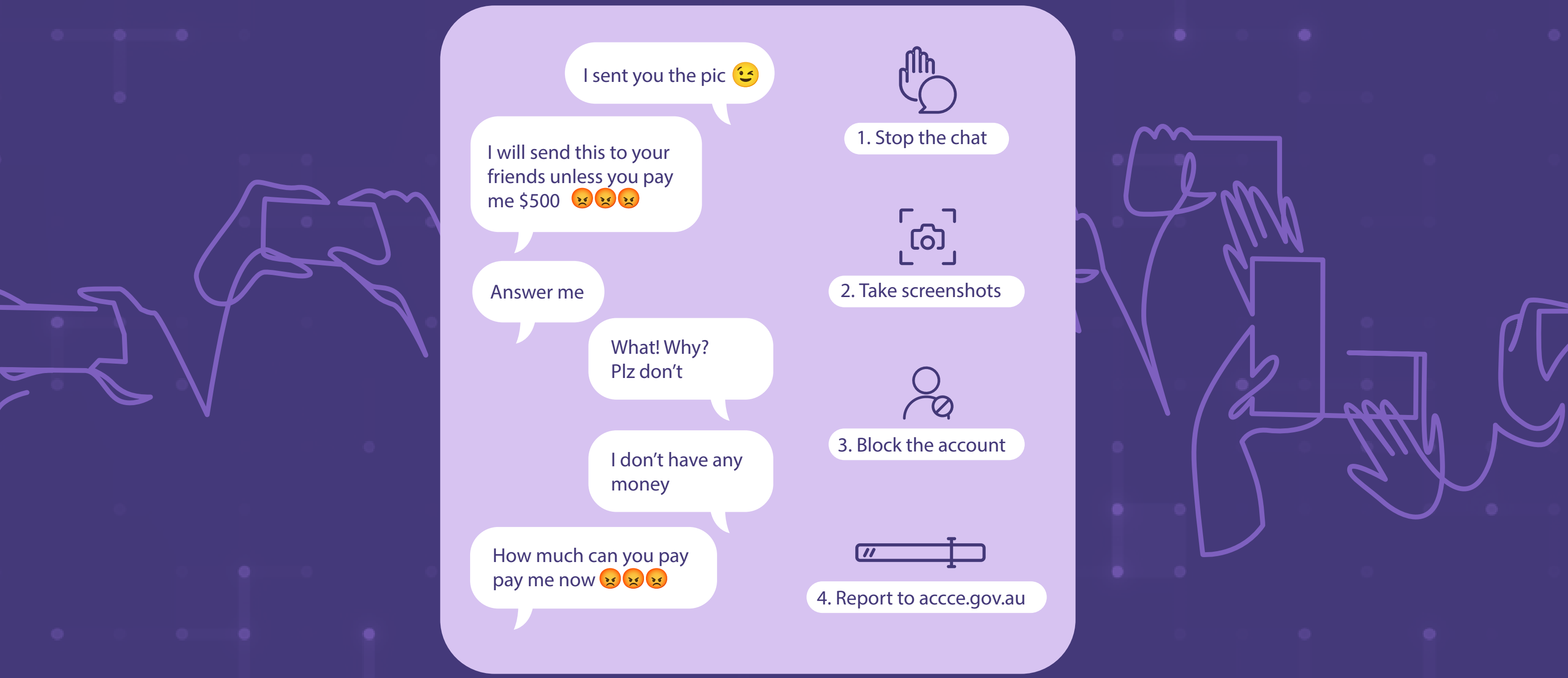
A central feature of the ACCCE's approach is cross-sector collaboration to deliver prevention messages at scale.

> “It's a whole network and ecosystem that you need for prevention to be successful.”
>
> *Law Enforcement*[79]

Partnerships bring together law enforcement, industry, NGOs, and community organisations to reach diverse audiences with tailored interventions. Examples include:

- Targeted youth outreach: The ACCCE has worked with Kids Helpline, Meta, and the U.S. youth prevention program **NoFiltr** to release educational resources for 13–17-year-olds, providing information on how to prevent and respond to sexual extortion. These materials also guide parents and caregivers on recognising risks, reporting incidents, and accessing support.[223]
- Family-focused prevention: The ACCCE collaborated with Project Paradigm on **It's Never Too Early,** a campaign encouraging parents, carers, and expectant families to start early conversations about child sexual abuse prevention.[224]
- Mass communication campaigns: To reach high-risk groups directly, the ACCCE developed a 30-second animated advertisement for boys aged 13–17, shown on Snapchat, which reached an estimated five million people.[79,225]

Figure 9. Animated sexual extortion campaign on Snapchat



I sent you the pic 😉

I will send this to your friends unless you pay me $500 😡😡😡

Answer me

What! Why? Plz don't

I don't have any money

How much can you pay pay me now 😡😡😡

1. Stop the chat
2. Take screenshots
3. Block the account
4. Report to accce.gov.au

- Education and training: **ThinkUKnow**, led by the Australian Federal Police, equips schools, families, and community groups with practical tools to address online safety and sexual extortion risks. Resources include presentations, fact sheets, conversation cards, activity packs, and culturally tailored materials for linguistically diverse communities, offering multiple entry points for discussions about online risks.[152]

While the ACCCE actively collects participation data—such as the number of presentations delivered and audiences reached—measuring the true impact of prevention efforts remains challenging, as many outcomes are not directly visible in the data. The ACCCE's approach focuses on equipping parents and caregivers with practical tools and information, recognising their key role in supporting children's online safety. Ongoing efforts aim to reach families less likely to engage and to strengthen education and awareness initiatives across all communities.

Conclusion

Technology-facilitated CSEA is a preventable global threat. The task ahead is clear: close evidence gaps, identify and scale up what works, and accelerate the translation of knowledge into action. In a constrained funding environment, this means maximising impact through shared knowledge and evidence, coordinated agendas, and lessons drawn from offline CSEA and broader violence prevention efforts. To build a safer digital world, we must fortify the weakest links, recognising that risks and harms migrate to the least protected spaces, and ensure that every child benefits from the same level of protection. Effective prevention depends on placing children's rights and voices at the centre, investing in sustainable, evidence-based action; and strengthening collaboration across all sectors and stakeholders. Through shared responsibility, the global community can accelerate progress toward a safer digital environment where children can learn, play, and connect free from exploitation and abuse.

> **From pain to purpose, from survival to strength.**

Survivor, Philippines[138]

Acknowledgements

Suggested citation: WeProtect Global Alliance (2025). Global Threat Assessment 2025, Preventing technology-facilitated child sexual exploitation and abuse: From insights to action (by Lau LS, Mayevskaya Y, Fanton d'Andon C, Ware M, and Hermosilla S). WeProtect Global Alliance: https://www.weprotect.org/global-threat-assessment-25/

Authors

WeProtect Global Alliance

WeProtect Global Alliance is a global movement bringing together more than 350 government, private sector and civil society organisations working to transform the global response to child sexual exploitation and abuse online.

Care and Protection of Children (CPC) Learning Network, Columbia University

The CPC Learning Network, housed at Columbia University's Mailman School of Public Health, advances child health and well-being through research, policy, and practice. With partners in over 20 countries, the CPC generates rigorous, locally grounded evidence and tools to strengthen child protection systems and promote the well-being of children, youth, and families globally.

This report was researched and written by Ling San Lau, Yana Mayevskaya, Sabrina Hermosilla, Cécile Fanton d'Andon, and Matthew Ware, with additional contributions from Claire Cunningham, Hannah Thompson, Cassie Landers, Hanna-Tina Fischer, Jonathan Huynh, and Lisberma Peralta Aquino.

WeProtect Global Alliance would like to thank all of the organisations and individuals who supported the development of the Global Threat Assessment 2025. We gratefully acknowledge the children and survivors whose experiences and insights informed this report and guide collective efforts to keep children safe. Support provided to the report's development, as a member of the Steering Committee or a contributor, does not imply endorsement (in part or in full) of the contents of this report.

Expert Steering Committee

Aengus Ó Dochartaigh	MOORE | Preventing Child Sexual Abuse, Johns Hopkins University
Afrooz Kavani Johnson	UNICEF
Anil Raghuvanshi	ChildSafeNet
Beth Hepworth	PGI
Carolina Piñeros	RedPapaz
Dan Sexton	Internet Watch Foundation (IWF)
Debra Clelland	DeafKidz International
Elena Martellozzo	Childlight, Global Child Safety Institute, University of Edinburgh
James Smith	PGI
Jess Lishak	Tech Coalition
Nina Vaaranen-Valkonen	Protect Children
Ricardo de Lins e Horta	Brazil Government
Sambath Sokunthea	Cambodian Government
Soyoung Park	South Korean Regulator, KCSC
Wirawan Boom Mosby	The HUG Project Thailand

Contributors

The following organisations provided survivor and youth insights to inform our research:

VoiceBox

A UK-based, youth-led social enterprise amplifying the voices of young people aged 13–25. VoiceBox hosted two sessions with young people aged 14–18 from seven countries, including marginalised communities, refugees, and survivors of genocide. Their insights inform the report and the prevention framework.

