WeProtect GLOBAL ALLIANCE

PA CRISP

GLOBAL THREAT ASSESSMENT 2021

Contents

01

Foreword

Welcome to WeProtect Global Alliance's third Global Threat Assessment: the first we have produced since we launched as an independent entity in April 2020.

Over that time, COVID-19 has had an unprecedented impact. The online world has become ever more central to children's lives. To protect children from sexual exploitation and abuse online, we must first understand the problem we are facing. And to do that, we must listen: to governments; to the private sector; to civil society; and, most importantly, to victims and survivors of abuse.

For the first time, we have surveyed thousands of young adults globally on their experiences of online sexual harms. We share exclusive findings from the technology industry about their response to this crime. We have gathered intelligence from online safety companies on emerging trends. All this, combined with an unprecedented response from our members, has made this our most comprehensive assessment yet.

We have been struck by three insights:

1 The scale of child sexual exploitation and abuse online is increasing. This sustained growth is outstripping our global capacity to respond. Child sexual abuse remains a chronically underfunded issue. That is why we have worked so hard to build this Global Alliance. We all agree – all 98 governments, 53 companies, 61 civil society organisations and nine international institutions – that child sexual abuse online is unacceptable. We all agree we need to collaborate to end it. However, we now know that will require a step change in our global response.

2 Prevention needs to be prioritised in our response. Too often we are waiting for the abuse to take place before we act. A strong law enforcement and judicial response is essential, but for a truly sustainable strategy, we should be actively preventing abuse. This is about more than promoting children's online safety. It is more than Safety by Design, and other initiatives that make it harder for offenders to exploit online services. It is more than deterrence of potential offenders. Prevention is all of this, and more. We need to ensure we are creating safe online environments where children can thrive. Promising work is already underway, but it needs more support.

3 There is hope. Over the past decade, child sexual exploitation and abuse online has moved up the global agenda. More countries, companies and civil society organisations are involved in tackling this crime. Online safety technology is more accessible and advanced. Governments are clarifying and enforcing the responsibilities of online service providers in preventing and addressing child sexual abuse on their platforms. The pace of change may be slower than we would like, but it is happening. Our role as an Alliance is to nurture these green shoots and help them to grow.

Finally, we would like to thank PA Consulting, Crisp, Economist Impact, the dedicated project Steering Committee, as well as contributors from across our membership and beyond, for bringing this document together. Your insights, challenge and commitment have been invaluable. We believe that future Global Threat Assessments will tell the story of how our collaboration and ingenuity will overcome the problem and ensure children around the world can enjoy the benefits of the digital world free from sexual exploitation and abuse.

Iain Drennan
Executive Director
WeProtect Global Alliance

Ernie Allen
Chair
WeProtect Global Alliance

02

Executive summary

Children today face a sustained threat of child sexual exploitation and abuse online.

Our global response to this crime needs a new approach, or more children will continue to be placed at risk and suffer the trauma of abuse.

The best opportunity for change is to improve online safety for children and reduce opportunities for offenders.

Consistent with previous Global Threat Assessments, this report reveals that child sexual exploitation and abuse online continues to proliferate. **Many of the emerging trends threaten to further increase the volume and complexity of cases** and exacerbate the challenges for those working to reduce risk and harm.

This report also spotlights opportunities to enhance the response, harnessed within a multi-layered approach. Regulators, civil society organisations, the technology industry and law enforcement all have a part to play.

Figure 1: The scale of the challenge.

The scale of the challenge

In 2020, **1,038,268** individual media files were exchanged via INHOPE's child sexual abuse material collection and classification platform.[1]

In May 2021, Europol took down a child sexual abuse site on the dark web with more than **400,000** registered users.[2]

More than **3,000,000** accounts are registered across the 10 most harmful child sexual abuse sites on the dark web.[3]

On average, 30 analysts at the US National Center for Missing and Exploited Children (NCMEC) process **60,000** Cyber Tipline reports of child sexual abuse online every day.[4]

While describing the rapid diversification of harms associated with the threat, we also consider the root causes of child sexual exploitation and abuse. Technology is now integrated into all aspects of everyday life. Despite this, we continue to falsely differentiate our treatment of 'online' (as opposed to 'in-person') abuse, as exemplified by lower sentencing for 'online' offences.[5] This demonstrates how our response has failed to keep pace with the threat.

Since the 2019 Global Threat Assessment, the nature of harm has continued to grow and diversify.

In the past two years, the reporting of child sexual exploitation and abuse online has reached its highest levels. Evidence indicates an increase in:

- The incidence of online grooming.[6] [7]
- The volume of child sexual abuse material available online.[8]
- The sharing and distribution of child sexual abuse material.[9]
- Livestreaming for payment.[10]

The scale and rate of change is unprecedented, as illustrated by data from the US National Center for Missing and Exploited Children (NCMEC) and the Internet Watch Foundation (IWF).

+100%

Increase in reports from the public of online sexual exploitation, (NCMEC)[11]

From 2019 to 2020.

77%

Increase in child self-generated sexual material, (IWF)[12]

From 2019 to 2020.

The COVID-19 pandemic is undeniably one contributory factor behind the spike in child sexual exploitation and abuse online (see Theme Chapter: *COVID-19*). The rise in child 'self-generated' sexual material is another trend that challenges the existing response.

Increased reporting may not necessarily equate to a *proportionate* increase in offending: some may be due to increased public awareness and more proactive detection by online service providers. However, levels of abuse may be higher than is suggested by available data:

1 Child sexual exploitation and abuse is an under-reported crime.[13] In a global survey by Economist Impact, 54% of respondents said they had experienced online sexual harms during childhood, including being sent sexually explicit content or being asked to do something they felt uncomfortable with.

There is relatively less data regarding the scale of the issue in Global South countries (see Glossary of Terms). Estimated rates of abuse and exploitation are likely to be revised upwards as this evidence gap is addressed.

2 While most companies that responded to the WeProtect Global Alliance / Technology Coalition survey use tools to detect child sexual abuse material (image and video 'hash-matching' are used by 87% and 76% respectively), only 37% use tools to detect online grooming. This suggests that a significant proportion of such activity may be going undetected.[14]

Even offenders with minimal technical ability can evade detection by using easily accessible encrypted messaging services and anonymity tools. At the other end of the scale, as highlighted by Crisp, some dark web (see Glossary of Terms) offenders employ advanced techniques to obfuscate their activities. The use of 'hidden services' to distribute child sexual abuse material increased by 155% from 2019 to 2020.[15] Detection is likely to be low overall, especially in jurisdictions where digital investigative capabilities are limited.

Recent trends have the potential to fuel the sustained growth in offending:

- New ways of monetising child sexual abuse material and the growth of child 'self-generated' content in exchange for payment are both reinforcing commercial drivers for abuse.
- Increasing volumes of child 'self-generated' material is creating complex challenges for policymakers.
- Offenders are diversifying their production methods, for example by coercing children to perform sexual acts that are captured on camera ('capping'). The Australian Centre to Counter Child Exploitation reports that 'capping' generates approximately 60-70% of referrals to its Victim Identification Unit.[16]

This report helps build a more accurate picture of offender behaviour. The prevailing stereotype of 'stranger danger' is not borne out by the evidence. Child sexual abuse is often perpetrated by family members,[17] [18] [19] [20] with indications this has been exacerbated by COVID-19 restrictions. And while some offenders are motivated by sexual interest in children, this is not exclusively the case. According to the Lucy Faithfull Foundation, only 15-20% of the offenders they currently work with are paedophiles "in that prepubescent children are their primary sexual interest".[21] We must continue to improve our understanding of the various pathways to offending, to inform future deterrence and prevention of abuse.

We must continue to improve our understanding of the various pathways to offending, to inform future deterrence and prevention of abuse.

This Global Threat Assessment highlights priority focus areas and emerging opportunities to arrest the growth of child sexual exploitation and abuse online.

WeProtect Global Alliance's Global Strategic Response (GSR) provides a comprehensive global strategy to eliminate child sexual exploitation and abuse.[22]

This Global Threat Assessment identifies four focus areas within the response framework:

Recommended focus area / opportunity:	Internet regulation
GSR Category:	Policy / legislation

Some countries are evolving their legislative response to include laws that place legal responsibilities on online service providers.

Internet regulation has the potential to make online environments safer for children. Mature supporting legal frameworks and careful consultation will be required to ensure the right outcomes are achieved.

Recommended focus area / opportunity:	Law enforcement capacity-building
GSR Category:	Criminal justice

While some nations benefit from an advanced law enforcement response, many police agencies face fundamental challenges preventing them from keeping up with the threat. Most are underfunded, underequipped and overwhelmed by the scale of offending.

Governments must increase their investment in law enforcement. This would improve national digital policing capabilities and enable more collaboration on technically sophisticated and cross-border offending through the creation of multi-national, specialised investigative units.

Recommended focus area / opportunity:	Voluntary co-operation, transparency and online safety technologies
GSR Category:	Technology

Powerful complements to regulation, voluntary co-operation and transparency enable the responsiveness required to tackle a fast-evolving threat.

Since the 2019 Global Threat Assessment, significant steps have been taken to influence platforms to comply with 'Safety by Design' principles and stimulate global investment in online safety technologies. With the right supporting frameworks in place, and wider uptake, such solutions have the potential to significantly boost the threat response overall.

Recommended focus area / opportunity:	Societal initiatives (various)
GSR Category:	Societal

There needs to be a renewed focus on a range of societal initiatives, including:

- Interventions aimed at empowering young people to develop healthy sexual behaviours.
- Initiatives that tackle the root causes of child sexual exploitation and abuse – for example, attitudes to women. A recent UNICEF Evidence Review found that "the strongest predictor of accepting attitudes (towards child sexual abuse) was… views supporting male power towards women".[23]
- Societal interventions to reduce stigmas that prevent both the disclosure of abuse and those at risk of offending from seeking help.

Child sexual exploitation and abuse online is one of the most urgent and defining issues of our generation.

These recommended focus areas have the potential to stop child sexual exploitation and abuse from happening – or from happening again. In broad terms, prevention is about:

Reducing the risk of offending, by identifying those at risk of committing crimes and helping them address problematic behaviours, and by close risk management of convicted offenders.

Reducing the risk to children. Creating environments that are safer for children. The onus must not be on children to reduce their risk of suffering abuse.

Reducing risk overall, by counteracting structural drivers of abuse. Effective prevention encompasses societal interventions that tackle the root causes of child sexual exploitation and abuse.

Prevention represents the best route to ensuring the sustainability of the future response.

This should sit alongside the role of frontline services in continuing to respond to cases, disrupt offenders, and support victims and survivors. The key lies in balancing investment in prevention as part of an integrated, whole system response.

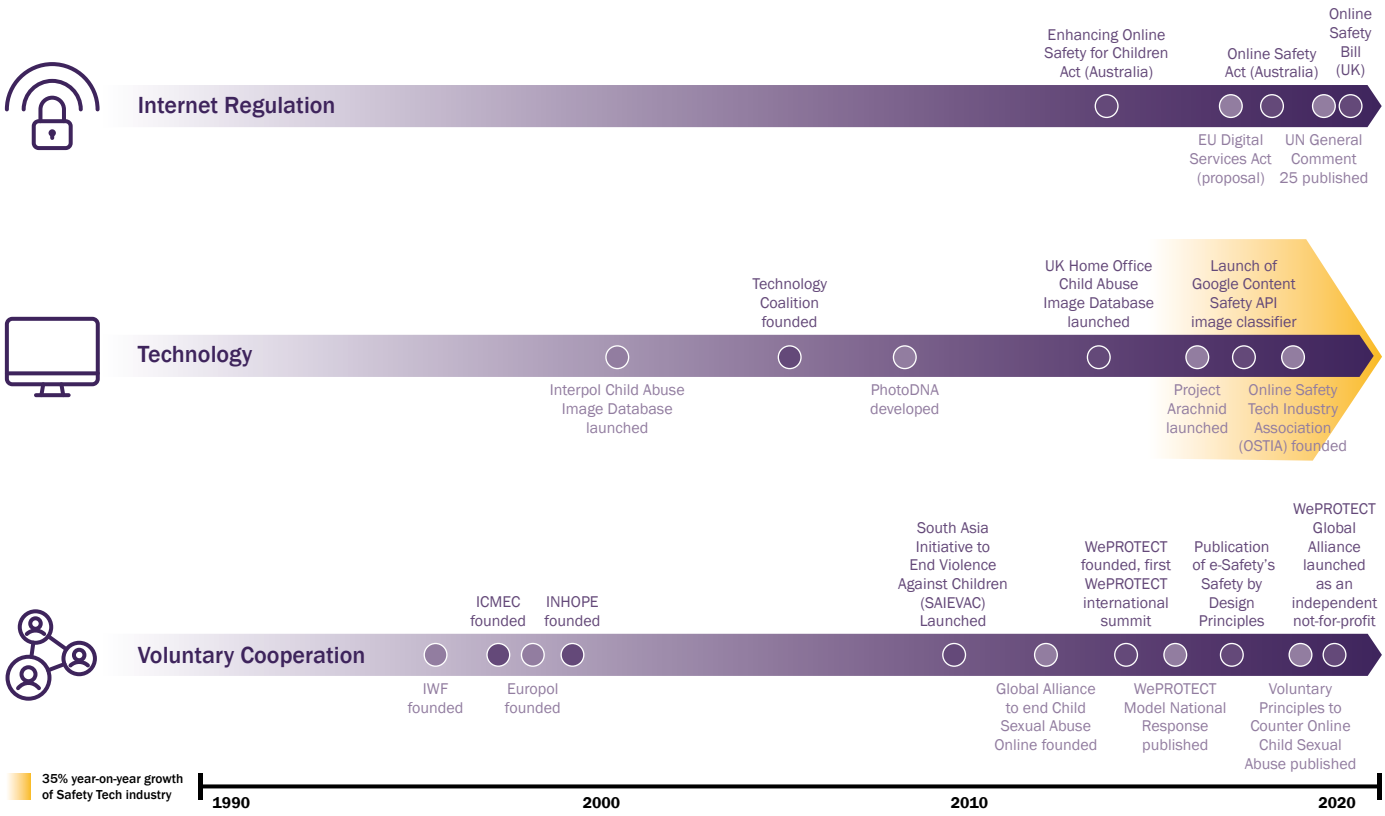
Together we have the knowledge, means and opportunity to take action, improve the global response, and prevent more children from being harmed.

Child sexual exploitation and abuse online is one of the most urgent and defining issues of our generation. Nations face different challenges and are at different stages in the evolution of their threat response. Some have experienced the rapid acceleration of internet connectivity in recent years, and societal consciousness of online harms is relatively nascent. In others, there is already coherent consumer demand for proactive action to address the issue.

Technology solutions implemented by online service providers can bring global benefit, as can local legislative approaches – by incentivising multi-national companies to improve their transparency, accountability and responsiveness overall. Figure 2 shows key developments in the past three decades that have boosted the international response to child sexual exploitation and abuse online. The momentum for these developments is likely to be sustained as online services evolve and consumers worldwide become more aware – and less tolerant – of these harms.

The key recommendations emerging from this year's Global Threat Assessment are detailed in Chapter 7: Recommendations. While measures must be tailored and prioritised according to local context, these are actions that all companies, communities and governments can take to improve the response to child sexual exploitation and abuse online. We have a global shared responsibility to work together to keep children safe from harm. In 2021 we have an unprecedented opportunity to do so by sustaining global momentum to transform our collective response.

Figure 2: Charting some of the key developments relating to enablers for an enhanced preventative response.



03 Introduction

KEY DEFINITIONS

Child sexual abuse is "the involvement of a child [anyone under 18] in sexual activity that he or she does not fully comprehend, is unable to give informed consent to, or for which the child is not developmentally prepared and cannot give consent". This is the definition of child sexual abuse adopted by WeProtect Global Alliance ('the Alliance'), based on World Health Organization (WHO)[24] guidelines.

Child sexual exploitation is a form of child sexual abuse that involves any actual or attempted abuse of a position of vulnerability, differential power or trust. This includes, but is not limited to, profiting monetarily, socially or politically from the sexual exploitation of another. This can be perpetrated by individuals or groups of offenders. What distinguishes child sexual exploitation from child sexual abuse is the underlying notion of exchange present in exploitation.[25] There is significant overlap between the two concepts, because exploitation is often a feature of abuse, and vice versa.[26]

Child sexual exploitation and abuse online is partly or entirely facilitated by technology, i.e. the internet or other wireless communications. This concept is also referred to as Online Child Sexual Exploitation and Abuse (OCSEA), and 'technology-facilitated' child sexual exploitation and abuse.

Scope

This report is the third Global Threat Assessment published by the Alliance to outline the scale and scope of child sexual exploitation and abuse online, and to galvanise the response.

The Global Threat Assessment 2019 concluded that emerging trends signal a 'tsunami' of growth in child sexual exploitation and abuse online, "leaving ever more victims and survivors in its wake".[27] It focalised the threat through four lenses: victims; offenders; technology trends; and socio-economic context.

This report takes a 'harms-based' approach to enable a more nuanced exploration of differences in victim and survivor experiences, offender methods, technologies, and socio-economic contexts for the different manifestations of child sexual exploitation and abuse online. This is defined in Figure 3: Harms definitions. This approach enables a more complete assessment of the factors at play for each harm, and intervention opportunities and response strategies.

The harms examined are interconnected, as illustrated in Figure 4 and throughout.

We also examine three cross-cutting themes:

- COVID-19.
- Technology.
- Regulation, voluntary co-operation and transparency.

NOTE ON HARMS TERMINOLOGY

The 'harms' (defined in Figure 3) are descriptions of abuses committed by perpetrators. They are not worded to reflect the experiences of victims and survivors. This is to enable an exploration of the factors linked to offending: where the primary onus for disruption and prevention sits. This terminology is not intended in any way to diminish the impact on victims, which is also explored in respect of each harm, including in corresponding case studies.

Figure 3: Harms definitions.

Harm	Definition
Grooming children online for the purpose of sexual exploitation and abuse	An individual builds a relationship, trust and emotional connection with a child or young person to manipulate, exploit and abuse them (facilitated, partly or entirely, by the internet or other wireless communications).[28] There is not always an intent to meet in person. *Note: Some organisations use the alternative term 'online enticement' (as defined by NCMEC[29]) to refer to this harm.*
Producing child sexual abuse material	Creating child sexual abuse material *(see Glossary of Terms)* by in-person photography / video / audio recording; creating textual content or non-photographic (for example, computer-generated) visual material; or manipulating existing child sexual abuse material to create new unique imagery.
Searching for and / or viewing child sexual abuse material	Seeking child sexual abuse material on the internet and viewing or attempting to view it.
Sharing and / or storing child sexual abuse material	Downloading, storing, hosting, uploading and / or sharing child sexual abuse material.
Child 'self-generated' sexual material	Content of a sexual nature, including nude or partially nude images and video, that has been produced by children of themselves. Child 'self-generated' sexual material is not a harm per se (it can be produced voluntarily and shared as part of a developmentally appropriate exchange, for example, between adolescents). However, there are scenarios in which harm is caused, primarily: • When a child or adolescent is coerced into producing 'self-generated' sexual material. • When voluntarily 'self-generated' sexual material is shared against an adolescent's wishes. This report examines the characteristics of harmful 'self-production'. This phrase appears in quotation marks throughout the report to avoid implying willingness on the part of the child or young person involved. While the content may meet the definition of child sexual abuse material, the intent is likely to be unclear and cannot be taken for granted in any circumstances.
Livestreaming child sexual exploitation and abuse	Transmitting child sexual abuse and exploitation in real-time over the internet.

Aims

The primary goal of this report is to detail the scale and scope of the threat of child sexual exploitation and abuse online, with an assessment that is comprehensible and meaningful to audiences across the globe. It aims to encourage evidence-based action by recognising the significant progress achieved to date, and highlighting opportunities to reduce the risk to children, to prevent abuse before it takes place.

Methodology

This report is a meta study that distils findings from multiple international studies to increase their global reach, collate a holistic picture of the threat, and offer a balanced assessment where information is incomplete or experts disagree (caveating where appropriate).

This secondary research is supported by various forms of primary research:

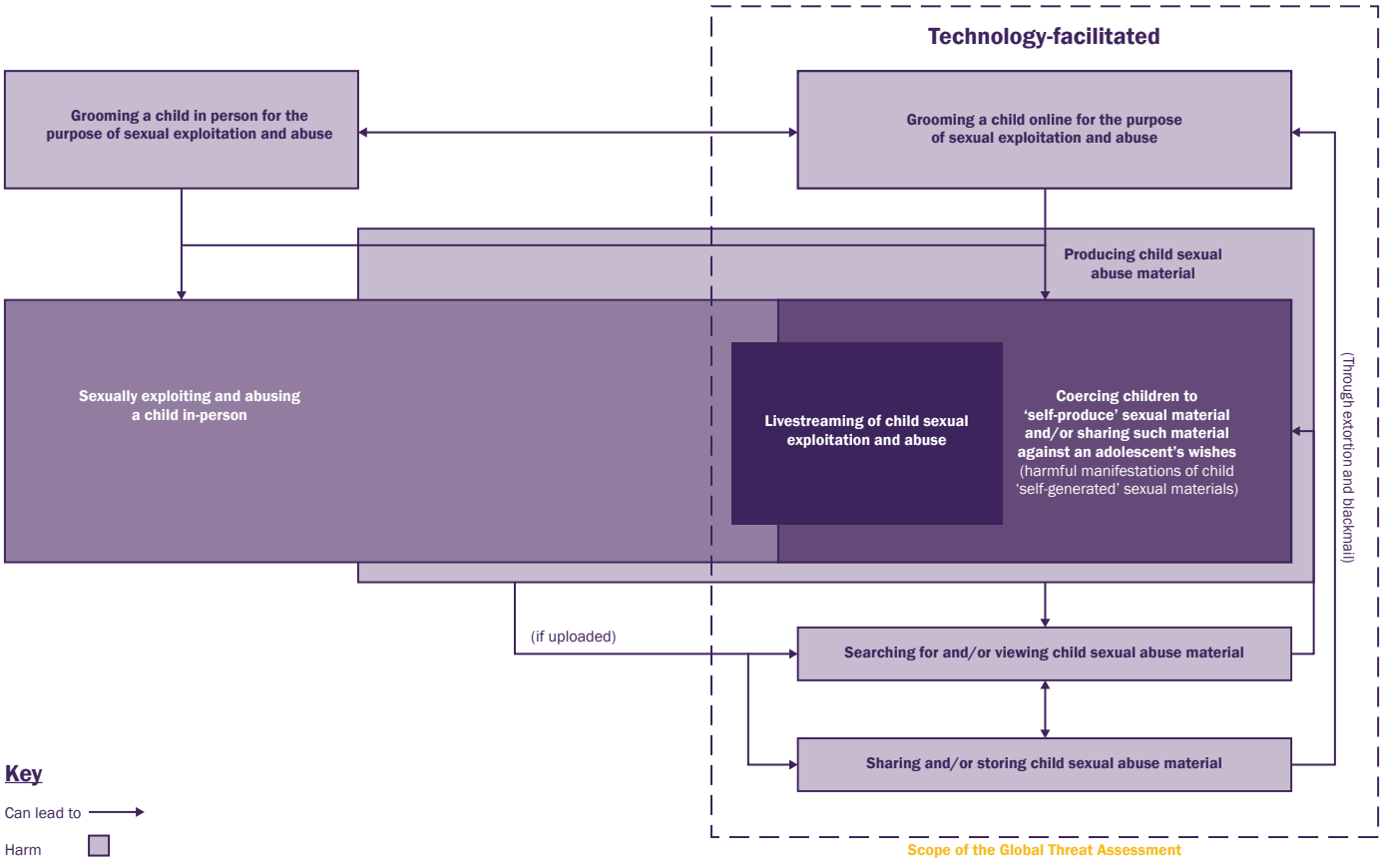
- Interviews with law enforcement officials, child safety advocates, academics, technology industry representatives and other experts.
- Case studies provided by member organisations and their affiliates.
- An anonymised survey of 32 global technology companies, which was conducted by the Alliance in collaboration with the Technology Coalition.
- Vignettes developed by Crisp, a leading provider of online safety technologies. These vignettes are included in call-out boxes (example at Figure 6).

The development of this report was guided by a Steering Committee comprised of 20 experts from law enforcement, government, the technology industry, Non-Governmental and Intergovernmental Organisations (NGOs and IGOs), and academia (see page 66).

CRISP

Crisp provides Actor Risk Intelligence on the agendas and tradecraft of individuals and groups in order to prevent online harms, misinformation and abuse. Its Actor Intelligence Graph analyses digital conversations in real-time to reveal relationships between actors and their groups in order to predict online harms as early as possible. Crisp protects over two billion daily users, covering an estimated 450 million children. **www.crispthinking.com**

Figure 4: Harms map.



Research approach

58

Case studies reviewed

+230

Literature items reviewed

55

Organisations consulted

34

Interviews conducted

04

ECONOMIST IMPACT

ECONOMIST IMPACT

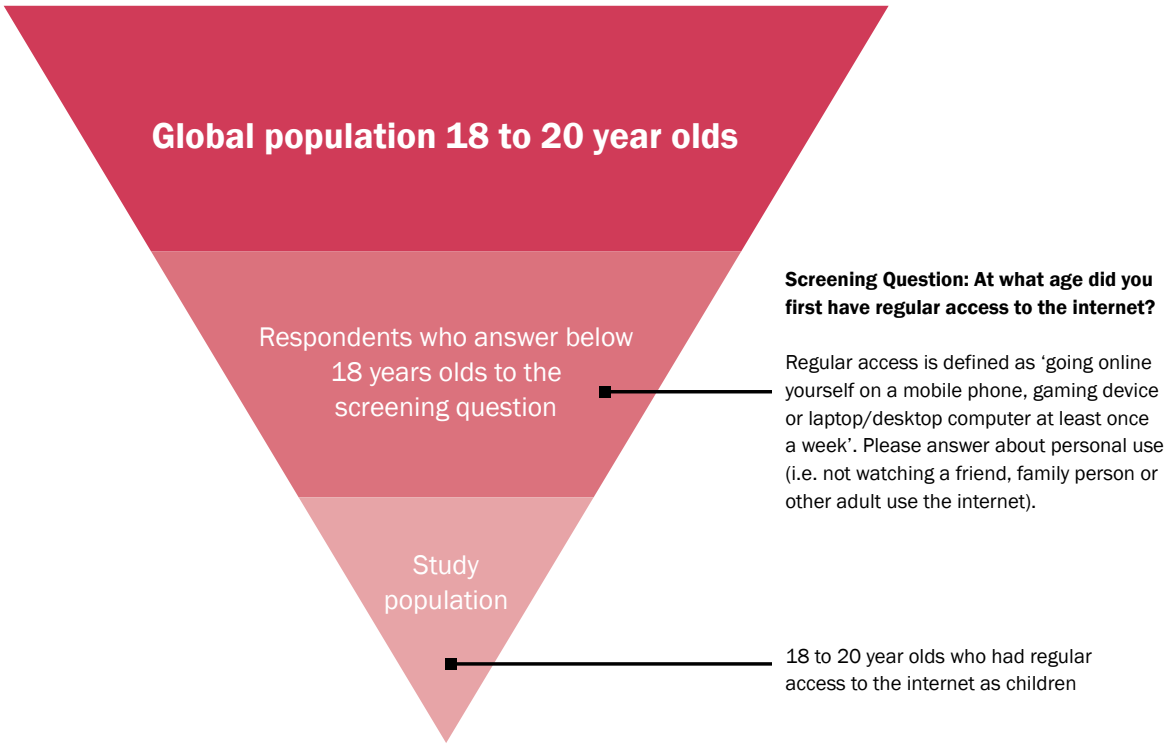
Estimates of childhood exposure to online sexual harms and their risk factors

A GLOBAL STUDY OF CHILDHOOD EXPERIENCES OF 18 TO 20 YEAR OLDS

The internet, social media and other digital apps / platforms can be a double-edged sword for children and young people.

They provide important fora for learning and interaction, as well as a platform for positively exploring sexuality and fostering relationships between children.[i] At the same time, they can be used to facilitate the sexual exploitation and abuse of children both by adults — known and unknown — and by peers, and enable access to age-inappropriate content.

To help fill the global knowledge gap on the potential scale and scope of online sexual harms against children, Economist Impact and WeProtect Global Alliance conducted a study that gathers evidence from more than 5,000 18 to 20 year olds in 54 countries around the world who had regular access to the internet as children.[ii]



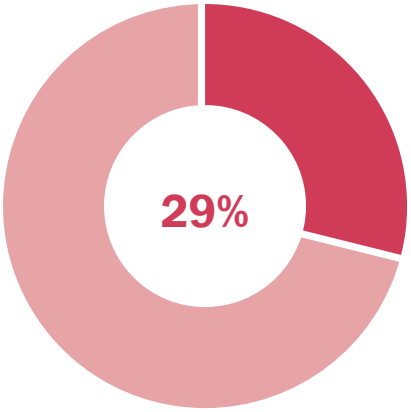
The questionnaire asked respondents about their exposure to online sexual harms and their risk factors during childhood. Questions centred on four online sexual harms.[iii] These online harms are:

- Being sent sexually-explicit content from an adult or someone they did not know before they were 18.
- Being asked to keep part of their sexually-explicit online relationship with an adult / or someone they did not know before a secret.
- Having sexually-explicit images of them shared without consent (by a peer, adult, or someone they did not know before).
- Being asked to do something sexually-explicit online they were uncomfortable with (by a peer, adult, or someone they did not know before).