Secrets Worth Sharing

A UK-based organisation promoting open discussion about childhood sexual abuse through podcasts, workshops, and events. Secrets Worth Sharing reviewed qualitative research tools and contributed survivor perspectives incorporated into the report.

Marie Collins Foundation

Supports victims and/or survivors of technology-assisted child sexual abuse, as well as their families and the professionals who work with them, providing advocacy, education, and recovery services. The Marie Collins Foundation reviewed qualitative research tools, contributed survivor insights, and facilitated a workshop with survivors to review the prevention framework.

International Justice Mission (IJM) Philippines

A global organisation tackling human trafficking, modern-day slavery, and exploitation and abuse of children. IJM contributed survivor insights relevant to the prevention framework and integrated throughout the report.

Footprints to Freedom

A Netherlands-based, survivor-led organisation empowering survivors of human trafficking; implementing grassroots interventions in Uganda, Kenya, and Rwanda; and scaling initiatives across Africa through their African Survivor Coalition. Footprints to Freedom contributed survivor perspectives incorporated throughout the report.

Protect Children

Based in Helsinki, Protect Children advocates for the right of every child to be free from sexual violence, develops prevention programmes, and researches and rehabilitates offenders. Protect Children contributed a survivor foreword and additional insights included throughout the report.

In addition to our Expert Steering Committee, the following individuals and organisations offered their insights to guide this research:

- ECPAT
- European Union
- Global Online Safety Regulators Network (GOSRN)
- Google
- INHOPE
- International Criminal Police Organization (INTERPOL)
- Lucy Faithfull Foundation
- National Center for Missing & Exploited Children (NCMEC)
- National Crime Agency (NCA)
- National Organisation for the Treatment of Abuse (NOTA)
- Safe Futures Hub
- Snap
- Virtual Global Taskforce (VGT)
- World Economic Forum

Safe Futures Hub

The prevention framework was developed as part of the Safe Futures Hub, a joint initiative of the Sexual Violence Research Initiative (SVRI), Together for Girls, and the WeProtect Global Alliance, which works to advance solutions to end sexual violence against children.

Visual design and layout of the report was developed by Rec Design. The prevention framework was visually designed by Together Creative.

Staying current with emerging evidence

Table 3. Select pending publications and living resources

Initiative name	Description	Anticipated
Disrupting Harm 2 (research conducted jointly by UNICEF Innocenti, ECPAT, and INTERPOL)	Expansion of population-based surveys with children and caregivers, as well as trauma-informed in-depth interviews with young survivors in 12 additional countries, to improve global understanding of child sexual exploitation and abuse online.	2025-2026
Global Boys Initiative (ECPAT)	An upcoming publication will feature a case study from Pakistan with survivor and practitioner testimonials, highlighting initiatives to prevent and respond to boys' sexual exploitation.	2025-2026
INSPIRE: Seven Strategies for Ending Violence Against Children (developed by WHO with global partners)	**INSPIRE** is an evidence-based technical package outlining seven strategies and two cross-cutting activities to prevent violence against children aged 0-17. It supports countries in coordinating multi-sector action and tracking progress.	Ongoing
Prevention Global (delivered by MOORE | Preventing Child Sexual abuse, Johns Hopkins Bloomberg School of Public Health and The Royal's Institute of Mental Health Research)	Launched in 2024, **Prevention Global** is a knowledge platform and ambitious research initiative evaluating 7 programs developed to prevent child sexual abuse perpetration and leading gold-standard perpetration prevalence surveys across four continents (Brazil, Germany, Tanzania, and the U.S.).[176] It also publishes knowledge products exploring key aspects of prevention, including **Serving Youth**, covering victimisation prevalence in U.S. youth-serving environments and providing a practical desk guide for leaders; **Scalability**, exploring barriers and opportunities for scaling programs; and **Making The Case**, revealing public perception of child sexual abuse as a preventable issue.[125,176,226]	2026

Initiative name	Description	Anticipated
Responsible Behavior with Youth and Children (RBYC)[74]	**RBYC** is a program for 11–14-year-olds that aims to prevent problematic sexual behaviour and help young adolescents develop safe, appropriate interactions – with younger children, their peers, and adults – both online and offline. It has been tested in the U.S. and is currently being adapted and evaluated across 24 schools in Germany (22 in randomised controlled trials and 2 in pilot studies).	2026
Safe Futures Hub Global Living Systematic Review and PbK Framework	Safe Futures Hub, in collaboration with Oxford University, is developing a **Global Living Systematic Review** to provide continuously updated evidence on preventing childhood sexual violence, with a focus on low- and middle-income countries. In December 2025, the Hub will also launch its **Practice-Based Knowledge (PbK) Framework**, which recognises lived expertise, brings in underrepresented voices, and highlights why and how interventions succeed in real-world contexts.	2025-2026

Glossary of terms

Artificial Intelligence (AI)-generated child sexual abuse material (CSAM)

The misuse of AI technologies to wholly or partly create any sexualised or sexually explicit representation of a child. This includes images, videos, audio, animations, or other media produced by AI. It is a form of digitally generated CSAM (DG-CSAM) (see related, deepfakes).[26]

Bundling

A feature that consolidates related reports of widespread incidents, such as viral content, into a single report or smaller set of reports, reducing redundant submissions while retaining information on all reported users and incidents.[12]

Chatbots

An automated conversational tool, often powered by AI, that can simulate children or adults and interact with users as companions, advisors, or friends, but may pose risks such as misinformation, data collection, or exposure to inappropriate content.[59]

Child sexual abuse material (CSAM)

Material, such as images or videos, that depicts and/or documents acts that are sexually abusive and/or exploitative to a child. Such material can be used in criminal intelligence investigations and/or serve as evidence material in criminal court cases.[26]

Child sexual abuse online

Any form of sexual abuse of children which has a link to the digital environment. This includes the sexual abuse of children that is facilitated by technology and committed elsewhere and then repeated by sharing it online through social media or other digital dimensions.[26]

Child sexual exploitation online

All acts of a sexually exploitative nature carried out against a child that have a connection to the digital environment. This includes any use of technology that results in sexual exploitation or causes a child to be sexually exploited or that results in or causes images or other material documenting such sexual exploitation to be produced, bought, sold, possessed, distributed, or transmitted. Compared with *abuse*, the exchange or distribution of things of value, including but not limited to images or videos, are often components of exploitation.[26]

Deepfake

A deepfake is AI-generated content (e.g., a photo, video, animation or audio) that realistically depicts a person doing or saying something they never did.[227] It may be used to refer to content depicting real children in simulated sexualised situations.

Digital well-being

Impact of technologies on an individual's mental, physical, social, and emotional health.[228]

End-to-end encryption

A security method that ensures only the sender and intended recipient can access the contents of a communication, preventing third parties including service providers from viewing or scanning the data.[229]

First-person generated/produced sexual content involving children

Children and adolescents under 18 years may take sexual pictures or videos of themselves. While this conduct in itself is not necessarily illegal or socially unacceptable, there are risks that any such content can be circulated online or in-person to harm children or be used as a basis for extortion. We use this term, as well as 'sexting', which is a common colloquial reference to taking and sharing images that are sexual in nature. Children often share that they do not relate to the notion of 'self-generated' content and in contexts such as non-consensual sharing, it may be unhelpful.[233]

Generative Artificial Intelligence (AI)

Generative AI is a form of artificial intelligence that uses machine learning models to analyse the patterns and structure of its training data in order to create new content, including text, images, audio, or other media, that mimics those inputs.[230]

Grooming

Grooming or online grooming refers to the process of establishing/building a relationship with a child either in person or through the use of the internet or other digital technologies to facilitate sexual contact with that person. In the report, grooming without qualifiers refers to grooming for sexual purposes.[26]

Harmful sexual behaviours

Sexual actions initiated by a child or young person that are developmentally inappropriate, coercive, or abusive, and may cause harm to themselves or others. Problematic sexual behaviour refers to sexual actions that may be inappropriate or concerning but do not meet the threshold for harm or abuse. This report uses the term harmful sexual behaviours to capture the full spectrum of concerning behaviours, while recognising that early-stage or less severe behaviours still require intervention to prevent them from escalating.[108]

Hash matching

An algorithm known as a hash function is used to compute a fingerprint, known as a hash, from a file. Comparing such a hash with another hash stored in a database is called hash matching. In the context of online safety, hash matching can be a primary means for the detection of known illegal or otherwise harmful images and videos.[231]

Livestreamed abuse

Often transmitted to viewers through dedicated livestreaming platforms or social media, the content is delivered instantaneously, allowing viewers to watch and engage while the abuse is occurring. Compared with other formats, this may leave less of a digital footprint of the abuse.[26]

Non-consensual sharing of intimate imagery (NCII)

A term commonly associated with adults that refers to sharing sexual or sexually suggestive imagery without the consent of the person depicted. This may arise when content initially shared consensually is later shared or forwarded without consent, or when pictures are taken without consent (such as in the context of grooming or sexual extortion). The key concept is the 'loss of control' over the depictions.[26] This term requires caution when used in relation to children who have not reached the age of sexual consent (see related, first-person generated/produced sexual content involving children).