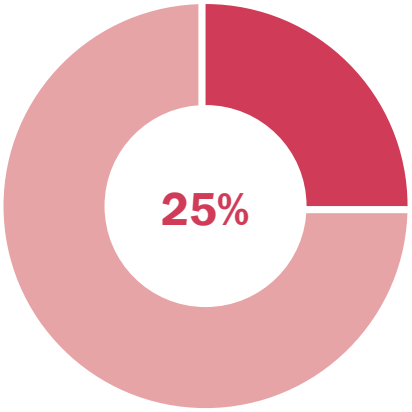
The key findings of this research are presented below. Full findings and methodology can be found in *Estimates of childhood exposure to online sexual harms and their risk factors: A global study of childhood experiences of 18 to 20 year olds* on the *WeProtect Global Alliance website.*

KEY FINDINGS

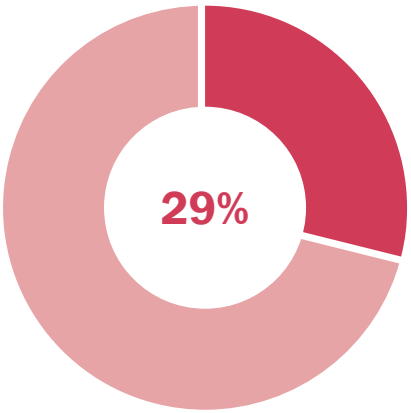
54% **of respondents had experienced at least one online sexual harm during childhood.**[iv]



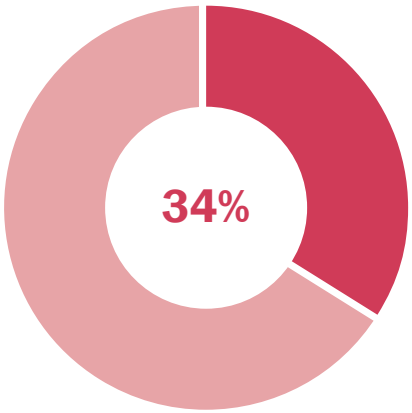
Received sexually explicit content from an adult they knew or someone they did not know before they turned 18



Had an adult they knew or someone they did not know ask them to keep part of their online sexual explicit interactions a secret

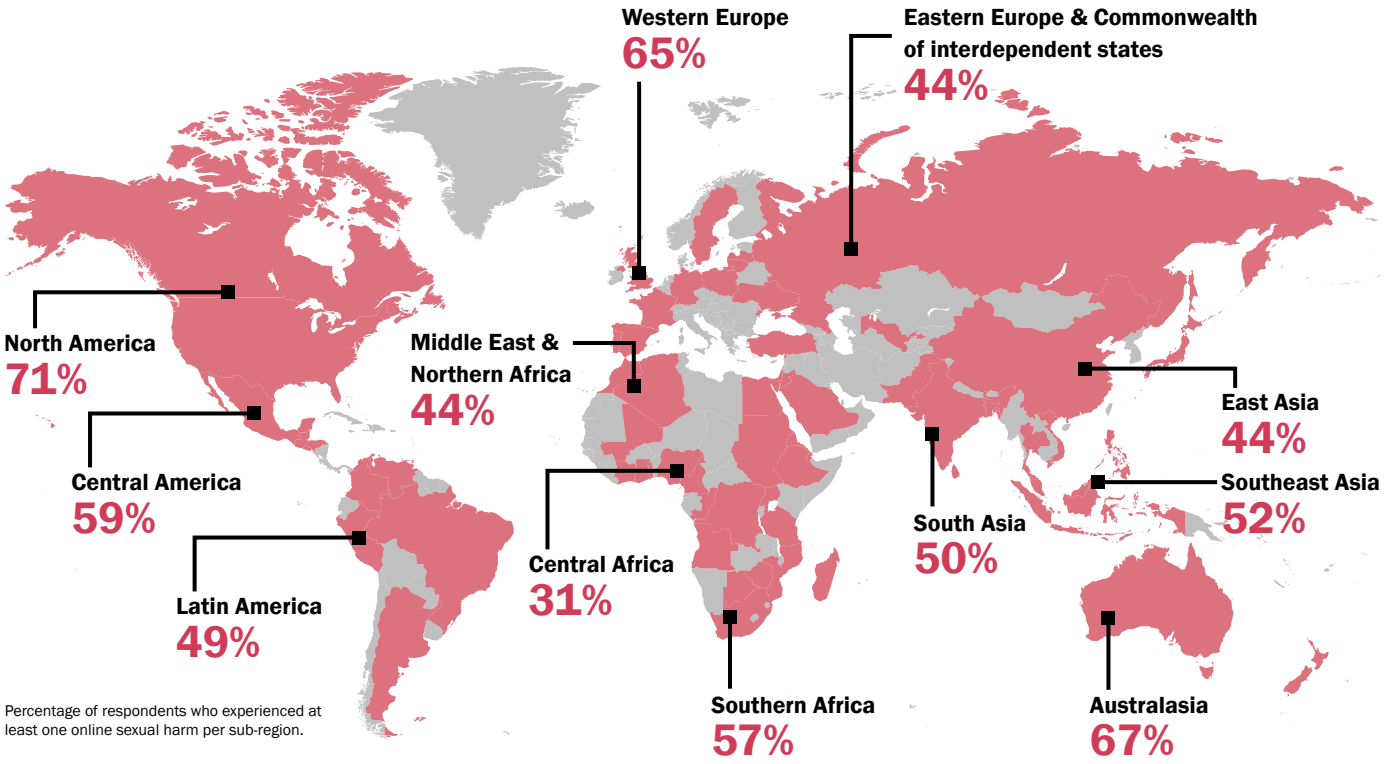


Had someone share sexually explicit images and/or videos of them without permission



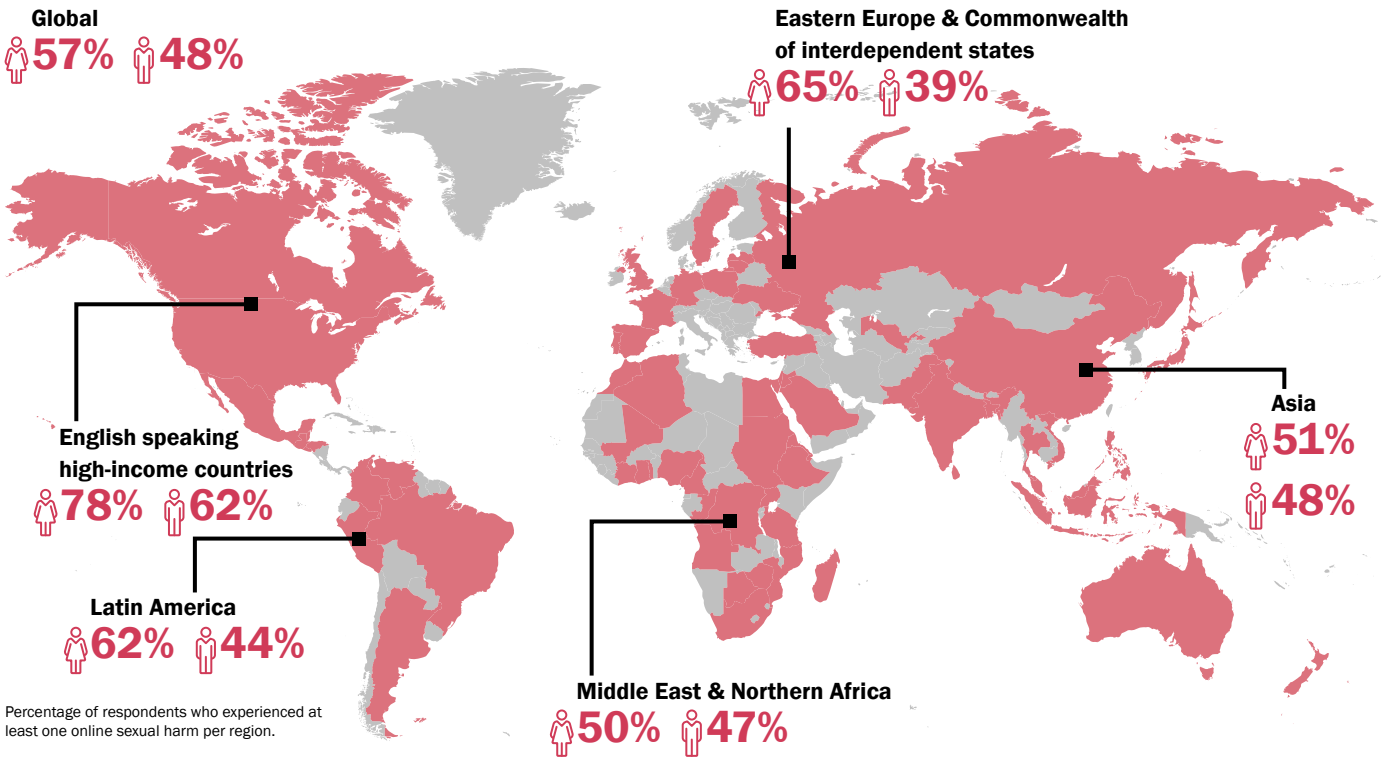
Were asked to do something sexually explicit online they were uncomfortable doing

Child online sexual harms are OCCURRING EVERYWHERE...



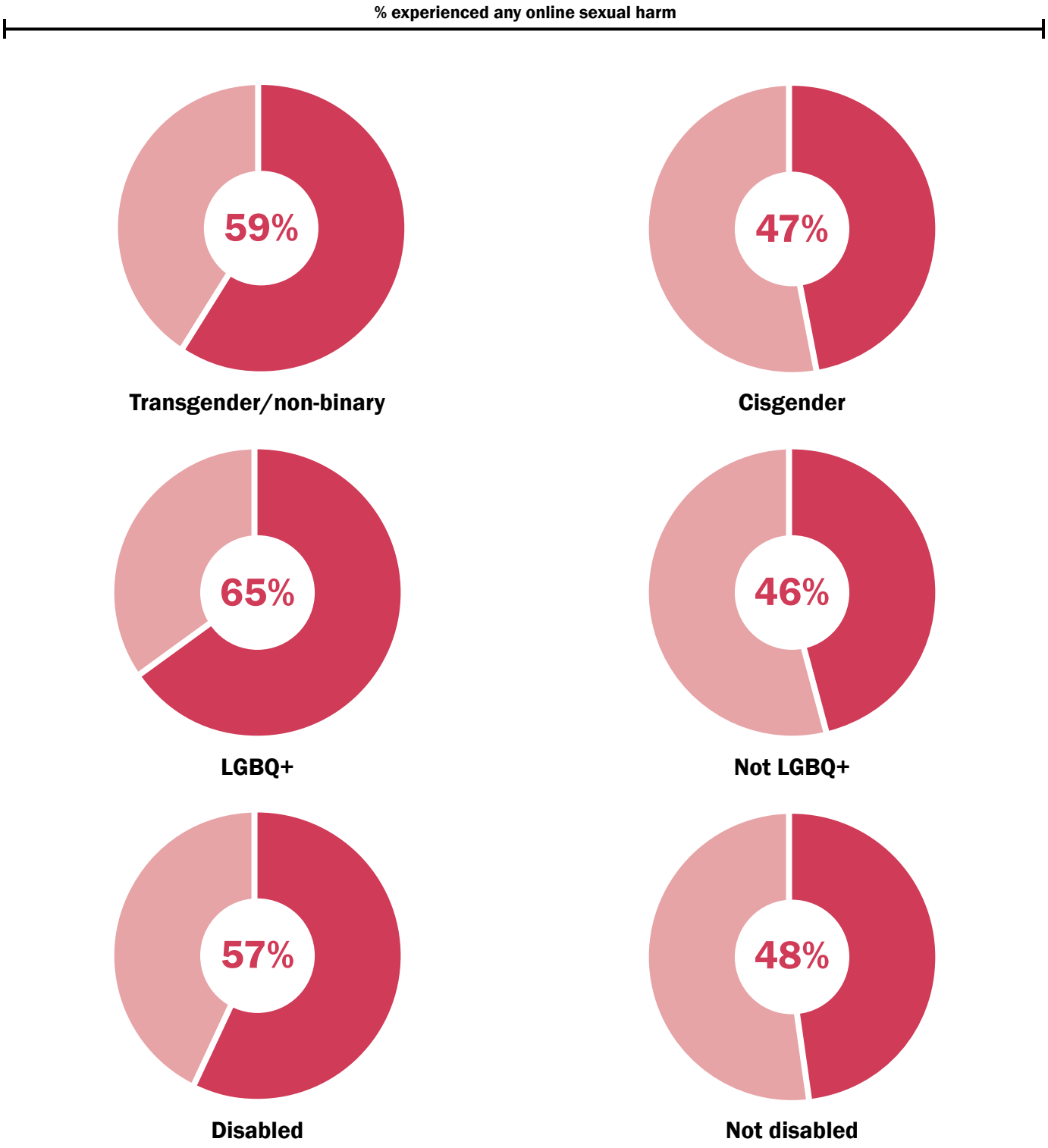
Percentage of respondents who experienced at least one online sexual harm per sub-region.

...and although girls are more at risk, NEARLY HALF OF BOYS had experienced at least one online sexual harm.



Percentage of respondents who experienced at least one online sexual harm per region.

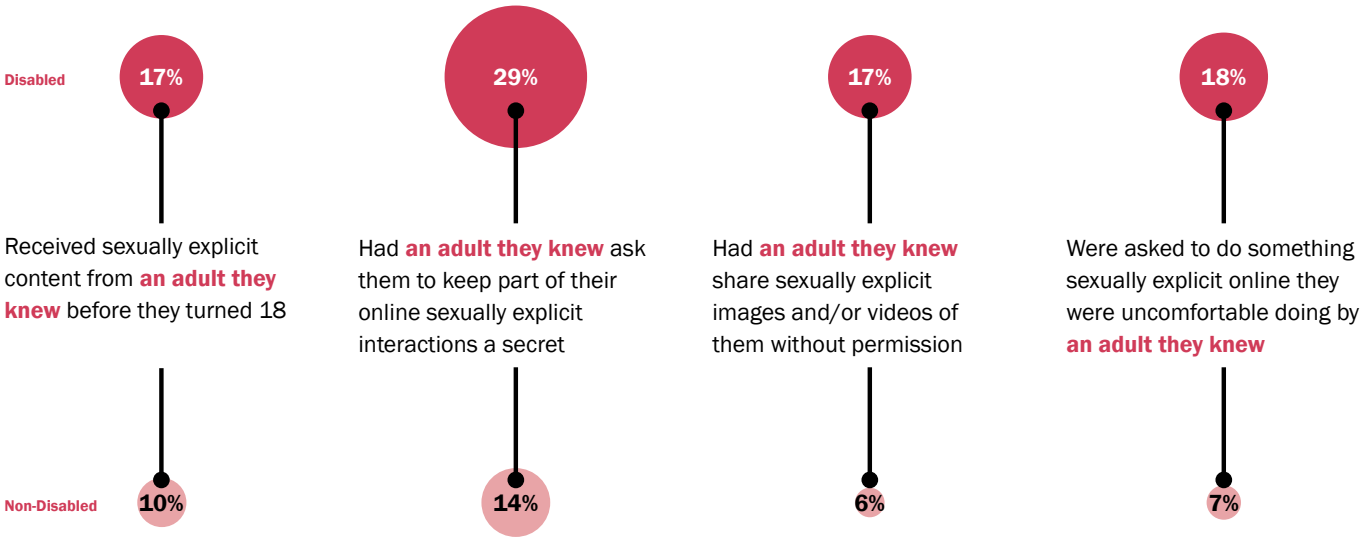
Respondents who identified as transgender/non-binary, LGBQ+ and/or disabled were MORE LIKELY to experience online sexual harms during childhood.



Percentage of respondents who experienced at least one online sexual harm by self-identified characteristic.

Respondents were asked if they self-identified as transgender/non-binary, LGBQ+, and/or disabled. The data in this graphic is from analysis that disaggregated the sample on the basis of those responses. The number of respondents who identified with these characteristics in any singular region was too small for accurate analysis on geographical variations in experiences for these groups.

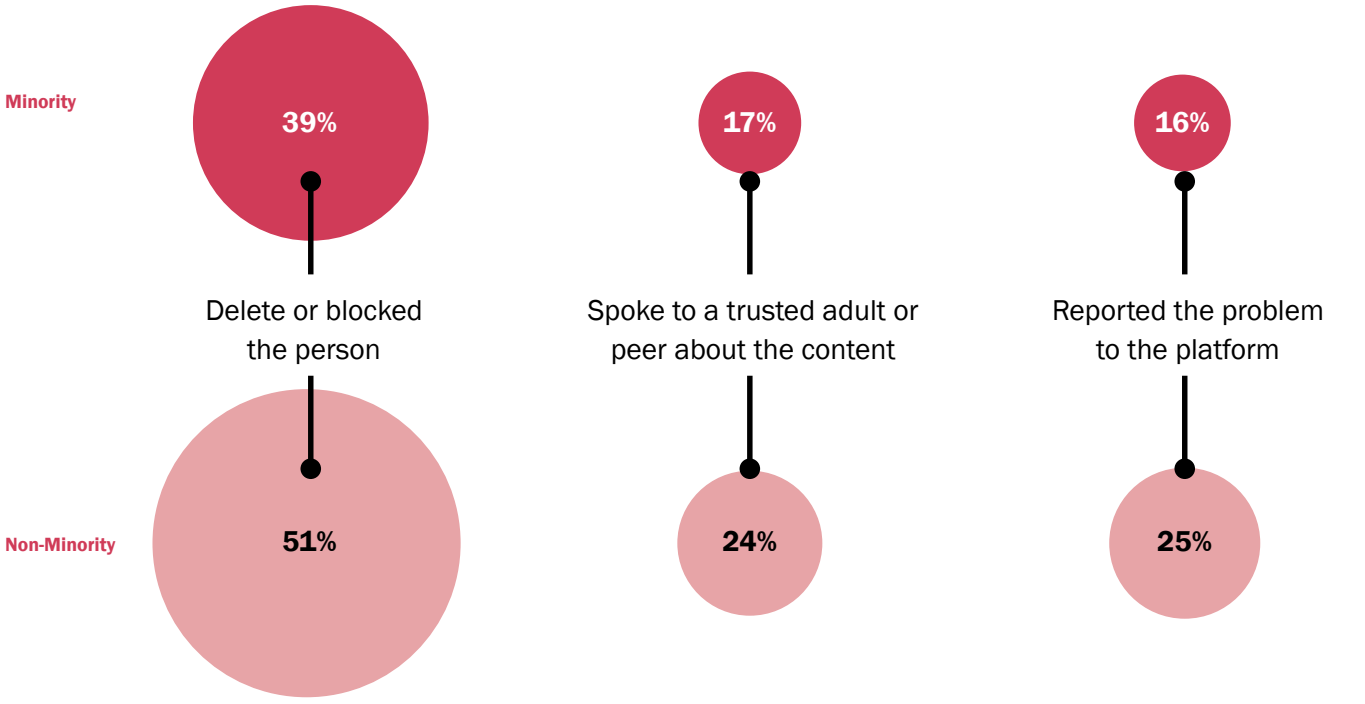
Respondents who identified as disabled were MORE LIKELY to be targeted by an adult they knew.