Offender

Person who has committed offences or is guilty of a crime involving child sexual exploitation and abuse.[26]

Online enticement

When an individual communicates with a child through the internet (or other technology) intending to commit a sexual offense or abduction.[232]

Perpetrator

A person who may have engaged in sexual exploitation of children (irrespective of their engagement in the criminal justice process). We use the term perpetrator and potential perpetrator to refer to people who have, or may, engage in these acts regardless of whether they have met the specific definition of a crime or been arrested/convicted of a crime.[26]

Sexual extortion of children

A process whereby children are coerced into continuing to produce sexual material and/or to perform distressing acts under threat of exposure to others of the material that depicts them. When the motivation is primarily financial, we also use the term 'financial sexual extortion'.[26]

Survivor

People who have suffered harm and victimisation. The use of the term 'survivor' may be reflective of a process of healing. Recognising the variety of preferences people with lived experience have for terminology, we use the terms 'victim' and 'survivor' interchangeably in the report.[26]

Technology facilitated child sexual exploitation and abuse (technology-facilitated CSEA, also referred to as TFCSEA)

Technology-facilitated CSEA refers to the use of digital technologies at any stage to prepare, commit, or disseminate (in the case of CSAM) the sexual exploitation or sexual abuse of a child. It encompasses harms committed in both digital and non-digital (offline) environments - including, for example, exchanging information, coordinating actions, and contacting children to groom or coerce them. This term acknowledges that technology plays a role in facilitating abuse, and perpetuating the harms caused by abuse, in both physical and digital spaces.[26]

Victim

People who have been subjected to harmful and/or criminal acts as rights-holders. Recognising the variety of preferences people with lived experience have for terminology, we use this term interchangeably with 'survivor' in the report.[26]

References

1. Navigating the Unknown: Reflections on AI, the Metaverse, and Keeping Young People Safe | VoiceBox [Internet]. [cited 2025 Sept 27]. Available from: https://voicebox.site/article/navigating-unknown-reflections-ai-metaverse-and-keeping-young-people-safe

2. MOORE | Preventing Child Sexual Abuse | Johns Hopkins Bloomberg School of Public Health [Internet]. [cited 2025 Sept 27]. Available from: https://publichealth.jhu.edu/moore-center-for-the-prevention-of-child-sexual-abuse

3. United Nations Department of Economic and Social Affairs [Internet]. Global Internet Use Continues To Rise But Disparities Remain. [cited 2025 Nov 20]. Available from: https://social.desa.un.org/sdn/global-internet-use-continues-to-rise-but-disparities-remain

4. GSMA. Smartphone owners are now the global majority, New GSMA report reveals [Internet]. Newsroom. 2023 [cited 2025 Nov 4]. Available from: https://www.gsma.com/newsroom/press-release/smartphone-owners-are-now-the-global-majority-new-gsma-report-reveals/

5. ITU. Statistics [Internet]. [cited 2025 Nov 21] . Available from: https://www.itu.int/en/ITU-D/Statistics/pages/stat/default.aspx

6. Generative AI: Risks and opportunities for children | Innocenti Global Office of Research and Foresight [Internet]. [cited 2025 Aug 29]. Available from: https://www.unicef.org/innocenti/generative-ai-risks-and-opportunities-children

7. Industry. Data collected by the CPC Learning Network through key informant interviews.

8. Academic. Data collected by the CPC Learning Network through key informant interviews.

9. Intergovernmental. Data collected by the CPC Learning Network through key informant interviews.

10. Safe Online. Disrupting Harm [Internet]. Available from: https://safeonline.global/wp-content/uploads/2023/12/DH-data-insights-8-151223.pdf

11. Civil Society. Data collected by the CPC Learning Network through key informant interviews.

12. National Center for Missing and Exploited Children. CyberTipline Data [Internet]. [cited 2025 Sept 3]. Available from: https://ncmec.org/gethelpnow/cybertipline/cybertiplinedata

13. INHOPE Releases Annual Report 2024 [Internet]. [cited 2025 May 5]. Available from: https://inhope.org/EN/articles/inhope-annual-report-2024

14. IWF 2024 Annual Data & Insights Report [Internet]. [cited 2025 May 6]. Available from: https://www.iwf.org.uk/annual-data-insights-report-2024/

15. How AI is being abused to create child sexual abuse material (CSAM) online [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/

16. 118th Congress. S.474 - REPORT Act [Internet]. 2024. Available from: https://www.congress.gov/bill/118th-congress/senate-bill/474

17. UK Public General Acts. Online Safety Act 2023 [Internet]. 50 Oct 26, 2023. Available from: https://www.legislation.gov.uk/ukpga/2023/50

18. Social media ban in Australia | A simple guide [Internet]. UNICEF Australia. [cited 2025 Sept 27]. Available from: https://www.unicef.org.au/unicef-youth/staying-safe-online/social-media-ban-explainer?srsltid=AfmBOop6gJckegYUrtle7BkiDMa6ZKUVy0aaGjHrYShDthWRHUqp8_9A

19. Presidência da República, Casa Civil, Secretaria Especial para Assuntos Jurídicos. LEI No 15.211, DE 17 DE SETEMBRO DE 2025 [Internet]. Available from: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/L15211.htm

20. Presidência da República, Casa Civil, Secretaria Especial para Assuntos Jurídicos. LEI No 15.100, DE 13 DE JANEIRO DE 2025 [Internet]. Available from: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/lei/l15100.htm

21. New Online Safety Code of Practice for App Distribution Services Enhances Protection for Singapore Users [Internet]. Infocomm Media Development Authority. [cited 2025 Aug 29]. Available from: https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2025/online-safety-code-of-practice-for-app-distribution-services

22. Making the digital and physical world safer: Why the Convention against Cybercrime matters | UN News [Internet]. 2024 [cited 2025 Sept 27]. Available from: https://news.un.org/en/story/2024/12/1158526

23. UN Cybercrime Convention - Full Text [Internet]. United Nations : Office on Drugs and Crime. [cited 2025 Aug 25]. Available from: //www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

24. Global Digital Compact | Office for Digital and Emerging Technologies [Internet]. [cited 2025 Sept 10]. Available from: https://www.un.org/digital-emerging-technologies/global-digital-compact

25. Lantern: advancing child safety through signal sharing [Internet]. https://technologycoalition.org/. [cited 2025 Sept 27]. Available from: https://technologycoalition.org/programs/lantern/

26. ECPAT. Terminology Guidelines [Internet]. 2025 [cited 2025 Aug 29]. Available from: https://ecpat.org/terminology/

27. Call for consultants, global Living Systematic Review consultant(s):... [Internet]. Safe Futures Hub. [cited 2025 Sept 27]. Available from: https://www.safefutureshub.org/call-for-consultants-global-living-systematic-review-consultants-what-works-to-prevent-childhood-sexual-violence

28. Prevention Global. Prevention Global launches with new online resource hub and landmark impact evaluations [Internet]. [cited 2025 Sept 27]. Available from: https://www.prevention.global/

29. Model National Response to end child sexual exploitation & abuse online - WeProtect Global Alliance [Internet]. 2020 [cited 2025 May 1]. Available from: https://www.weprotect.org/resources/frameworks/model-national-response/

30. Bronfenbrenner U. Toward an experimental ecology of human development. Am Psychol. 1977;32(7):513–31.

31. UNICEF. Corporate reporting on child rights in relation to the digital environment [Internet]. Available from: https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/reporting

32. Workshop. Data collected by the CPC Learning Network through key informant interviews.

33. Convention on the Rights of the Child, 20 November 1989 [Internet]. [cited 2025 Sept 10]. Available from: https://ihl-databases.icrc.org/en/ihl-treaties/crc-1989

34. OHCHR. General comment No. 25 (2021) on children's rights in relation to the digital environment [Internet]. OHCHR. [cited 2025 Nov 3]. Available from: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

35. United Nations. Guiding Principles on Business and Human Rights : Implementing the United Nations "Protect, Respect and Remedy" Framework [Internet]. Available from: https://digitallibrary.un.org/record/720245?v=pdf

36. UNICEF. Children's Rights Business Principles 2012 [Internet]. [cited 2025 Nov 3]. Available from: https://www.unicef.org/media/96136/file/Childrens-Rights-Business-Principles-2012.pdf

37. WeProtect Global Alliance. Children and Young People present their roadmap for a safer digital world [Internet]. Available from: https://www.weprotect.org/news/children-and-young-people-present-their-roadmap-for-a-safer-digital-world/

38. SafetyNet: insights from young people around the world [Internet]. Safe Futures Hub. [cited 2025 Sept 22]. Available from: https://www.safefutureshub.org/resources/safetynet-insights-from-young-people-around-the-world

39. Thorn. Evolving Technologies Horizon Scan [Internet]. Available from: https://www.thorn.org/research/library/evolving-technologies-horizon-scan/