Percentage of respondents who experienced an online sexual harm by an adult they knew (disabled and non-disabled).

Disabled is defined as an impairment or condition (physical or mental) that affects the respondent's ability to carry out daily activities.

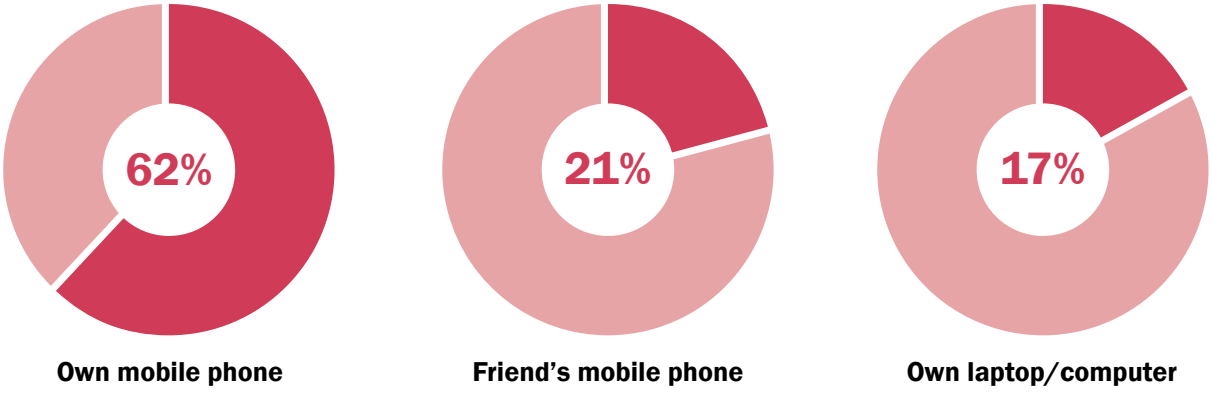
Respondents who identified as racial or ethnic minorities were LESS LIKELY to take action in cases where an adult they knew or someone they did not know before tried to send them sexually explicit content.



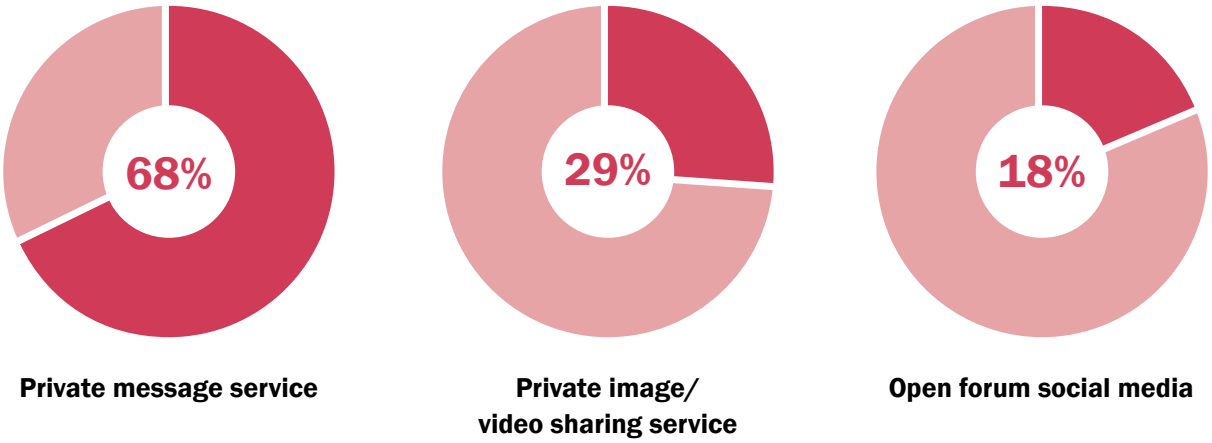
Percentage of respondents who took a certain action (minority and non-minority).
Minority is defined as race, nationality or ethnicity that is different to that of most people living in respondent's country.

TWO-THIRDS **of respondents who received sexually explicit material online as children received it through a private messaging service, most commonly on their personal mobile device.**

Device where respondent received content



Platform where respondent received content



KEY FINDINGS

The scale and scope of online sexual harms against children today is likely to be different. Ethical concerns about surveying children through an internet-based tool prevented us from collecting data from respondents under the age of 18.

Why are the levels likely to be different today?

- Rapidly increasing internet penetration among individuals of all ages means that more children are receiving regular access to the internet at younger ages.
- A larger percentage of children of all ages have access to both individual and adults' and / or peers' mobile phones more frequently and are using a wider range of platforms.
- COVID-19 has forced children to spend more time online and left people everywhere feeling more isolated.
- Digital platforms have become a common way for children to explore sexuality with their peers, but these fora for expression and exploration also open doors to new forms of abuse and exploitation.

Additional research is needed to understand how the dynamic internet and social media / digital platform landscape is changing the way children engage and what this means for their safety against online threats. Our study is a first step in painting a global picture of the issue, and identifying where future research would be valuable.

METHODOLOGY

This study is based on data gathered through an online survey of 5,302 18 to 20 year olds who had regular access to the internet* as children (under 18) conducted from May to June 2021.

The survey was fielded in 21 languages across 54 countries, which were aggregated into 12 sub-regions** — each containing a minimum of 390 respondents — for analysis. The global sample and regional aggregation were used for analysis of gender and other demographic characteristics experiences.

Notes:

*'Regular access to the internet' is defined as someone going on the internet (i.e. not watching a friend, family person or other adult use the internet) at least once a week.

**Australasia, Central Africa, Central America, East Asia, Eastern Europe & Commonwealth of Independent States, Middle East & North Africa, North America, Southeast Asia, Southern Africa, South America, South Asia and Western Europe.

END NOTES

i Following the definition of a child in the Convention on the Rights of the Child, 'children' refers to people under 18 years old in this study.

ii 'Regular access to the internet' is defined as someone going on the internet themselves (i.e. not watching a friend, family person or other adult use the internet) at least once a week. 'Children' is defined as people aged under 18 years old. For a full discussion of how this sampling method is likely to affect results, see the full paper.

iii A set of harmful behaviours considered as risk factors for potential or actual child sexual exploitation and abuse online.

iv 54% of respondents had experienced one or more of the online sexual harms asked about in this survey.

05

Themes

COVID-19

COVID-19 created a 'perfect storm' of conditions that fuelled a rise in child sexual exploitation and abuse across the globe.[30]

It may be years before the full scale of pandemic-related abuse is revealed. In the meantime, frontline services require an urgent boost to support the additional known victims created by COVID-19.

While lockdowns may have accelerated pathways into offending, the longer-term impacts of the pandemic threaten to reinforce commercial drivers of abuse.

Many countries reported an increase in child sexual exploitation and abuse during COVID-19 (see Figure 5). The Netclean 2020 survey of global law enforcement also indicated consensus across the policing community that there was an increase in attempts to contact children, volumes of child 'self-generated' sexual material, and activity on the dark web.[31] Some law enforcement agencies anticipate a further rise in the volume of detected child sexual abuse material as more moderators resume their usual working practices.[32]

Addressing this will require government investment to boost the capacity of frontline services, and industry collaboration to reduce reporting backlogs.

The true impact of COVID-19 is difficult to distinguish, primarily because the increase in reports of child sexual exploitation and abuse during the pandemic is not necessarily indicative of an equivalent increase in offending. Changes in working practices, including mandated shifts to home working, negatively affected some of the key reporting agencies. In some cases analysts were less able to assess reports or perform moderation duties to established standards, resulting an increase in 'false positives'.[33] Heightened awareness of the issue may be contributing to the sustained increase observed in 2021, as news media and police agencies continue to spotlight alarming spikes in rates of reported abuse.

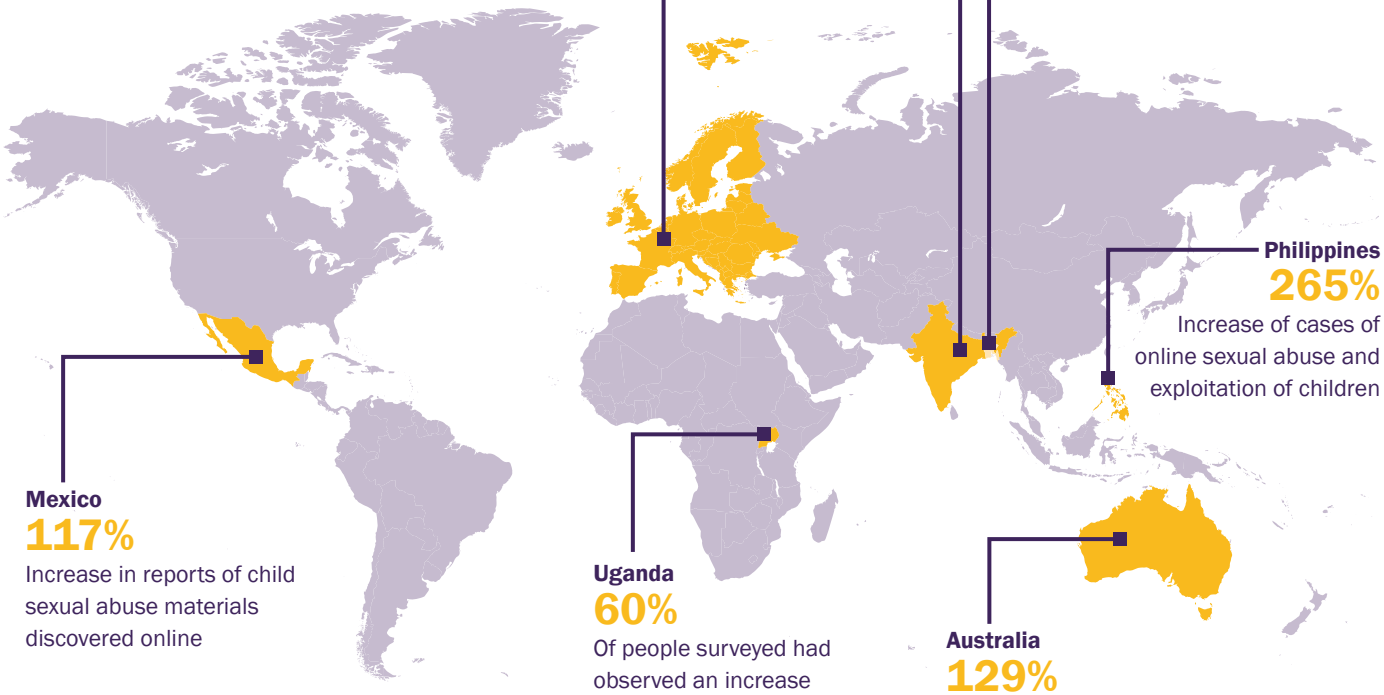
Figure 5: Increases in child sexual abuse during COVID-19. [34 35 36 37 38 39 40]

NCMEC experienced a
106%
increase in reports of suspected child sexual exploitation to its global CyberTipline

Europe
50%
Increase in some countries in child sexual abuse online

India
95%
Increase in internet searches for child sexual abuse materials

Bangladesh
40%
Increase in calls to child helplines



Philippines
265%
Increase of cases of online sexual abuse and exploitation of children

Mexico
117%
Increase in reports of child sexual abuse materials discovered online

Uganda
60%
Of people surveyed had observed an increase in sexual violence against children since the start of lock down

Australia
129%
Increase of reports of child sexual abuse materials discovered online

> ***In September 2020, the closure of schools affected 827 million pupils worldwide.[41]***

During the pandemic some perpetrator prevention initiatives recorded increased demand for self-help services.[42] [43] Early on, there were concerns that individuals perpetrating abuse might be at greater risk because of "stress, lack of positive social supports, barriers to help-seeking, and increased opportunity" caused by confinements, "all of which are associated with risk of offending".[44] Increased demand for self-help suggests that such concerns have to some extent been borne out, and that lockdowns may have helped open and accelerate pathways into offending for some individuals.

For many established offenders, lockdowns provided more opportunities to contact children (due to more being online at home, as a result of school closures) and more autonomy to network. In a global survey of frontline workers involved in child protection, 72.8% said there had been at least some increase in activity in online abuse communities during the pandemic.[45]

Use of 'hidden services' (websites hosted within a proxy network so their location cannot be traced) also increased, suggesting that more offenders learned to obfuscate their activities.[46] Additionally there was a rise in online abuse as a form of 'proxy' offending for individuals who in other circumstances might have sought to abuse children in-person.[47] This is particularly concerning as some children are now at greater risk of livestreaming abuse due to economic hardship caused or worsened by COVID-19. As ECPAT highlighted: "As families lose their income, particularly in the Global South, they may see an opportunity in 'live-streaming shows'".[48] This is not least because the pandemic has increased demand for livestreaming as an alternative to 'in-person' abuse.[49] In this sense the pandemic also risks reinforcing commercial drivers of abuse in the long term. There is already evidence that children are reacting to weakened economic prospects by 'self-producing' sexual material in exchange for payment.[50]

> ***The World Bank estimates that the pandemic will push an additional 88 to 115 million people into extreme poverty, causing this number to reach up to 150 million in 2021.[51]***

Lockdowns heightened many risk factors for abuse. Timely intervention to boost stretched frontline services will be critical to supporting additional victims.

Undoubtedly, lockdowns will have reduced the risk to children experiencing abuse in environments outside the home (such as institutional settings). However, for many others, lockdowns created or exacerbated vulnerabilities (such as loneliness or mental health needs[52]); increased the time they spent online[53] (and therefore accessible to predators[54]); and prevented access to support networks (such as trusted adults, friends) that might normally afford protection.[55] The risk of suffering sexual abuse online during the pandemic is likely to have been greater for children experiencing a convergence of these risk factors.

As highlighted in Harms Chapter: *Producing child sexual abuse material,* a significant proportion of child sexual abuse is perpetrated by family. COVID-19 lockdowns will have caused many children to be trapped at home with their abusers. The suffering of such victims is likely to have been prolonged due to reduced access to the usual reporting channels through the pandemic. In Paraguay, reports of child sexual abuse decreased by 50% during lockdown, only to increase after the relaxation of measures – presumably because victims (and trusted adults, such as teachers or health workers) were able to leave home in order to report offences.[56] In Jamaica, a decline in official reports of abuse was contradicted by the increasing number of hotline calls, suggesting that children may be in situations where normal reporting pathways are not accessible, and that "abuse is most likely taking place at home".[57] Australia noted a decrease in reports of child maltreatment during the first phase of the pandemic, only to observe a rebound when restrictions eased.[58]

In 2020, pandemic-related disruptions in child protection services were reported in 104 countries representing a total population of 1.8 billion children.[59] In many regions, policing capabilities were also affected. According to Netclean's 2020 report, the capacity of law enforcement to investigate child sexual exploitation and abuse fell during the pandemic.[60] Interpol indicated that the pandemic resulted in fewer reports reaching police, difficulties progressing existing investigations, and reduced use of the International Child Sexual Exploitation Database.[61]

As countries emerge from lockdowns, and as victims make delayed reports of abuse, the increased volume of cases is likely to exacerbate existing backlogs for frontline services. Without timely government intervention, the ripple effect of COVID-19 has the potential to prolong children's suffering and reduce case resolution rates. This may be likely if more governments across the world divert funds away from public services to stimulate the post-pandemic economic recovery.[62] [63] Such action will weaken the immediate threat response and may undermine the possibility of meaningful prevention in the future. In lower income countries, the situation could be exacerbated if other nations follow the UK's lead in reducing Official Development Assistance (ODA),[64] as spending priorities shift. The impact of such cuts could extend to increasing the long-term impact of future health crises, including the proliferation of child sexual exploitation and abuse.

05
Themes

Technology

The pace of technological change continues to complicate the response to child sexual exploitation and abuse online.

However, in recent years online safety technologies have advanced significantly. With wider uptake, these tools and techniques could enable the required step change in the global threat response.

In 1995, less than 1% of the world's population were active internet users.[65] Today, this figure has grown to 59.5%.[66] Global average download speeds are also increasing,[67] and the number of active mobile devices in the world is expected to reach 17.62 billion by 2024 – an increase of 3.7 billion devices compared to 2020 levels.[68] Some parts of the world are experiencing these changes at a significantly accelerated pace, such as the African continent (see Figure 6). Under 18s now account for one in three internet users across the globe.[69]

Figure 6: Internet usage in Africa. [70 71 72]

SPOTLIGHT:
Internet usage in Africa

4G
rollout across the continent will bring millions more young people fast internet

Sub-Saharan Africa 2020-2025:

130m
new internet users

70%
increase in smart-phone usage

20%
number of internet users grown by year-on-year

As highlighted in United Nations General Comment 25 (see *Glossary of Terms*), the digital environment facilitates access to a range of children's rights as ever more societal functions come to rely on digital technologies. The educational opportunities of such technologies have the potential to be especially transformative. The growth in mobile devices has been hailed as a powerful opportunity to reach the global population of girls who represent "two thirds of the world's out of school primary age children".[73] For children, the social benefits of connecting are also broad. According to the 2020 EU Kids Online survey, the majority "say they find it easier to be themselves online at least sometimes".[74] This can be especially transformative for young people whose freedom of expression is otherwise limited (such as by disabilities or impairments, or due to inhabiting a restrictive socio-environmental context).[75]

For some children, the benefits of connectivity are currently countered by negative impacts, and experiences of harmful behaviours and sexual abuse.

There is evidence to suggest that for some children, being online is exposing them to sexual interactions[76] and sexual images.[77] [78] While some (older) children may perceive these as positive opportunities to explore their sexual identity, for others, including young children, the developmental impact is more likely to be negative.[79] As explained in Harm Chapter: *Searching for and / or viewing child sexual abuse material*, habitual exposure to pornography is linked to the development of harmful sexual behaviour (see *Glossary of Terms*) in adolescents.[80] [81]

The Economist Impact study commissioned alongside this report found that of the survey respondents who said they had been sent sexually explicit material, 62% had received it on their mobile device. In many countries, smartphones are now children's preferred means of going online.[82] [83]

Increased internet access via connected mobile devices contributes to the sense of entrapment for children who become victims of abuse, as offenders seem to infiltrate all aspects of their daily lives.[84] Thorn's 2021 survey of US youth revealed that many children respond to harmful online sexual interactions by downplaying their impact and not disclosing them: tactics that are likely to magnify and / or extend the harm caused.[85]

There are positive signs that advocates – including children and young people themselves – are beginning to challenge the apparent 'normalisation' of sexual abuse. In the UK in early 2021, revelations of 'rape culture' in schools inspired teens to share their experiences of sexual harassment as part of the 'Everyone's Invited' movement. It has since amassed more than 50,000 testimonials and generated similar momentum in the US.[86] [87] [88] While the internet has played a role in the proliferation of sexual exploitation and abuse, it also provides young people with a platform from which to demand change.[89]

Many police forces lack the capabilities required to investigate child sexual exploitation and abuse online.

Even offenders with minimal technical knowhow can complicate the detection of crimes by using anonymisation solutions such as Tor and Virtual Private Networks (VPNs), which are now mainstream and built into some browsers by default.[90] The use of encryption is also increasing (see Harm Chapter: *Regulation, voluntary co-operation, and transparency*). The overall effect is a significant hindrance to investigations caused by technologies with a low barrier to use. Offenders on the dark web pose a different set of challenges. Among the most technologically advanced, they exploit the opportunities afforded by new tools to enable their offending and evade detection.

The number of active mobile devices in the world is expected to reach

17.62 BILLION

by 2024

The Economist Impact study commissioned alongside this report found that of the survey respondents who said they had been sent sexually explicit material

62%

had received it on their mobile device.

Offenders on the dark web seek new tools to aid exploitation.

Offenders on the dark web are becoming increasingly sophisticated and comfortable with cutting-edge technology used to create and distribute child sexual abuse material. Complicating matters, an emerging tech-savvy generation of dark web offenders are employing and promoting advanced security techniques and services to evade detection.

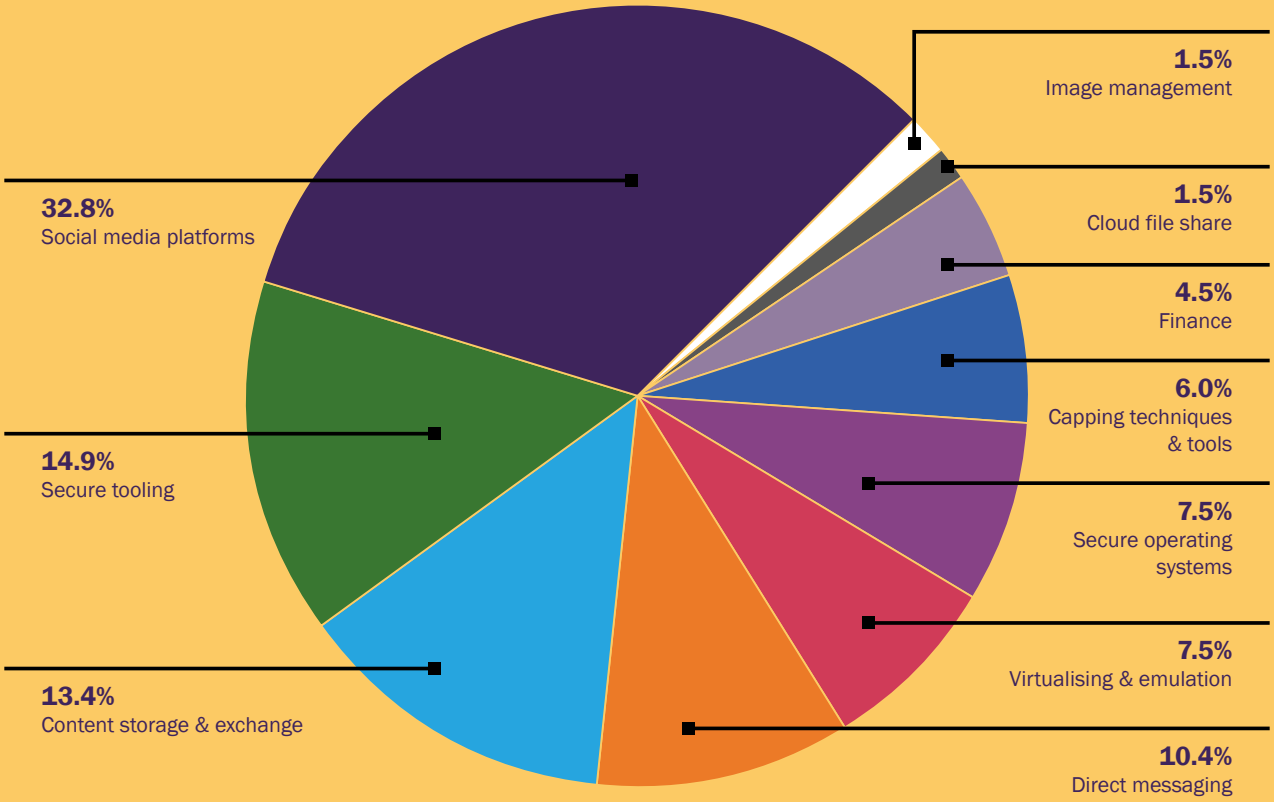
Making it even more difficult for law enforcement to investigate and prosecute these crimes, these offenders are continually searching online for new options and solutions to facilitate their exploitation of children. Distressingly, their operational toolkit is evolving and expanding at the current rate of online technology innovation.

Crisp analysts were able to gauge the level of perpetrator interest in technology topics by closely examining conversations that took place in a range of offender forums on the dark web, in February 2021.

Of the 'technology topics' discussed in these forums, nearly one-third related to platforms on which offenders would seek to engage children or vulnerable users, along with wider discussions on 'tradecraft' (see *Glossary of Terms*). Most concerningly, more than two-thirds of the discussion centred on topics such as technical tools for direct messaging, exchanging funds, or how to securely acquire and store content, both locally and in the cloud — all of which can make identifying and prosecuting offenders more challenging.

For definitions of technology topics, please see the *Glossary of Terms.*

Figure 7: Technology topics discussed on dark web offender forums.



Like other internet-enabled crimes, child sexual exploitation and abuse online throws up fundamental investigative challenges for many police agencies: most commonly, limited digital capabilities; insufficiently skilled personnel; and a lack of access to tools to expedite aspects of the investigative process. Sri Lanka recently reported a lack of technical staff in investigation units,[91] while Thai police have stated they require more resources trained in the investigation of dark web and crypto-currency payments linked to abuse.[92]

Some countries address this issue by bundling online child sexual exploitation and abuse into the remit of cybercrime units, where cases compete for attention with high volume, often complex crimes like fraud. In some places co-operation with online service providers also lags behind. According to Interpol, non-compliance with police warrants is a major global challenge.[93] Discrepancies in corporate data retention policies can also complicate evidence-gathering for police agencies.

The root cause of many of these issues is chronic under-funding of policing. Investment is urgently required to build law enforcement's digital investigative capabilities worldwide, and develop and enhance collaboration mechanisms critical to effectively tackling cross-border and technologically sophisticated offending.[94]

Some legislative frameworks are still not fit for the digital age. Gaps risk creating a sense of impunity surrounding child sexual abuse online.

In recent decades, there has been more consistency in legislative approaches to child sexual abuse, catalysed by international instruments such as the Lanzarote Convention (see *Glossary of Terms*). However, gaps persist. Since 2006, the International Centre for Missing and Exploited Children has regularly conducted a review of child sexual abuse material legislation in the 196 Interpol member countries. The first survey found legislation to be 'sufficient' in just 27 countries; the latest edition (2018) reveals that 71 are still yet to define child sexual abuse material, while only 32 require internet service providers to report such offences.[95]

The role of technology in child sexual exploitation and abuse crimes throws up a raft of specific legislative challenges.

Discrepancies in the treatment of 'online' versus in-person abuse are common and cited as a reason why internet offenders seemingly operate with impunity. A case review by the charity International Justice Mission (IJM) highlighted that only Scotland, Canada, Australia and Sweden punish livestreaming of abuse "on a par with contact offending".[96] Many countries also have no defined legal position on the use of non-photographic child sexual abuse material.[97] [98] The impact of this gap may grow as offenders diversify production methods using technologies like Computer-Generated Imagery (CGI) (see Harm Chapter: *Producing child sexual abuse material*). Such shortcomings risk creating a sense of impunity to further fuel offending, not least because offenders have been noted to purposely target children in jurisdictions with weak provisions.[99]

The good news is that the technology now exists to protect children and catch offenders. With wide uptake, online safety tools and techniques have the potential to transform the global threat response.

In recent years there have been significant advances in online safety technologies. Key examples include:

- Grooming detection tools and 'Safety by Design' features that reduce offender opportunity and promote safe online behaviours (see Harm Chapter: *Grooming children online for the purpose of sexual exploitation and abuse*).
- Deterrence mechanisms that disrupt pathways to offending (see Harm Chapter: *Searching for and /or viewing child sexual abuse material*).
- Hash-matching' (see *Glossary of Terms*) solutions to detect and remove 'known' child sexual abuse material, and classifiers used to detect first generation material (see Harm Chapter: *Sharing and / or storing child sexual abuse material*).

The expanding Safety Tech sector has played a pivotal role in the development of many such technologies. In the UK alone, where Safety Tech companies collectively hold 25% of the global market share, the sector has experienced an estimated 35% annual growth rate since 2016,[100] and is on track to achieve £1bn in revenues by 2024 (see Figure 8 below).[101] More than half (52%) of UK firms have an established international presence.[102]

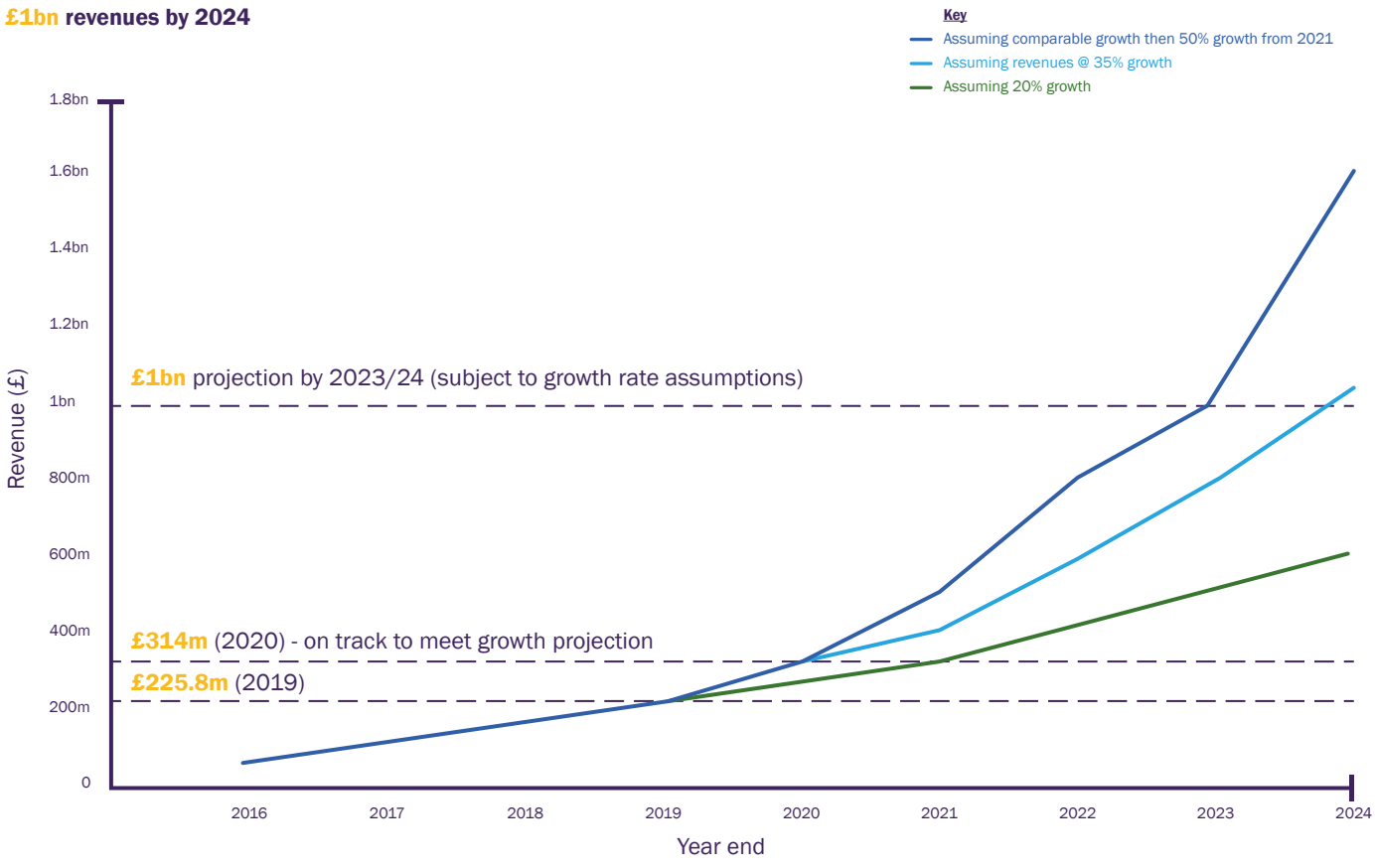
By reducing offender opportunities and enhancing the protections afforded to children, online safety technologies have the potential to boost the global response to child sexual exploitation and abuse online. This is without factoring the possible impact of tools and techniques still in development, for example:

- Improved facial recognition, which could speed up the identification of child victims.[103]
- Predictive analytics, which are already used by some authorities to identify children at high risk of abuse, to enable early intervention.[104]
- Tools that can harvest metadata (see *Glossary of Terms*) to detect potential child sexual abuse material, even if the material itself is not discoverable.[105]
- Camera 'fingerprinting' techniques used to attribute photos and / or videos to a specific device. In some countries these techniques are already being used to streamline and strengthen prosecutions.[107]

WHAT IS 'SAFETY TECH'?