40. UNICEF. Childhood in a Digital World [Internet]. [cited 2025 Nov 20]. Available from: https://www.unicef.org/innocenti/reports/childhood-digital-world

41. 10 countries with the highest percentage of web traffic from mobile phones | Business Insider Africa [Internet]. [cited 2025 Aug 29]. Available from: https://africa.businessinsider.com/local/lifestyle/10-countries-with-the-highest-percentage-of-web-traffic-from-mobile-phones/04wvy3f

42. Facts and Figures 2024 - Youth Internet use [Internet]. [cited 2025 Aug 29]. Available from: https://www.itu.int/itu-d/reports/statistics/2024/11/10/ff24-youth-internet-use

43. Slater SO, Arundell L, Grøntved A, Salmon J. Age of first digital device use and screen media use at age 15: A cross-sectional analysis of 384,591 participants from 55 countries. Public Health Pract [Internet]. 2025 June 1 [cited 2025 Sept 2];9:100596. Available from: https://www.sciencedirect.com/science/article/pii/S2666535225000151

44. Coded Companions: Young People's Relationships With AI Chatbots | VoiceBox [Internet]. [cited 2025 Sept 27]. Available from: https://voicebox.site/article/coded-companions-young-peoples-relationships-ai-chatbots

45. Snap Digital Well-Being Index | Snapchat Safety [Internet]. [cited 2025 Sept 27]. Available from: https://values.snap.com/safety/dwbi

46. Häubi RB. How the UN plans to connect every school to the internet by 2030 [Internet]. SWI swissinfo.ch. 2024 [cited 2025 Sept 2]. Available from: https://www.swissinfo.ch/eng/international-geneva/the-un-plans-to-connect-every-school-to-the-internet-by-2030/83325727

47. Peng D, Yu Z. A Literature Review of Digital Literacy over Two Decades. Educ Res Int [Internet]. 2022 [cited 2025 Sept 3];2022(1):2533413. Available from: https://onlinelibrary.wiley.com/doi/abs/10.1155/2022/2533413

48. World Health Organization. 1st Global Ministerial Conference on Ending Violence Against Children [Internet]. [cited 2025 Nov 4]. Available from: https://www.who.int/teams/social-determinants-of-health/violence-prevention/1st-global-ministerial-conference-on-ending-violence-against-children

49. INHOPE. Launching Version 3 of the Universal Classification Schema [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://inhope.org/EN/articles/what-s-new-in-version-3-of-the-universal-classification-schema

50. WeProtect Global Alliance. Child protection online: Global legislative, regulatory and policy update January 2025.

51. WeProtect Global Alliance. Child protection online: Global legislative, regulatory and policy update June 2025.

52. Patchin JW, Hinduja S. The nature and extent of youth sextortion: Legal implications and directions for future research. Behav Sci Law. 2024;42(4):401–16.

53. MikeHarrison. Global Taskforce on child sexual abuse online - WeProtect Global Alliance [Internet]. 2022 [cited 2025 Nov 3]. Available from: https://www.weprotect.org/global-taskforce-on-child-sexual-abuse-online/

54. Government. Data collected by the CPC Learning Network through key informant interviews.

55. Transparency reporting on child sexual exploitation and abuse online [Internet]. 2023 Sept [cited 2025 Sept 30]. (OECD Digital Economy Papers; vol. 357). Report No.: 357. Available from: https://www.oecd.org/en/publications/transparency-reporting-on-child-sexual-exploitation-and-abuse-online_554ad91f-en.html

56. Grossman S, Pfefferkorn R, Thiel D, Shah S, DiResta R, Perrino J, et al. The Strengths and Weaknesses of the Online Child Safety Ecosystem. 2024 Apr 22 [cited 2025 Sept 5]; Available from: https://purl.stanford.edu/pr592kc5483

57. Childlight Into the Light Index [Internet]. [cited 2025 Apr 30]. Available from: https://www.childlight.org/into-the-light

58. 2024 Annual Report [Internet]. National Center for Missing & Exploited Children. [cited 2025 Aug 25]. Available from: http://www.missingkids.org/content/ncmec/en/footer/about/annual-report.html

59. UNICEF. The risky new world of tech's friendliest bots [Internet]. Available from: https://www.unicef.org/innocenti/stories/risky-new-world-techs-friendliest-bots

60. Data from the youth consultations led by Voicebox.

61. Davis P. Spike in online crimes against children a "wake-up call" [Internet]. National Center for Missing & Exploited Children. [cited 2025 Sept 27]. Available from: http://www.ncmec.org/content/ncmec/en/blog/2025/spike-in-online-crimes-against-children-a-wake-up-call.html

62. Deepfake Nudes & Young People: Navigating a New Frontier in Technology-facilitated Nonconsensual Sexual Abuse and Exploitation [Internet]. Thorn. [cited 2025 Sept 5]. Available from: https://www.thorn.org/research/library/deepfake-nudes-and-young-people/

63. Online child sex abuse material, boosted by AI, is outpacing Big Tech's regulation [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/news-media/iwf-in-the-news/online-child-sex-abuse-material-boosted-by-ai-is-outpacing-big-techs-regulation/

64. Thiel D, DiResta R, Stamos A. Cross-Platform Dynamics of Self-Generated CSAM. 2023 June 6 [cited 2025 Aug 25]; Available from: https://fsi.stanford.edu/publication/cross-platform-dynamics-self-generated-csam

65 How Instagram's Algorithm Connects and Promotes Pedophile Network - Tech News Briefing - WSJ Podcasts [Internet]. [cited 2025 Aug 25]. Available from: https://www.wsj.com/podcasts/tech-news-briefing/how-instagrams-algorithm-connects-and-promotes-pedophile-network/A683C0B4-2E6F-4661-9973-10BD455DB895

66. AI enabling 'DIY child abuse' tools, with child victims in models, IWF warns MPs [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/news-media/news/ai-giving-offenders-diy-child-sexual-abuse-tool-as-dozens-of-child-victims-used-in-ai-models-iwf-warns-mps/

67. Aws Ai, Hugging Face, Inflection, Metaphysic, Stability AI, Teleperformance. Safety by Design for Generative AI: Preventing Child Sexual Abuse. Thorn [Internet]. 2024; Available from: https://info.thorn.org/hubfs/thorn-safety-by-design-for-generative-AI.pdf

68. Thorn. Synthetic Media Framework Case Study: Thorn. [cited 2025 Nov 4]; Available from: https://partnershiponai.org/wp-content/uploads/2024/11/case-study-thorn.pdf

69. Sivathasan N, Clahane P, Kemoli D. TikTok profiting from sexual livestreams involving children, BBC told. BBC [Internet]. 2025 Mar 2; Available from: https://www.bbc.com/news/articles/cedl8eyy4pjo

70. Ovaska A, Insoll T, Soloveva V, Vaaranen-Valkonen N, Di GR. Findings from Italian language respondents to Re-Direction surveys of CSAM users on dark web search engine. JRC Publ Repos [Internet]. 2025 [cited 2025 Nov 3]; Available from: https://publications.jrc.ec.europa.eu/repository/handle/JRC138231

71. FATF Annual Report 2023-2024 [Internet]. [cited 2025 Sept 30]. Available from: https://www.fatf-gafi.org/en/publications/Fatfgeneral/FATF-Annual-report-2023-2024.html

72. Protect Children. Tech Platforms Used by Online Child Sexual Abuse Offenders [Internet]. 2024. Available from: https://www.suojellaanlapsia.fi/en/post/tech-platforms-child-sexual-abuse

73. Ending the Scourge: The Need for the STOP CSAM Act — Testimony of Michelle DeLaune, President and CEO, National Center for Missing & Exploited Children (PDF) [Internet]. Room 226, Dirksen Senate Office Building, Washington, DC; 2025 [cited 2025 Sept 5]. p. 16. Available from: https://www.judiciary.senate.gov/imo/media/doc/2025-03-11_testimony_delaune.pdf

74. Responsible Behavior with Youth and Children | MOORE | Preventing Child Sexual Abuse [Internet]. [cited 2025 Sept 5]. Available from: https://publichealth.jhu.edu/moore-center-for-the-prevention-of-child-sexual-abuse/responsible-behavior-with-youth-and-children

75. The emergence of immersive technologies and Extended Reality - WeProtect Global Alliance [Internet]. [cited 2025 May 1]. Available from: https://www.weprotect.org/thematic/extended-reality/

76. Child safeguarding and immersive technologies [Internet]. NSPCC Learning. [cited 2025 Aug 25]. Available from: https://learning.nspcc.org.uk/research-resources/2023/child-safeguarding-immersive-technologies

77. Data from Marie Collins Foundation survivor consultation session.

78. Edwards G, Christensen L. Cyber strategies used to combat child sexual abuse material [Internet]. Australian Institute of Criminology; 2021 [cited 2025 Nov 4]. Available from: https://www.aic.gov.au/publications/tandi/tandi636

79. Law enforcement. Data collected by the CPC Learning Network through key informant interviews.

80. Walsh K, Mathews B, Parvin K, Smith R, Burton M, Nicholas M, et al. Prevalence and characteristics of online child sexual victimization: Findings from the Australian Child Maltreatment Study. Child Abuse Negl. 2025 Feb;160:N.PAG-N.PAG.