Safety Tech providers develop technology or solutions to facilitate safer online experiences, and protect users from harmful content, contact, or conduct.[106]

Figure 8: Chart showing projected growth for the UK Safety Tech Industry, reproduced with the permission of the UK Department for Digital, Media, Culture, and Sport. [108]



APPLE: EXPANDED PROTECTIONS FOR CHILDREN

Apple are considering the introduction of additional child safety features in the United States. These include:

- New device-level tools that would warn children and, in the case of those under 13, their parents or guardians when receiving or sending sexually explicit photos, if parents or guardians have elected to be notified.
- Updates to Siri and Search to help users in the event they encounter sexually unsafe situations online and offline, and also to intervene when users try to search for child sexual abuse material to provide resources and warnings aimed at abuse prevention.
- Use of the new NeuralHash tool to identify 'known' child sexual abuse material stored in iCloud Photo Library, by 'matching' content against a hash database of child sexual abuse images. If the matching of hashes exceeds a minimum threshold, it will trigger a human review for confirmation before a report is sent to NCMEC. The matching process is powered by a cryptographic technology called Private Set Intersection and Threshold Secret Sharing, which determines if there is a match without revealing the result - unless and until the threshold is met. Apple cannot learn anything about a user's account unless a collection of matching images to 'known' CSAM has been detected.

Critically, the features could be compatible with Apple's encrypted iMessaging service and demonstrate the continued potential to counter the threat of child sexual exploitation and abuse even within encrypted environments, by adopting device-level and server-side technologies whilst preserving data privacy.

GLOBAL PARTNERSHIP TO END VIOLENCE AGAINST CHILDREN: SAFE ONLINE FUND

The Safe Online initiative is part of the Global Partnership to End Violence Against Children. It invests in programmatic interventions, evidence generation and technological innovation to combat child sexual abuse online. Since 2017, Safe Online has invested a total of USD 48m in 60 projects. In 2020, USD 10m of this was invested in the design and integration of technology solutions.

Alongside financial investments to strengthen the response to child sexual abuse online, the End Violence Partnership's Safe Online initiative fosters knowledge generation and collaboration to maximise the use of collective resources and ensure investments have a broad impact.

Safe Online plays a critical role in advocating and driving collaborative action to align global, regional and national efforts to combat online harms against children.

This vision relies on governments and private sector companies increasing investments to scale up solutions that keep children safe. As highlighted by the End Violence Partnership, lack of investment remains the biggest obstacle to an effective response to child sexual exploitation and abuse online.[109] Broad and consistent uptake of technologies will be key to avoid offenders simply diverting children onto platforms that do not have safety mechanisms integrated.

As uptake increases, international alignment on the legal basis for using such technologies will become increasingly critical,[110] recognising that many raise ethical and privacy considerations. Governments need to consult closely with companies to develop legal frameworks to enable responsible innovation that puts children's rights at the centre of technology design and deployment. This must include protection of children's right to privacy, 'age appropriate' explanations, and non-discrimination in the application of AI algorithms.[111] Mechanisms to protect younger children merit special consideration to ensure they are not deprived opportunities due to perceived risks, not least because low digital literacy could ultimately make them more susceptible to abuse.[112]

05

Themes

Regulation, voluntary co-operation and transparency

The pace of technological change continues to complicate the response to child sexual exploitation and abuse online.

The proliferation of child sexual exploitation and abuse online has fuelled debate on internet regulation in recent years.

As more countries move to regulate online service providers, voluntary co-operation and transparency will continue to be critical to cohere the global response.

Regulation aims to provide standards for balancing user privacy and safety to enable a more consistent approach to tackling online harms.

There has been significant momentum towards the regulation of digital services and online safety in the past three years. Among the first to pursue a legislative solution are Australia, Germany, the UK, the European Union, and Ireland (see Figure 10).

Effective regulatory systems conform to a consistent four-step cycle (see Figure 9).

The regulation of online harms is relatively immature compared to other sectors – such as aviation, food, and financial services. Transparency is limited, and voluntary accountability and corrective action are inconsistent. However, increasing awareness of harm is creating growing international pressure for consistent transparency, accountability standards and corrective action to be enforced through legislation and regulation.

Figure 9: Steps in an effective regulatory cycle.

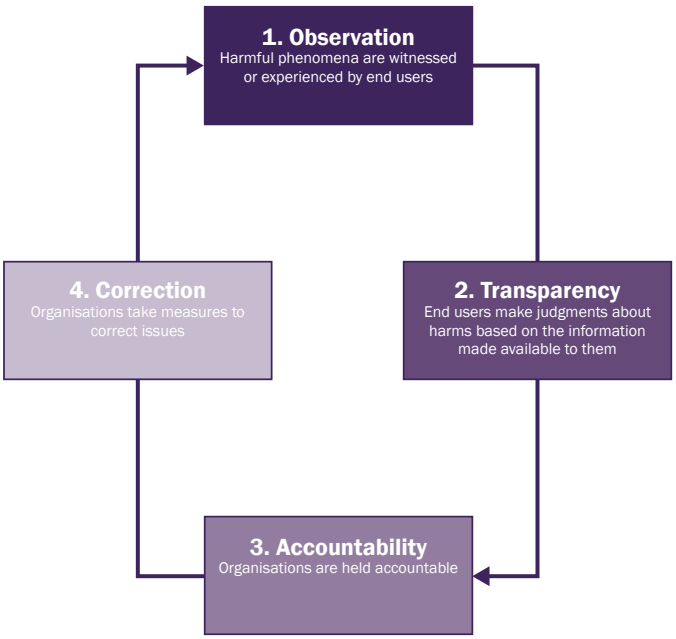
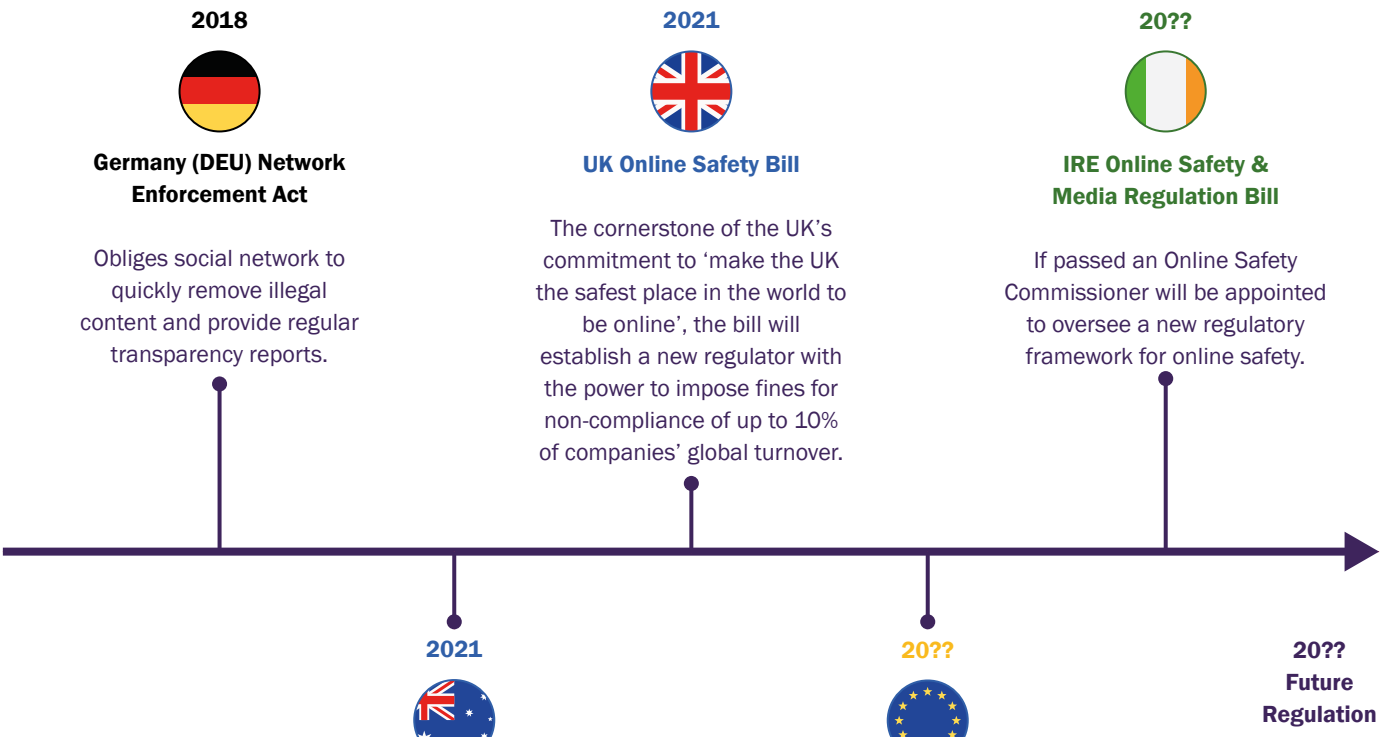


Figure 10: The road to internet regulation. [113] [114] [115] [116] [117] [118]



In the physical world, legal frameworks help companies and authorities balance individual privacy and safety, but in the online realm such standards are nascent. By clarifying the responsibilities of online service providers, regulation could establish a more consistent balance to better protect internet users from harm – particularly children.[119]

Increasing use of End-to-End Encryption (E2EE) exemplifies the risk of not having consistent online safety standards, and supports the case for regulation.

Encryption and E2EE have grown in popularity in recent years as the public have become more conscious of protecting their online data and privacy. E2EE is one of the most effective privacy safeguards available. The UN Special Rapporteur on Freedom of Expression has described E2EE as "the most basic building block for digital security on messaging apps", highlighting the protection it can afford to minorities at "serious risk of human rights violations and persecution".[120] E2EE is already integrated into some messaging services, and a number of large platforms have announced plans to implement[121] or extend the functionality.[122]

WHAT IS 'END-TO-END' ENCRYPTION (E2EE)?

A form of encryption wherein the content of each message is visible only to the sender and recipient. Unscrambling the message requires a private decryption key exchanged between correspondents, so that while the message may be intercepted, it cannot be viewed or monitored by the service provider, law enforcement or any other third party.[123]

However, E2EE undermines efforts to tackle child sexual exploitation and abuse online. Most detection technologies (for example, 'hash-matching'; grooming detection algorithms; classifiers to identify child sexual abuse material) are not readily deployable within E2EE environments.

Disagreement in Europe over the use of automated detection technologies has provided an inadvertent preview of the likely consequences if it were no longer possible to deploy such tools. NCMEC saw a 58% decrease in EU-related Cyber Tipline reports when their use was discontinued by some companies in December 2020 in order to comply with the European e-Privacy directive.[124] [125] A temporary derogation to the legislation was agreed in May 2021,[126] but this only enables detection to be reinstated for three years. As highlighted by ECPAT,[127] a long-term legislative response is required to resolve the issue. It is hoped that the EU's adoption of a new child rights strategy,[128] and work to enhance the fight against child sexual abuse online,[129] will pave the way to a solution.

By hiding the scale of detectable child sexual exploitation and abuse online,[130] the proliferation of E2EE could make it difficult to argue for increased investment to combat the threat.[131] It is also likely to complicate investigation by law enforcement, because applications for warrants to gain access to suspects' devices (to secure evidence of crimes) would not be able to cite the content of communications. Instead, these would be limited to the incorporation of metadata (see *Glossary of Terms*) and other indicators that point to 'probable' suspicious activity.[132] While such intelligence can be used by platforms to monitor high-risk actors, as explained by the Virtual Global Taskforce, metadata "is usually insufficient to meet the threshold required for a search warrant".[133] The National Crime Agency (NCA) in the UK highlighted its investigation into prolific online offender David Wilson, who used fake social media profiles to trick at least 500 young boys into sending sexual videos and images of themselves, and then proceeded to blackmail and terrorise them. The NCA warned that not only would E2EE have reduced the likelihood of Wilson's offences being detected, it would also have potentially prevented access to the 250,000 messages that provided the evidence to convict him.[133] Increased use of E2EE could also undermine the detection of abuse in non-encrypted environments, by reducing access to child sexual abuse material required to train classifiers and other tools that detect illegal content.[135]

Innovation is underway to make detection tools compatible with E2EE. 'Homomorphic' encryption is emerging as a potential solution because it offers a way of analysing encrypted data without decrypting it first.[136] Research efforts are focused on improving the efficiency of the technology, to enable deployment at scale. Other proposals include:

- Building detection tools into browsers and device operating systems (reducing reliance on platforms to detect abuse).[137]
- The use of secure 'enclaves' that would provide a protected environment in which to decrypt, scan, and then recrypt content for onward transmission.[138]
- The creation of digital 'signatures' for content at the point of transmission. These would be transmitted alongside encrypted content, enabling online service providers to screen messages for the signatures ('hashes') of known child sexual abuse material.[139] [140]

None of these solutions would directly facilitate law enforcement access to content: police would still require suspects' or victims' devices to prove offences.[141] However, they could enable more proactive detection and removal of child sexual abuse material (as opposed to reactive activity, triggered by user reports or police investigations).[142] Privacy proponents might argue that such measures are disproportionate given that the benefits of E2EE are more relevant than the issue of child sexual exploitation and abuse online for the majority of internet users.[143]

Voluntary co-operation and transparency are key complements to regulation, required to cohere the global response.

By helping companies balance user privacy and safety, internet regulation could partially mitigate the impact of E2EE on the detection of child sexual exploitation and abuse online. Laws have potential to enhance prevention: the Canadian Centre for Child Protection regard regulation as critical to reduce the "high levels of image recidivism" and "long delays in removal times", by the provision of commercial and legal incentives "to prevent images from surfacing or resurfacing in the first place".[144]

Implementing new internet laws will undoubtedly bring challenges. They represent uncharted territory for many governments, and throw up difficult questions, such as:

- How to prevent harm without unduly curtailing freedom of expression.
- What constitutes 'harmful' content (illegal content is easier to define).
- How to mitigate the risk that laws have a disproportionate commercial impact on smaller companies.
- For companies with an international user base, how to ensure compliance with regulation in different jurisdictions.[145]

Adaptability and close consultation with online service providers will be critical through implementation, to increase the chance of laws delivering anticipated benefits.