81. Under 10s groomed online 'like never before' in 2023 find IWF [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/news-media/news/under-10s-groomed-online-like-never-before-as-hotline-discovers-record-amount-of-child-sexual-abuse/

82. Girls & Young Women-Led Assessment on Online Sexual Exploitation, Abuse & Technology-Facilitated Gender-Based Violence in Africa [Internet]. ECPAT. [cited 2025 May 1]. Available from: https://ecpat.org/resource/girls-young-women-led-assessment-on-online-sexual-exploitation-abuse-technology-facilitated-gender-based-violence-in-africa/

83. Protecting Children From Violence and Exploitation in Relation to the Digital Environment | UNICEF [Internet]. [cited 2025 Sept 5]. Available from: https://www.unicef.org/documents/protecting-children-violence-and-exploitation-relation-digital-environment

84. Huang TF, Chun-Yin H, Fong-Ching C, Fong-Ching C, Chiu CH, Ping-Hung C, et al. Adolescent Use of Dating Applications and the Associations with Online Victimization and Psychological Distress. Behav Sci [Internet]. 2023;13(11):903. Available from: https://pubmed.ncbi.nlm.nih.gov/37998650/

85. Technology-facilitated Child Sexual Exploitation and Sexual Abuse in Burkina Faso, Côte d'Ivoire, Guinea and Niger [Internet]. ECPAT. [cited 2025 Sept 5]. Available from: https://ecpat.org/resource/technology-facilitated-child-sexual-exploitation-and-sexual-abuse-in-burkina-faso-cote-divoire-guinea-and-niger/

86. Pinto Cortez, Cristián & Guerra, Cristobal. Parental styles and online sexual abuse prevention factors. 2024. Límite (Arica). 19. 1-9. 10.4067/s0718-50652024000100209. Available from: https://www.researchgate.net/publication/383135600_Parental_styles_and_ online_sexual_abuse_prevention_factors

87. Wright MF. The Associations among Cyberbullying Victimization and Chinese and American Adolescents' Mental Health Issues: The Protective Role of Perceived Parental and Friend Support. Int J Environ Res Public Health [Internet]. 2024;21(8). Available from: https://pubmed.ncbi.nlm.nih.gov/39200678/

88. Friedman-Hauser G, Katz C. "She has a history of making things up": Examining the disclosure and reporting of online sexual abuse among children with disabilities. Child Abuse Negl [Internet]. 2025;163 ((Friedman-Hauser G., galf@haruv.org.il) The Bob Shapell School of Social Work, Tel Aviv University, Israel). Available from: https://awspntest.apa.org/record/2026-05574-001

89. Wright MF, Wachs S. Longitudinal
Associations between Different Types of Sexting, Adolescent Mental Health, and Sexual Risk Behaviors: Moderating Effects of Gender, Ethnicity, Disability Status, and Sexual
Minority Status. Arch Sex Behav [Internet]. 2024 Mar 1 [cited 2025 Sept 30];53(3):1115–28. Available from: https://doi.org/10.1007/s10508-023-02764-7

90. Gemara N, Mishna F, Katz C. 'If my parents find out, I will not see my phone anymore': Who do children choose to disclose online sexual solicitation to? Child Fam Soc Work [Internet]. 2025 [cited 2025 Sept 5];30(1):4–14. Available from: https://onlinelibrary.wiley.com/doi/abs/10.1111/cfs.13069

91. Lusky-Weisrose E, Klebanov B, Friedman-Hauser G, Avitan I, Katz C. Online sexual abuse of children with disabilities: Analyzing reports of social workers' case files in Israel. Child Abuse Negl. 2024 Aug;154:N.PAG-N.PAG.

92. Hong JS, Kim J, Lee JM, Saxon S, Thornberg R. Pathways from Polyvictimization to Offline and Online Sexual Harassment Victimization Among South Korean Adolescents. Arch Sex Behav. 2023 Oct;52(7):2779–88.

93. Tanaya NLTP, Puteri NMM. Child Sexual Abuse and Exploitation through Livestreaming in Indonesia: Unequal Power Relations at the Root of Child Victimization. J Int Womens Stud [Internet]. 2023 Apr;25(3):1–14. Available from: https://vc.bridgew.edu/jiws/vol25/iss3/6

94. Children P. What Drives Online Child Sexual Abuse Offending? Understanding Motivations, Facilitators, Situational Factors, and Barriers [Internet]. Protect Children. 2024 [cited 2025 Aug 31]. Available from: https://www.suojellaanlapsia.fi/en/post/2know-final-report-1

95. Napier SS, Seto MC, Cashmore J, Shackel R. Characteristics that predict exposure to and subsequent intentional viewing of child sexual abuse material among a community sample of Internet users. Child Abuse Negl. 2024 Oct;156:106977.

96. Lahtinen HM, Honkalampi K, Insoll T, Nurmi J, Quayle E, Ovaska AK, et al. Investigating the disparities among child sexual abuse material users: Anonymous self-reports from both charged and uncharged individuals. Child Abuse Negl. 2025 Mar;161:107299.

97. Chauviré-Geib K, Gerke J, Fegert JM, Rassenhofer M. The Digital Dimension: Victim's Experiences of Technology's Impact on Penetrative Child Sexual Abuse. J Child Sex Abuse. 2025 Apr 28;1–21.

98. Christensen LS, Woods J. "It's Like POOF and It's Gone": The Live-Streaming of Child Sexual Abuse. Sex Cult. 2024 Aug 1;28(4):1467–81.

99. Ringrose J, Regehr K. Recognizing and addressing how gender shapes young people's experiences of image-based sexual harassment and abuse in educational settings. J Soc Issues. 2023 Dec;79(4):1251–81.

100. 20 arrested in international operation targeting child sexual abuse material [Internet]. [cited 2025 Sept 30]. Available from: https://www.interpol.int/News-and-Events/News/2025/20-arrested-in-international-operation-targeting-child-sexual-abuse-material

101. 25 arrested in global hit against AI-generated child sexual abuse material [Internet]. Europol. [cited 2025 Sept 30]. Available from: https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material

102. UNICEF. Who Perpetrates Online Child Sexual Exploitation and Abuse? [Internet]. [cited 2025 Nov 4]. Available from: https://safeonline.global/wp-content/uploads/2023/12/DH-data-insights-8-151223.pdf

103. Child sexual abuse material (CSAM) [Internet]. Thorn. [cited 2025 Sept 30]. Available from: https://www.thorn.org/research/child-sexual-abuse-material-csam/

104. Salter M, Wong T. Parental Production of Child Sexual Abuse Material: A Critical Review. Trauma Violence Abuse. 2024 July;25(3):1826–37.

105. Finkelhor D, Turner H, Colburn D. The prevalence of child sexual abuse with online sexual abuse added. Child Abuse Negl. 2024;149.

106. Finkelhor D, Shattuck A, Turner HA, Hamby SL. The lifetime prevalence of child sexual abuse and sexual assault assessed in late adolescence. J Adolesc Health. 2014;55(3):329-333.

107. Russell DH, Trew S, Smith R, Higgins DJ, Walsh K. Primary prevention of harmful sexual behaviors by children and young people: A systematic review and narrative synthesis. Aggress Violent Behav. 2025 Apr;81:N.PAG-N.PAG.

108. Safe Futures Hub. Children Displaying Harmful Sexual Behaviour: Evidence and Responses [Internet]. 2025 [cited 2025 Nov 4]. Available from: https://cdn.safefutureshub.org/files/Children-displaying-harmful-sexual-behaviour-Evidence-and-responses.pdf

109. Tunagur MT, Oksal H, Büber Ö, Kurt Tunagur EM, Sarıgedik E. Risk Factors and Predictors of Penetrative Online Child Sexual Abuse. J Pediatr Health Care. 2025;39(2):198–205.