Ultimately, a global solution will be required: international agreement is the only way to reduce the risk of creating what Australia's e-Safety Commissioner characterises as "a regulatory 'splinternet' of different laws between countries and regions". Such global inconsistencies could undermine effective oversight,[146] whether due to companies or internet users themselves adapting their activities to evade regulation. It is possible that "as big platforms crack down...there is an exodus to spaces that are more difficult to scrutinise and moderate".[147] Already the user bases for some larger platforms appear to be shrinking: globally the time spent using the five most downloaded social-media apps fell by 5% in 2020.[148]

In the meantime, voluntary co-operation and transparency exist as important complements to regulation. In addition to bridging emerging gaps between different regulatory frameworks, co-operation and transparency also enable responsiveness to tackle a fast-evolving threat.

Transparency from online service providers is critical to improving our understanding of the threat, and what makes for an effective response. As detection and disruption tools become more advanced, transparency is increasingly important to establish consistent standards for their proportionate use, and to "alleviate fears about 'mission creep' and misuse of technology".[149]

International voluntary co-operation has advanced (see Figure 11), alongside technology innovation. More work is needed to ensure that initiatives are geographically inclusive, and involve the broad range of stakeholders with a role in providing online services. For example, extending beyond platforms to device manufacturers and mobile network operators.

Figure 11: Examples of international voluntary co-operation.

Voluntary Principles

Developed at the Five Country Ministerial Digital Industry Roundtable in 2019, the Voluntary Principles provide a framework for technology companies of all sizes to tackle the threat of child sexual exploitation and abuse online.[150] A list of Alliance Members and other companies that have endorsed the Principles is found **here**.

Digital Trust and Safety Partnership

Industry framework established by nine of the world's biggest technology companies in February 2021. The scope of the partnership is broad and encompasses the handling of all harmful content and behaviour online.[151]

Technology Coalition 'Project Protect'

'Project Protect' has established a multi-million dollar Research and Innovation Fund to develop tools to prevent and eradicate child sexual exploitation and abuse online, to be spearheaded by the global companies that comprise the Tech Coalition consortium.[152]

NCMEC saw a 58% decrease in EU-related Cyber Tipline reports when their use was discontinued by some companies in December 2020 in order to comply with the European e-Privacy directive.

06
Harms

Grooming children online for the purpose of sexual exploitation and abuse

As more children enjoy increased access to the internet, there is a significant risk that the incidence of online grooming continues to grow, unless protective solutions are implemented.

In 2020, NCMEC reported a 97.5% increase in 'online enticement'[153] – a broad category of exploitation that encompasses online grooming. According to NCMEC it involves "an adult communicating with someone believed to be a child via the internet with the intent to commit a sexual offence or abduction".[154]

Netclean's 2020 survey of 470 police officers from 39 countries also uncovered an increase in attempts to contact children, corroborating the inference that the incidence of online grooming is increasing.[155]

Grooming can often lead to the full spectrum of harms comprising child sexual exploitation and abuse: including production of imagery; coercion; extortion; and in-person abuse, the consequences of which can be severe. A NCMEC study of sexual extortion reports logged between 2014 and 2016 revealed that of the victims who had experienced a negative outcome, one in three had engaged in self-harm, or threatened or attempted suicide.[156] There is evidence that online grooming is also being used by traffickers to recruit children for commercially motivated sexual exploitation.[157]

It is difficult to dig deeper into the prevalence of online grooming because many countries are yet to define it in law. A benchmarking exercise conducted by Economist Impact in 2020 to rank country responses to child sexual abuse revealed that of 60 countries examined, only 21 had legislation that outlaws online grooming for sexual purposes.[158] The absence of a legal definition complicates reporting and investigation on a national and international level. Grooming is criminalised in the 'Lanzarote Convention' (the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse – see Glossary of Terms).

However, this definition supposes a proposal to meet followed by 'material acts' leading to a meeting. It needs updating to address situations where the abuse is perpetrated solely online.[159]

Characteristics of the digital environment have created new risk factors for online grooming.

A 2017 study estimated that by age 12, 50% of children in the world have social media accounts:[160] a digital 'footprint' which "help predators immerse themselves in children's lives as a precursor to making contact".[161] Information gleaned through features such as geotagging of images and 'checking in' to places can also be used by offenders to heighten their victims' sense of entrapment, or provide opportunities for an offender to physically locate a child. The internet has to some extent also normalised communication with strangers – the 2020 EU Kids Online Survey found that being in contact with someone unknown online is a common experience for 37% of children.[162]

The internet enables grooming tactics that are not replicable in the physical world:

> ***"For those whose intent it is to exploit children, it's far easier today than it was 20 or 30 years ago to cast as wide a net as possible. They can send a thousand requests in a matter of days, and receive 999 declines. It takes just one accepted chat or friend request to open the door."***
>
> Thorn, April 2021[163]

An analysis of reports of 'Online Coercion and Sexual Extortion of Children' logged by NCMEC between

2013 — 2016

revealed the use of multiple platforms in

42%

of cases.

How children respond in such situations is a function of a complex interplay of factors. Since early 2020, these include a child's individual experience of COVID-19. As the UK charity the NSPCC warned: "Feelings of loneliness brought on by the pandemic situation have led some children to seek company and support from strangers, putting them at increased risk of being groomed."[164]

Online environments offer diverse opportunities for those seeking to groom.

A common tactic employed by perpetrators of online grooming is the use of multiple channels to access a wider pool of potential victims and evade detection. Offenders seek to systematically migrate a conversation from a public platform to a private messaging forum — a technique known as 'off-platforming'. Typically, exchanges are moved onto applications that either use E2EE (assuring that communications cannot be monitored), or those lacking built-in tools to detect predatory behaviour. Offenders frequently migrate in high numbers to newer platforms with underdeveloped safety and moderation mechanisms. An analysis of reports of 'Online Coercion and Sexual Extortion of Children' logged by NCMEC between 2013 and 2016 revealed the use of multiple platforms in 42% of cases.[165] The Economist Impact survey commissioned alongside this report found that 68% of respondents who received sexually explicit material online as children received it through a private messaging service.

Children report having been approached by groomers "on social media networks, instant messaging apps, live streaming platforms, and voice or text chat services built into online multiplayer games".[166] Gaming platforms pose complex child safety challenges because within such environments, interactions between adults and children are relatively normalised. In-game socialisation is enabled by built-in audio and video chat, and platforms that allow gamers to livestream as they play. Europol has warned that children "are more exposed to potential offenders through online gaming",[167] partly as a result of COVID-19, which is credited with causing gaming industry growth in 2021 to exceed previous forecasts by 50%.[168]

MARIE COLLINS FOUNDATION: Olivia's Story

Olivia* was sexually groomed online by multiple offenders over a period of two years. She was 10 years old when the abuse was discovered. The primary offender groomed her through a children's gaming app before moving communications onto more private apps.

He shared Olivia's details with other abusers, who began to contact her directly, sending her links to pornographic videos to normalise the sexual behaviour and 'teach' her what to do. They were males in several different countries, communicating via the dark web.

Olivia eventually 'disclosed' the abuse by leaving her mobile device unlocked, with emails from the abusers on display for her father to see. She was receiving hundreds of emails from different men and was unable to keep the secret any longer: she was scared and wanted the abuse to stop.

The abuse had a huge impact on Olivia's mental health, and her sense of self.

The Marie Collins Foundation (MCF) is a UK-based charity whose vision is to ensure that all children and young people who suffer sexual abuse are supported to recover and live safe, fulfilling lives.[169]

*a pseudonym

Uncovering offenders' 'masked words' reveals more harmful content on gaming platforms.

The anonymity and borderless nature of the internet, along with ease of access to perceived safe spaces online, gives perpetrators the confidence to share child sexual abuse material, and tactics and 'tradecraft' for evading detection, through offender networking.

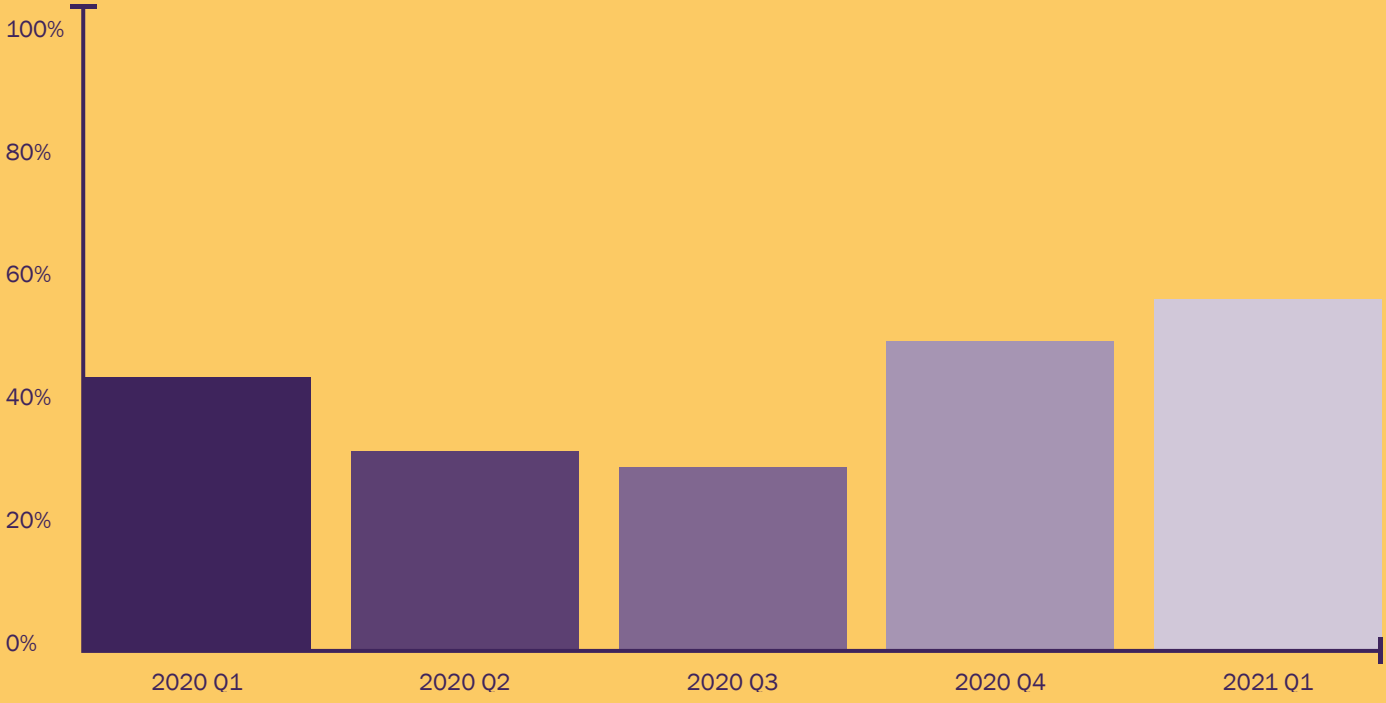
For the gaming industry, chat rooms, voice calls and livestreams have provided more ways for offenders to initiate contact with children and begin the grooming process. A Crisp analysis of dark web conversations featuring mentions of three popular global gaming platforms uncovered an ongoing dialogue between offenders, ostensibly to share relevant grooming tips. The number of conversations increased on average by 13% across the platforms from 2019 to 2020.

Crisp also observed the continued use of 'masked words' by offenders on the platforms themselves. These are words in which key letters are replaced with numbers or symbols in order to evade detection methods (e.g. typing '8!rthday' instead of 'Birthday'). By identifying when offenders attempted to mask words on the platforms, Crisp identified up to 50% more pieces of content containing these terms, leading to the identification of more harmful content and the bad actors behind it.

User safety — in gaming or on any social media / user-generated-content platform — demands the ability to quickly identify harmful content and the strategies behind its creation. The application of this intelligence is essential for the identification of offenders, and to inform policy updates to prevent future harm.

Figure 12: Additional content found when masked terms were identified.

Additional percentage of content containing key terms when looking for masked terms



Solutions exist to detect online grooming, but adoption is not widespread, and technical challenges persist.

Tools that use artificial intelligence to identify and block child grooming conversations are already in use. However, just 37% of companies who responded to a WeProtect Global Alliance / Technology Coalition survey deploy such technology.[170]

Detecting online grooming presents challenges. Building tools relies on developers having access to grooming chat 'scripts' to train algorithms. While there are examples of effective collaboration between police, platforms and developers, there is scope to streamline data-sharing to enhance innovation. Additional difficulties include developing tools that can work in multiple languages and overcome the use of slang and codewords. Continued innovation is required to enhance the accuracy of such tools, which would also minimise unjustified intrusions of user privacy.

The most effective solutions are those that can detect high-risk conversations to prevent grooming before it takes place. Such technology is complex however, not least because "chat can escalate very rapidly... a conversation can take a sexual turn in just three minutes".[171] Most grooming detection tools are not readily deployable within E2EE environments.

The incidence of online grooming could be significantly reduced by making online environments 'Safe by Design'.

'Safety by Design' is an initiative of the Australian e-Safety Commissioner, now popular worldwide, which establishes user safety as "a fundamental design principle that needs to be embedded in the development of technological innovations from the start". [172]

'Safety by Design' solutions with the most potential to reduce the risk of online grooming include age estimation and age verification tools. Such technology is still relatively nascent,[173] but could be used to exclude predators from children's forums, and ensure age-appropriate online experiences. Other examples include parental controls and content filters. Many mainstream platforms already incorporate some of these:

- Gaming platform **Roblox** has built-in security software blocking explicit content and preventing young users sharing their contact information.[174]
- Social networking platform **TikTok** has introduced default privacy and safety settings for under 18s.[175]
- **Instagram** is adding safety features to protect teenagers from unwanted direct messages from adults they don't know.[176]
- **YouTube** has developed 'Supervised Experiences' for children under 13, limiting their ability to upload content, chat or receive comments, and helping parents manage content they access.[177]

Such features can reduce children's risk of falling victim to online grooming by limiting offender opportunities and educating children about online risks. They can also increase the effectiveness of other safety mechanisms by reducing the volume of incidents overall to enable more targeted monitoring and safeguarding.

YOTI: AGE ESTIMATION TECHNOLOGY

YOTI is a UK-based global identity platform with age estimation technology.

YOTI's age estimation AI analyses an individual's face and produces an age estimate in 1-1.5 seconds without revealing or keeping any personal data. It currently delivers a mean accuracy rate of 2.19 years across all ages and 1.5 years for 13-25 year olds – ensuring age appropriate moderation with industry standard age thresholds. It's also inclusive for the 13% of the global population that doesn't own photo identification.

To date, YOTI age estimation technology has conducted more than 500 million age checks for partner organisations: including live streaming; ecommerce; adult; gaming; and telecom operators.

We must improve our understanding of online grooming to enable continued effective prevention and detection.

The effectiveness of interventions may be limited if gaps in knowledge and research are not addressed.

We still do not fully understand the interplay between online and 'in-person' grooming, and the complexities of intervening to prevent such abuse particularly if the groomer is known to the child (as is the case in most instances of 'in-person' grooming).[178] Linked to this, there is a need to improve our understanding of offending pathways for those who groom children online, and the risk and protective factors that affect the likelihood of a child being abused. It has been highlighted for example that children with disabilities may have particular vulnerabilities because they turn to the internet to compensate for a lack of real-world support or connections.[179] Insights on such questions can be applied to design powerful, tailored interventions to protect children and further remove or reduce offender opportunity.

06
Harms

Producing child sexual abuse material

When the abuse of a child is documented, the perpetrator also commits an offence of producing child sexual abuse material.