110. Leaked: Understanding and Addressing Self-Generated Sexual Content involving Young People in Thailand [Internet]. Evident. [cited 2025 Sept 6]. Available from: https://www.itsevident.org/major-projects

111. Disrupting Harm country reports | Innocenti Global Office of Research and Foresight [Internet]. 2022 [cited 2025 Sept 6]. Available from: https://www.unicef.org/innocenti/reports/disrupting-harm-country-reports

112. Trends and insights from a unique helpline preventing child sexual abuse [Internet]. Lucy Faithfull Foundation. [cited 2025 Sept 5]. Available from: https://www.lucyfaithfull.org.uk/research/trends-and-insights-from-a-unique-helpline-preventing-child-sexual-abuse/

113. Bailey A, Allen L, Stevens E, Dervley R, Findlater D, Wefers S. Pathways and Prevention for Indecent Images of Children Offending: A Qualitative Study. Sex Offending Theory Res Prev [Internet]. 2022 Dec 2 [cited 2025 Sept 5];17:1–24. Available from: https://sotrap.psychopen.eu/index.php/sotrap/article/view/6657

114. Protect Children. Our Voice Male Survivors: Experiences of Victims and Survivors of Child Sexual Abuse and Exploitation [Internet]. 2025. Available from: https://www.suojellaanlapsia.fi/en/post/our-voice-male-survivors

115. Tech Coalition | Assessing OCSEA Harms in Product Development [Internet]. Tech Coalition. [cited 2025 May 1]. Available from: https://www.technologycoalition.org/knowledge-hub/assessing-ocsea-harms-in-product-development

116. Detecting, Disrupting and Investigating Online Child Sexual Exploitation [Internet]. [cited 2025 Aug 30]. Available from: https://www.fatf-gafi.org/en/publications/Fatfgeneral/Online-child-sexual-exploitation.html

117. Internet Watch Foundation. Teenage boys targeted as hotline sees 'heartbreaking' increase in child 'sextortion' reports [Internet]. 2024 [cited 2025 Nov 10]. Available from: https://www.iwf.org.uk/news-media/news/teenage-boys-targeted-as-hotline-sees-heartbreaking-increase-in-child-sextortion-reports/

118. Self-Generated Child Sexual Abuse Fieldwork Findings Report by PIER [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/about-us/our-campaigns/self-generated-child-sexual-abuse-fieldwork-findings-report/

119. MikeHarrison. Link-sharing and child sexual abuse: understanding the threat - WeProtect Global Alliance [Internet]. 2023 [cited 2025 May 1]. Available from: https://www.weprotect.org/resources/library/link-sharing-and-child-sexual-abuse-understanding-the-threat/

120. Iyer C, Mehra S. Not a Child's Play: Taking Stock of Children's Gaming in India, Gaps, Emerging Risks and Responses [Internet]. Space2Grow; 2025 June. Available from: https://www.space2grow.in/_files/ugd/fcdbc5_0dead6ef6615455280abdbded0c2c605.pdf

121. Situation Analysis of Child Online Protection in Pakistan | UNICEF Pakistan [Internet]. [cited 2025 May 1]. Available from: https://www.unicef.org/pakistan/documents/situation-analysis-child-online-protection-pakistan

122. Online sexual abuse of primary children 1000% worse since lockdown [Internet]. [cited 2025 May 1]. Available from: https://www.iwf.org.uk/news-media/news/sexual-abuse-imagery-of-primary-school-children-1-000-per-cent-worse-since-lockdown/

123. CDC. A Public Health Approach to Community Violence Prevention [Internet]. Community Violence Prevention. 2025 [cited 2025 Sept 22]. Available from: https://www.cdc.gov/community-violence/php/public-health-strategy/index.html

124. Emery CR, Wong PWC, Haden-Pawlowski V, Pui C, Wong G, Kwok S, et al. Neglect, online invasive exploitation, and childhood sexual abuse in Hong Kong: Breaking the links. Child Abuse Negl. 2024 Jan;147:N.PAG-N.PAG.

125. Scalability | Prevention Global [Internet]. [cited 2025 Sept 22]. Available from: https://www.prevention.global/scalability

126. 2024: A Year of Urgency, Vision, and Partnership in Safeguarding Children Online – Safe Online [Internet]. [cited 2025 Sept 22]. Available from: https://safeonline.global/2024-a-year-of-urgency-vision-and-partnership-in-safeguarding-children-online/

127. Safe Online. Financing a Safe Digital Future: Safer Internet Day 2025 – Safe Online [Internet]. [cited 2025 Nov 4]. Available from: https://safeonline.global/financing-a-safe-digital-future-safer-internet-day-2025/

128. Ending Online Child Sexual Exploitation and Abuse | UNICEF [Internet]. [cited 2025 May 1]. Available from: https://www.unicef.org/documents/ending-online-child-sexual-exploitation-and-abuse

129. Kardefelt-Winther D, Maternowska C. Addressing violence against children online and offline. Nat Hum Behav. 2020;4:227–30.

130. Data for Change – Safe Online [Internet]. [cited 2025 Sept 27]. Available from: https://safeonline.global/data-for-change/

131. UNICEF. Data brief on Measuring Technology-facilitated Violence against Children in line with the International Classification of Violence against Children (ICVAC) [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://data.unicef.org/resources/data-brief-on-measuring-technology-facilitated-violence-against-children-in-line-with-the-international-classification-of-violence-against-children-icvac/

132. Safe Future Hub [Internet]. Available from: https://www.safefutureshub.org

133. Sexual Violence Research Initiative. SVRI Building the Field [Internet]. Available from: https://www.svri.org

134. Together for Girls [Internet]. Available from: https://www.togetherforgirls.org/

135. WeProtect Global Alliance. A global commitment to every child [Internet]. Available from: https://www.weprotect.org

136. General comment No. 24 (2019) on children's rights in the child justice system | OHCHR [Internet]. [cited 2025 Sept 22]. Available from: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-24-2019-childrens-rights-child

137. Reason J. The contribution of latent human failures to the breakdown of complex systems. Philos Trans R Soc Lond B Biol Sci [Internet]. 1997 Jan [cited 2025 Sept 27];327(1241):475–84. Available from: https://royalsocietypublishing.org/doi/10.1098/rstb.1990.0090

138. Data from the Philippines Survivor Network consultations with survivors.

139. Lundy L. 'Voice' is not enough: conceptualising Article 12 of the United Nations Convention on the Rights of the Child. Br Educ Res J. 2007;33(6):927–42.

140. O'Kane C. Active and Safe: The Global Program Guide for Meaningful Participation of Children and Young People in Advocacy and Prevention and Protection from Online Violence [Internet]. kindernothilfe; 2025 [cited 2025 Nov 6]. Available from: https://fliphtml5.com/dcrxp/efpp/Active_%26amp%3B_Safe_GUIDE/

141. O'Kane C. Active and Safe: Accompanying Toolkit for Meaningful Participation of Children and Young People in Advocacy and Prevention and Protection from Online Violence [Internet]. kindernothilfe; 2025 [cited 2025 Nov 6]. Available from: https://fliphtml5.com/dcrxp/kqad/Active_%26_Safe_TOOLKIT_web_19Aug2025/

142. UNICEF. Spotlight guidance on best practices for stakeholder engagement with children in D-CRIAs [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://www.unicef.org/childrightsandbusiness/reports/D-CRIA-Spotlight-guidance-stakeholder-engagement

143. Diagram adapted from Lansdown G, Haj-Ahmead J, Rusinow T, Sukura Y Friscia. Conceptual Framework for Measuring Outcomes of Adolescent Participation [Internet]. 2018 [cited 2025 Nov 4]. Available from: https://www.unicef.org/media/59006/file

144. WeProtect Global Alliance. Visualising child and survivor participation [Internet]. Available from: https://www.weprotect.org/response/child-survivor-participation/mapping-participation-initiatives/#dataviz

145. European Union. BeSmartOnline - Maltese Safer Internet Centre [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://better-internet-for-kids.europa.eu/en/saferinternetday/malta

146. Be Smart Online. A Safer Internet for Malta [Internet]. [cited 2025 Oct 29]. Available from: https://www.besmartonline.info

147. VoiceBox. VoiceBox | By young people, for young people [Internet]. [cited 2025 Nov 4]. Available from: https://voicebox.site/

148. How can service providers work with boys at-risk and survivors of sexual exploitation and abuse in a gender-sensitive way? [Internet]. ECPAT. [cited 2025 May 1]. Available from: https://ecpat.org/story/global-boys-initiative-case-studies/

149. SecretsWorthSharing. Secrets Worth Sharing | How to talk about childhood sexual abuse [Internet]. SecretsWorthSharing. [cited 2025 Nov 4]. Available from: https://www.secretsworthsharing.com

150. CPC Learning Network. Secrets Worth Sharing founder testimony.

151. Global Threat Assessment 2023 Data - WeProtect Global Alliance [Internet]. 2023 [cited 2025 May 1]. Available from: https://www.weprotect.org/global-threat-assessment-23/data/

152. Resources | ThinkUKnow [Internet]. [cited 2025 Sept 22]. Available from: https://www.thinkuknow.org.au/resources-tab

153. World Vision. Tackling Online Child Sexual Exploitation [Internet]. [cited 2025 Oct 29]. Available from: https://wvi.org.vn/special-projects/tackling-online-child-sexual-exploitation-ene29.html

154. End Violence. More progress and impact from our grantees [Internet]. End Violence. [cited 2025 Nov 4]. Available from: https://www.end-violence.org/node/7971

155. UNICEF. Parenting for the Digital Age | UNICEF [Internet]. [cited 2025 Nov 4]. Available from: www.unicef.org/documents/parenting-digital-age

156. National Crime Agency. National Crime Agency launches online campaign to tackle "sextortion" among young teenage boys [Internet]. Available from: https://www.nationalcrimeagency.gov.uk/news/national-crime-agency-launches-online-campaign-to-tackle-sextortion-among-young-teenage-boys

157. Think Before You Share Campaign from IWF [Internet]. [cited 2025 Sept 17]. Available from: https://www.iwf.org.uk/about-us/our-campaigns/think-before-you-share/

158. UNODC. Beware The Share [Internet]. [cited 2025 Nov 4]. Available from: www.unodc.org/roseap/uploads/documents/beware-the-share/index.html

159. Safe Online. Grantee Highlight – Safe Online [Internet]. [cited 2025 Nov 4]. Available from: https://safeonline.global/grantee-highlight/

160. Letourneau EJ, Schaeffer CM, Bradshaw CP, Ruzicka AE, Assini-Meytin LC, Nair R, et al. Responsible Behavior With Younger Children: Results From a Pilot Randomized Evaluation of a School-Based Child Sexual Abuse Perpetration Prevention Program. Child Maltreat [Internet]. 2024 Feb 1 [cited 2025 Sept 6];29(1):129–41. Available from: https://doi.org/10.1177/10775595221130737

161. Ruzicka AE, Assini-Meytin LC, Schaeffer CM, Bradshaw CP, Letourneau EJ. Responsible Behavior with Younger Children: Examining the Feasibility of a Classroom-Based Program to Prevent Child Sexual Abuse Perpetration by Adolescents. J Child Sex Abuse [Internet]. [cited 2025 Nov 7];30(4). Available from: https://www.prevention.global/resources/responsible-behavior-younger-children-examining-feasibility-classroom-based-program

162. Forum EEC. Cultural Adaptation and Evaluation of the RBYC Program in Germany: Towards Offender-Focused and School-Based Prevention of Child Sexual Abuse [Internet]. Preventing disease and ill health. 2025 [cited 2025 Sept 6]. Available from: https://euspr.hypotheses.org/2100

163. Schatz J, Deesawade R, Mosby W, Kavenagh M. Leaked: Understanding and Addressing Self-Generated Sexual Content Involving Young People in Thailand [Internet]. Evident & HUG Project: Bangkok; 2025 [cited 2025 Nov 4]. Available from: www.itsevident.org/_files/ugd/0bd10b_86d0e7f3921645f7bebc0fa399371860.pdf

164. Dodge A, Lockhart E. "Young People Just Resolve It in Their Own Group": Young People's Perspectives on Responses to Non-Consensual Intimate Image Distribution. Youth Justice J Natl Assoc Youth Justice. 2022 Dec;22(3):304–19.

165. Our story [Internet]. World Childhood Foundation - 25 Years. [cited 2025 Sept 27]. Available from: https://childhood.org/about-childhood/our-story/

166. The HUG Project - Protecting Thai children from sexual abuse and online sex trafficking [Internet]. The HUG Project. [cited 2025 Sept 22]. Available from: https://www.hugproject.org/

167. Evident | Translating evidence into action for social change [Internet]. Evident. [cited 2025 Sept 22]. Available from: https://www.itsevident.org

168. Deterring online child sexual abuse and exploitation: lessons from seven years of campaigning) - Lucy Faithfull Foundation [Internet]. [cited 2025 Sept 27]. Available from: https://www.lucyfaithfull.org.uk/research/deterring-online-child-sexual-abuse-and-exploitation-lessons-from-seven-years-of-campaigning/

169. ReDirection | Protect Children [Internet]. [cited 2025 Sept 22]. Available from: https://www.suojellaanlapsia.fi/en/redirection

170. Help Wanted. Help Wanted Prevention Intervention [Internet]. Help Wanted. [cited 2025 Nov 4]. Available from: https://staging.wp.helpwantedprevention.org/

171. Chatbots and Warning Messages - Innovations in the Fight Against Online Child Sexual Abuse [Internet]. Lucy Faithfull Foundation. [cited 2025 Sept 27]. Available from: https://www.lucyfaithfull.org.uk/research/chatbots-and-warning-messages-innovations-in-the-fight-against-online-child-sexual-abuse/

172. Rati. Meri Trustline [Internet]. Rati Foundation. [cited 2025 Nov 4]. Available from: https://ratifoundation.org/meri-trustline/

173. Internet Watch Foundation. IWF 2024: Meri Trustline – Supporting Children Facing Online Harms [Internet]. [cited 2025 Nov 4]. Available from: https://www.iwf.org.uk/annual-data-insights-report-2024/data-and-insights/meri-trustline/

174. UNICEF. Multidisciplinary Models of Care for Child Victims and Survivors of Sexual Abuse and Exploitation in the Digital Age | UNICEF [Internet]. [cited 2025 Nov 4]. Available from: https://www.unicef.org/documents/multidisciplinary-models-care-child-victims-and-survivors-sexual-abuse-and-exploitation

175. Prevention Global. Serving Youth Animation, Brieg, Infographic [Internet]. 2025 [cited 2025 Oct 29]. Available from: https://www.prevention.global/insight/serving-youth-animation-brief-infographic

176. Prevention Global. Serving Youth [Internet]. [cited 2025 Oct 29]. Available from: https://www.prevention.global/serving-youth

177. MyVoiceMySafety-global-poll-of-children.pdf [Internet]. [cited 2025 Sept 22]. Available from: https://www.weprotect.org/wp-content/uploads/MyVoiceMySafety-global-poll-of-children.pdf

178. ECPAT. Guidelines for ethical research on sexual exploitation involving children [Internet]. 2019 [cited 2025 Oct 29]. Available from: https://ecpat.org/guidelines-for-ethical-research/

179. Disrupting Harm: Conversations with Young Survivors about Online Child Sexual Exploitation and Abuse [Internet]. ECPAT. [cited 2025 May 1]. Available from: https://ecpat.org/resource/disrupting-harm-conversations-with-young-survivors-about-online-child-sexual-exploitation-and-abuse/

180. Luciana C. Assini-Meytin, McPhail I, Sun Y, Matthews B, Kaufman KL, Letourneau E. Child Sexual Abuse and Boundary Violating Behaviors in Youth Serving Organizations: National Prevalence and Distribution by Organizational Type. Child Maltreat [Internet]. 2024 [cited 2025 Oct 29];20(3):499–511. Available from: https://journals.sagepub.com/doi/10.1177/10775595241290765

181. Alliance WG. Health and wellbeing of frontline responders. 2025 [cited 2025 Sept 27]; Available from: https://www.weprotect.org/wp-content/uploads/Health-and-wellbeing-of-frontline-responders_May-2025.pdf

182. Towards digital safety by design for children | OECD [Internet]. [cited 2025 Sept 22]. Available from: https://www.oecd.org/en/publications/towards-digital-safety-by-design-for-children_c167b650-en.html

183. Tech Coalition | Child Safety Best Practices [Internet]. Tech Coalition. [cited 2025 May 1]. Available from: https://www.technologycoalition.org/knowledge-hub/child-safety-best-practices

184. Child Rights Impact Assessment: A Policy Tool for a Rights Respecting Digital Environment - Livingstone - 2025 - Policy & Internet - Wiley Online Library [Internet]. [cited 2025 Sept 22]. Available from: https://onlinelibrary.wiley.com/doi/10.1002/poi3.70008

185. UNICEF. Assessing child rights impacts in relation to the digital environment | UNICEF Child Rights and Business [Internet]. [cited 2025 Nov 4]. Available from: https://www.unicef.org/childrightsandbusiness/workstreams/responsible-technology/D-CRIA

186. Digital Futures Commission. Child Rights by Design - 5Rights Foundation & Digital Futures Commission [Internet]. Child Rights By Design | Digital Futures Commission. [cited 2025 Nov 4]. Available from: https://childrightsbydesign.5rightsfoundation.com/

187. Thorn & ATIH. Safety by Design for Generative AI: Preventing Child Sexual Abuse. 2024. Thorn Repository. Available at https://info.thorn.org/hubfs/thorn-safety-by-design-for-generative-AI.pdf.

188. Thorn. Safety by Design for responsible AI | Safer by Thorn [Internet]. Purpose-Built Trust and Safety Solutions | Safer by Thorn. 2025 [cited 2025 Nov 4]. Available from: https://safer.io/resources/safety-by-design-a-responsible-ai-framework/

189. Australian Government. Be Secure Quiz | eSafety Commissioner [Internet]. [cited 2025 Nov 4]. Available from: https://www.esafety.gov.au/educators/classroom-resources/be-secure/quiz

190. Human Mobile Devices. HMD Fuse | The phone that grows with your kids [Internet]. HMD - Human Mobile Devices. [cited 2025 Nov 4]. Available from: https://www.hmd.com/en_int/hmd-fuse

191. Apple Support. About Communication Safety on your child's Apple device [Internet]. Apple Support. [cited 2025 Nov 4]. Available from: https://support.apple.com/en-us/105069

192. Snapchat. Parents - Safeguards For Teens [Internet]. [cited 2025 Nov 4]. Available from: https://parents.snapchat.com/safeguards-for-teens

193. Google. Be Internet Awesome [Internet]. Be Internet Awesome. [cited 2025 Nov 4]. Available from: https://beinternetawesome.withgoogle.com/en-us

194. Lego. LEGO® - Code of conduct [Internet]. [cited 2025 Nov 4]. Available from: https://kids.lego.com/en-us/legal/kids-code-of-conduct

195. Instagram. Partner With Instagram to Keep Your Students Safe | About Instagram [Internet]. [cited 2025 Nov 4]. Available from: https://about.instagram.com/community/educators

196. Ngo VM, Gajula R, Thorpe C, Mckeever S. Discovering child sexual abuse material creators' behaviors and preferences on the dark web. Child Abuse Negl. 2024 Jan;147:106558.

197. Haluska R, Badovska M, Pleva M. Concept of Speaker Age Estimation Using Neural Networks to Reduce Child Grooming. Elektron Ir Elektrotechnika. 2024 Aug 26;30(4):61–7.

198. Thorn. Generative AI: Now is the Time for Safety By Design [Internet]. Thorn. 2023 [cited 2025 Nov 4]. Available from: https://www.thorn.org/blog/now-is-the-time-for-safety-by-design/

199. Tech Coalition. Insights to Action: Asia-Pacific Briefing on Combating OCSEA [Internet]. https://technologycoalition.org/. [cited 2025 Nov 4]. Available from: https://technologycoalition.org/news/insights-to-action-tech-coalition-asia-pacific-briefing-on-combating-ocsea/

200. National Center for Missing & Exploited Children. Take It Down [Internet]. Take It Down. [cited 2025 Nov 3]. Available from: https://takeitdown.ncmec.org/

201. Lantern 2024 Transparency Report [Internet]. https://technologycoalition.org/. [cited 2025 Aug 31]. Available from: https://technologycoalition.org/resources/lantern-2024-transparency-report/

202. U.K. Government. Online Safety Act: explainer [Internet]. GOV.UK. [cited 2025 Nov 4]. Available from: https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

203. Fiji approves 1st national child safeguarding policy [Internet]. [cited 2025 Sept 22]. Available from: https://english.news.cn/asiapacific/20250822/3042a592ecb344bb8eaa4bd2bf0ebebf/c.html

204. G7 #BeBrave Scorecard Report 2025 [Internet]. Brave Movement. [cited 2025 Sept 27]. Available from: https://www.bravemovement.org/resources/g7-scorecard-2025

205. Global Online Safety Regulators Network. GOSRN Regulatory Index 2024 [Internet]. [cited 2025 Nov 3]. Available from: https://www.esafety.gov.au/sites/default/files/2024-10/GOSRN-Regulatory-Index-2024-final.pdf

206. Tracking the shifts: Age assurance in motion | IAPP [Internet]. [cited 2025 Sept 27]. Available from: https://iapp.org/news/a/tracking-the-shifts-age-assurance-in-motion

207. Taylor J. Not just under-16s: all Australian social media users will need to prove their age – and it could be complicated and time consuming. The Guardian [Internet]. 2025 Sept 1 [cited 2025 Sept 28]; Available from: https://www.theguardian.com/technology/2025/sep/02/under-16s-ban-how-hard-will-it-be-for-australian-social-media-users-to-prove-their-age

208. Department of Infrastructure T. Age assurance consumer research findings [Internet]. Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts; 2025 [cited 2025 Sept 27]. Available from: https://www.infrastructure.gov.au/department/media/publications/age-assurance-consumer-research-findings

209. Faverio MA and M. 81% of U.S. adults – versus 46% of teens – favor parental consent for minors to use social media [Internet]. Pew Research Center. 2023 [cited 2025 Sept 27]. Available from: https://www.pewresearch.org/short-reads/2023/10/31/81-of-us-adults-versus-46-of-teens-favor-parental-consent-for-minors-to-use-social-media/

210. International A. Social media ban: what is it and what will it mean for young people? [Internet]. Amnesty International Australia. 2024 [cited 2025 Sept 27]. Available from: https://www.amnesty.org.au/social-media-ban-explained/

211. VPNs top App Store charts as UK age verification kicks in [Internet]. 2025 [cited 2025 Sept 27]. Available from: https://www.bbc.com/news/articles/cn72ydj70g5o

212. African Union. African Union Child Online Safety and Empowerment Policy | African Union [Internet]. 2024 [cited 2025 Nov 3]. Available from: https://au.int/en/documents/20240521/african-union-child-online-safety-and-empowerment-policy

213. Commonwealth of Australia. Age Assurance Technology Trial [Internet]. Age Assurance Technology Trial. [cited 2025 Nov 3]. Available from: https://ageassurance.com.au/report/

214. Eltaher F, Gajula R, Miralles-Pechuán L, Thorpe C, McKeever S. The Digital Loophole: Evaluating the Effectiveness of Child Age Verification Methods on Social Media. Conf Pap [Internet]. 2025 Jan 1; Available from: https://arrow.tudublin.ie/scschcomcon/442

215. Evershed N, Nicholas J. Social media ban trial data reveals racial bias in age checking software: just how inaccurate is it? The Guardian [Internet]. 2025 Sept 18 [cited 2025 Sept 23]; Available from: https://www.theguardian.com/news/2025/sep/19/how-accurate-are-age-checks-for-australias-under-16s-social-media-ban-what-trial-data-reveals

216. School SL. The "Segregate-and-Suppress" Approach to Regulating Child Safety Online [Internet]. Stanford Law School. 2025 [cited 2025 Sept 28]. Available from: https://law.stanford.edu/publications/the-segregate-and-suppress-approach-to-regulating-child-safety-online/

217. Safe Online. Kenya launches groundbreaking training handbook to combat online child sexual exploitation and abuse [Internet]. [cited 2025 Nov 4]. Available from: https://safeonline.global/kenya-launches-groundbreaking-training-handbook-to-combat-online-child-sexual-exploitation-and-abuse/

218. Thorn. For Victim Identification [Internet]. Thorn. [cited 2025 Nov 3]. Available from: https://www.thorn.org/solutions/victim-identification/

219. Rigr AI. Video Summarisation Tool by Rigr AI [Internet]. Video Summarisation Tool by Rigr AI. [cited 2025 Nov 3]. Available from: https://www.vst.rigr.ai

220. Safe Online Report 2024 – Safe Online [Internet]. [cited 2025 Sept 22]. Available from: https://safeonline.global/safe-online-report-2024/

221. Canadian Framework For Trauma-Informed Response in Policing – Introduction | Barrie Police Service [Internet]. [cited 2025 Sept 27]. Available from: https://www.barriepolice.ca/cftirp-introduction/

222. Landry G. Mobilising the Financial Sector Against the Sexual Exploitation of Children. ECPAT;

223. AFP records spike in financial sextortion reports over the school holidays | Australian Federal Police [Internet]. 2023 [cited 2025 Sept 22]. Available from: https://www.afp.gov.au/news-centre/media-release/afp-records-spike-financial-sextortion-reports-over-school-holidays

224. It's Never Too Early - Early education Project Paradigm collaboration | ACCCE [Internet]. [cited 2025 Sept 22]. Available from: https://www.accce.gov.au/resources/parents-carers/its-never-too-early-early-education-project-paradigm-collaboration

225. Sextortion Campaign [Internet]. Available from: https://www.accce.gov.au/sites/default/files/2022-11/sextortion%20campaign%20video.mp4

226. Prevention Global. Making The Case | Prevention Global [Internet]. [cited 2025 Nov 3]. Available from: https://prevention.global/making-the-case

227. U.S. Government Accountability Office. Science & Tech Spotlight: Deepfakes [Internet]. 2025 [cited 2025 Nov 3]. Available from: https://www.gao.gov/assets/gao-20-379sp.pdf

228. JISC. Digital wellbeing [Internet]. Digital wellbeing. [cited 2025 Nov 3]. Available from: https://digitalcapability.jisc.ac.uk/what-is-digital-capability/digital-wellbeing/

229. Knodel M, Baker F, Kolkman O, Celi S, Grover G. Definition of End-to-end Encryption [Internet]. Internet Engineering Task Force; [cited 2025 Nov 3]. Report No.: draft-knodel-e2ee-definition-04. Available from: https://datatracker.ietf.org/doc/draft-knodel-e2ee-definition-04

230. INHOPE. What is generative AI? [Internet]. 2024 [cited 2025 Nov 3]. Available from: https://inhope.org/EN/articles/what-is-generative-ai

231. Overview of Perceptual Hashing Technology [Internet]. www.ofcom.org.uk. 2022 [cited 2025 Nov 3]. Available from: https://www.ofcom.org.uk/online-safety/safety-technology/overview-of-perceptual-hashing-technology

232. Know2Protect, US Department of Homeland Security. ONLINE ENTICEMENT INFORMATIONAL BULLETIN [Internet]. Available from: https://www.dhs.gov/sites/default/files/2025-01/25_0121_K2P_online-enticement.pdf

233. 'Self-generated' sexual material - WeProtect Global Alliance [Internet]. 2022 [cited 2025 May 1]. Available from: https://www.weprotect.org/issue/self-generated-sexual-material/

weprotect
Global Alliance

CPC
LEARNING
NETWORK

COLUMBIA | Mailman School of Public Health