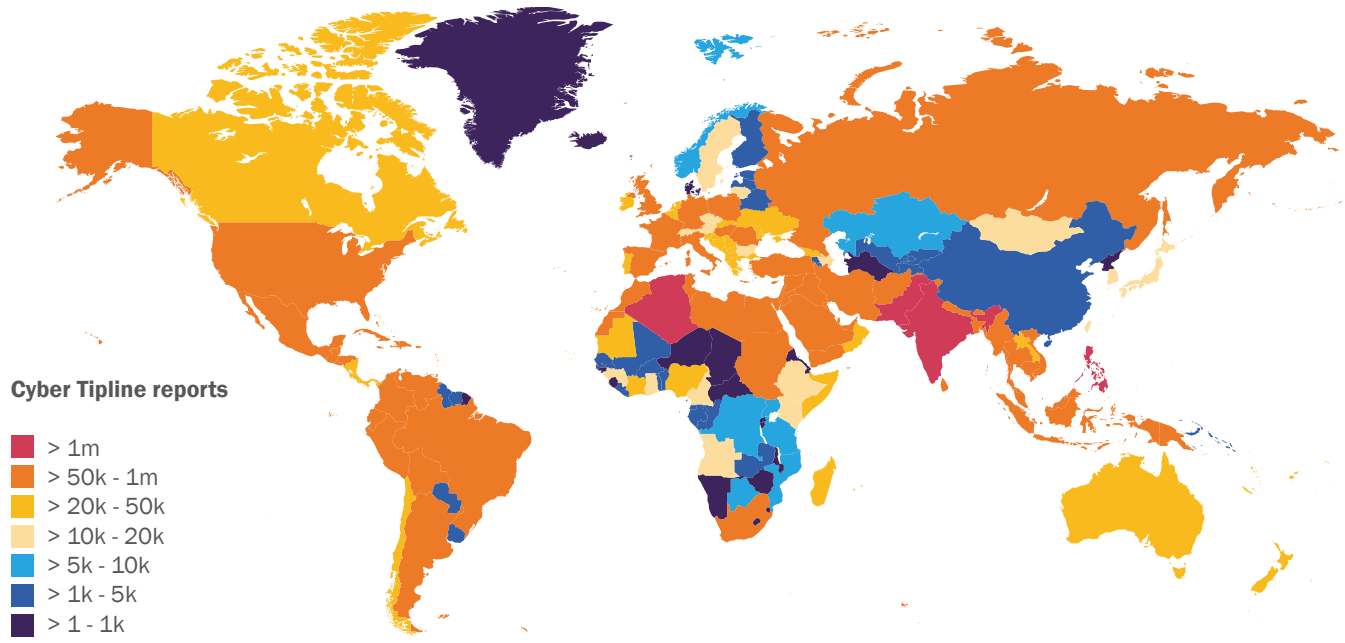
Offenders are evolving their production methods, often to take advantage of new technologies.

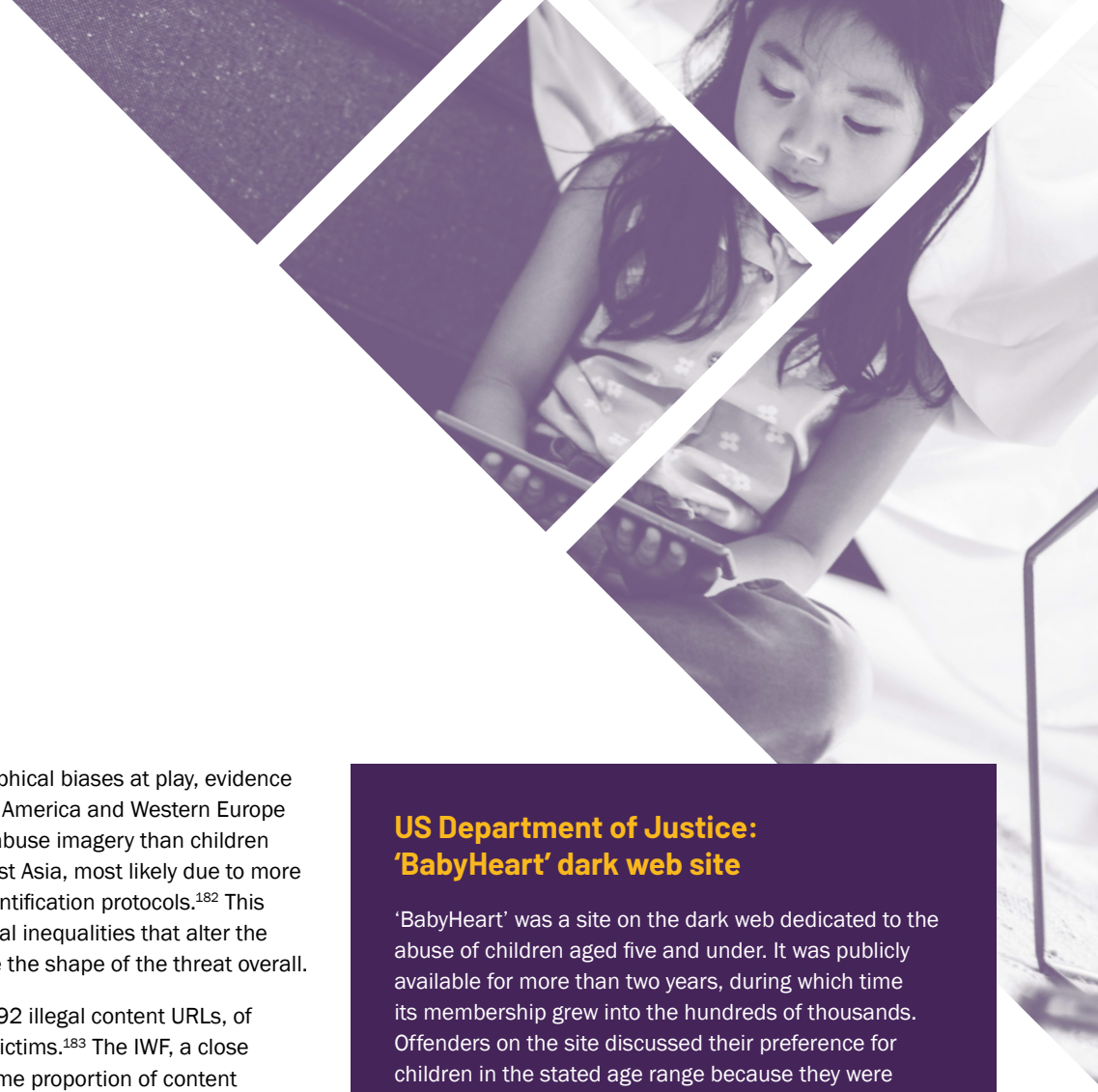
Production is most likely happening in all regions of the world. Girls of all ages appear in imagery most often.

A joint study by Thorn, Google and NCMEC in 2019 found that 81% of reports of child sexual abuse material came from Asia, Africa and Europe.[180] The latest evidence from NCMEC (see Figure 13 below) indicates that the same regions, with the addition of the Americas, continue to generate a large proportion of referrals.

Unfortunately, such data offer an inherently limited view of global trends. For one, the origin of reports may not be the same as the origin of the images. In addition, reports only convey the extent of the 'known' issue. It is highly likely that (more) production is happening in countries where there are fewer or no established mechanisms to detect it. This is supported by the results of the Economist Impact survey, which found that children are experiencing online sexual harms in all regions of the world.

Figure 13: The origins of reports of suspected child sexual exploitation received by NCMEC's Cyber Tipline in 2020. Reproduced with the permission of NCMEC. [181]





Further demonstrating the geographical biases at play, evidence indicates that children from North America and Western Europe are more likely to be identified in abuse imagery than children from Eastern Europe and Southeast Asia, most likely due to more advanced reporting and victim identification protocols.[182] This pattern is symptomatic of the global inequalities that alter the local impact of abuse, and change the shape of the threat overall.

In 2020, INHOPE assessed 267,192 illegal content URLs, of which 93% involved female child victims.[183] The IWF, a close partner to INHOPE, reports the same proportion of content featuring girls, of the URLs assessed by its team.[184] This does not necessarily mean girls are more subject to abuse than boys. In fact, the Economist Impact survey found only a slight difference in reported experiences of online sexual harms between male and female respondents. The abuse of boys may simply be less documented. It may suggest however that girls are more likely to experience prolonged harm as a result of production, sharing and further distribution of their imagery.

Child sexual abuse material is often produced by family members. This creates a raft of detection and prevention challenges.

According to the IWF, child 'self-generated' sexual material predominantly features children in a home setting.[185] Within the past year, more production in home environments has also been attributed to criminal groups adapting their ways of working through COVID-19, "escalating the use of online communication and exploitation in homes".[186] However, for the most part imagery is generated within family homes because family members are often producers of child sexual abuse material:

- A study of child sexual abuse cases in Colombia found that offenders are usually in the child's circle of trust or nuclear family.[187]
- In Mexico, 73% of sexual abuse offences against children are committed by relatives, and 75% of abuse occurs in victim's homes.[188]
- A study of 150 adult survivors in Australia found that 42% identified their biological, adoptive or step-father as the primary abuser, and producer of child abuse material.[189]
- A study of child abuse cases in Spain revealed that in 80.2% of cases, the abuser belonged to the victim's circle of trust – and was their biological father in 32% of cases.[190]

Suffering sexual abuse at the hands of a family member can create additional, complex trauma, not least because this type of abuse often starts when victims are younger, and lasts longer.[191] Victims of familial abuse are also least likely to disclose, although self-reporting is low generally among child sexual abuse victims. Just 2% of NCMEC's Cyber Tipline reports come from children themselves.[192]

Despite significant advances in image analysis and facial recognition technologies, victim identification rates remain low overall. As of April 2021, the Canadian Centre for Child Protection's Project Arachnid had processed 126 billion images, 85% of which feature victims who are as yet unidentified.[193] Victim identification challenges underscore the critical importance of educating whole communities and investing in child protection systems to improve the detection of abuse, so victims can be identified and safeguarded.

US Department of Justice: 'BabyHeart' dark web site

'BabyHeart' was a site on the dark web dedicated to the abuse of children aged five and under. It was publicly available for more than two years, during which time its membership grew into the hundreds of thousands. Offenders on the site discussed their preference for children in the stated age range because they were perceived as less likely – or unable – to report the abuse, and were considered to be 'lower risk'. Most of the imagery shared on 'BabyHeart' was undoubtedly produced through familial abuse or in other care provider scenarios. This starkly underscores the importance of prevention and detection mechanisms that do not rely on children coming forward, and which do not assume that families are protective.[194]

The Australian Centre to Counter Child Exploitation has identified 'capping' as the most problematic current offending trend, which is generating approximately

60%–70%

of referrals to its Victim Identification Unit.

In 2020, an AI 'bot' operating on Telegram generated

100,000

pornographic 'deepfakes' of real women and girls.

Offenders are evolving their production methods. Some are covert, and children may be unaware they are victims.

'Capping' has become more prevalent in recent years, with some law enforcement agencies reporting a marked increase during the COVID-19 pandemic.[195] [196] [197] It usually involves the grooming and sexual coercion of children and has been linked to the rise in child 'self-generated' material. Offenders target children on a variety of platforms and seek to gain their trust, before coercing them into sexual acts that are captured on camera. Material is then shared in dark web forums. According to Europol, the number of messages and threads in a section for 'cappers' in one dark web forum more than tripled between December 2019 and February 2020.[198]

The Australian Centre to Counter Child Exploitation has identified 'capping' as the most problematic current offending trend, which is generating approximately 60-70% of referrals to its Victim Identification Unit. 'Capping' also illustrates the potential for 'gamification' (see *Glossary of Terms*) of abuse. One site on the dark web monitored by law enforcement holds monthly competitions and 'capping battles', where cappers go head-to-head posting abusive imagery.[199]

While some children will know they have been victims of 'capping', others may be unaware. The covert creation of child sexual abuse material is a broader production trend enabled by a range of digital devices including webcams (sometimes hacked), and home or school security cameras. In South Korea, the phenomenon is known as 'molka' and is taken to the next level by the deployment of spy-cams in everyday objects such as pens.[200]

Technologies such as Computer-Generated Imagery (CGI) may enable further diversification of production, and require changes to legislation.

Currently 'deepfakes' and 'CGI' are not commonly encountered in child abuse investigations.[201] However, they may become more popular. In 2020, an AI 'bot' operating on Telegram generated 100,000 pornographic 'deepfakes' of real women and girls.[202] Relatedly, the adult virtual reality cyber-sex industry has seen significant growth, partly attributed to the impact of COVID-19 lockdowns.[203] The Australian e-Safety Commissioner has expressed significant concern about the potential use of virtual reality and other 'immersive technologies' as a "tool for online child sexual abuse".[204]

Computer-Generated Imagery (CGI) and 'deepfakes'

CGI is the creation of still or animated visual content with imaging software.[205] In the context of child sexual abuse, this refers to wholly or partly artificially or digitally created sexualised images of children.[206] 'Deepfake' is a form of CGI that uses artificial intelligence (AI) to replace one person's likeness with another in photos or recorded video.[207]

Key concerns are the low barriers to use and the convincing nature of the results. Even simple filters built into popular applications are capable of transforming content at the click of a button. Some types of CGI could create prioritisation challenges for police if it becomes difficult to distinguish a real child from a synthetic persona.[208]

CGI and associated technologies are unlikely to dominate in this space as things stand, primarily due to the availability of photographic child sexual abuse material online. However, they merit consideration, not least because they reiterate the need for an internationally agreed position on a range of non-photographic materials that contribute to proliferate the threat. For example, CGI; 'deepfakes'; anime; cartoons and drawings depicting child sexual abuse; and child-like 'sex dolls' sold on the internet.

CGI is harmful because "it is known to be used in grooming children... it fuels very real fantasies, encourages the propensity of sexual predators, and contributes to maintaining a market for child sexual abuse material".[209] There is ample evidence to support this position, including the fact that such material is often found alongside sexual photographs of children.[210] Yet very few countries have enshrined the principle in legislation.[211]

CGI can also be used to enable powerful disruption techniques, as exemplified by the case of 'Sweetie' – the CGI child persona used to entrap more than 1,000 predators.[212] Many offender networks require prospective members to share new material to gain entry to closed groups; artificial imagery could also be used to help police infiltrate such communities. Global law enforcement collaboration is critical to deconflicting the wider use of such tactics; consensus is also required on the ethics of deploying technology for such purposes.[213]

06

Harms

Searching for and / or viewing child sexual abuse material

Attempts to access child sexual abuse material are increasing. Tackling both the 'supply' and 'demand' sides of the issue is critical for sustainable long-term prevention.

Most child sexual abuse material is accessed through the surface web, E2EE apps, or via peer-to-peer (P2P) sharing.

It can take just three clicks to discover child sexual abuse content on the internet.[214] Most material is accessed this way – via the surface web, or through P2P networks.[215] According to Interpol, the latter were used more through 2020.[216]

Many individuals convicted for viewing child sexual abuse material are shown to have made little or no attempt to cover their tracks,[217] although evidently this sample is somewhat skewed. As highlighted in the Theme Chapter: *Technology*, a proportion of offenders use advanced tools and methods to evade detection. One documented technique involved creating apps that directed users to closed messaging groups used to share imagery.[218] According to Europol, distribution of child sexual abuse imagery "routinely takes place on social networking platforms".[219]

Offenders often use platforms and E2EE applications, environments that combine surface web accessibility with a high level of security. As highlighted in Europol's 2021 Serious Organised Crime Threat Assessment, "the widespread use of encryption tools, including E2EE apps, has lowered the risk of detection" for those who offend against children.[220] Use of apps creates significant challenges for law enforcement, as police need to infiltrate closed messaging groups to obtain evidence of offences. Once entry is gained, many police agencies are limited to the use of manual data collection. The Child Rescue Coalition is leading the development of a solution to streamline acquisition of evidence from mobile device applications in real-time. The tool is designed for use by undercover officers who have infiltrated offender groups. By reducing the need for manual data collection, it could significantly enhance the efficiency of undercover operations. Continued collaboration with international law enforcement is critical to maximise its impact, and ensure that it supports enhanced victim identification and safeguarding.[221]

The dark web hides the most extreme content and enables sharing and networking across offender communities.

Dark web

The layer of information and pages that can only be accessed through so-called 'overlay networks' (such as Virtual Private Networks (VPN) and peer-to-peer (P2P) file sharing networks) that obscure public access. Users need special software to access the dark web because a lot of it is encrypted, and most dark web pages are hosted anonymously.[222]

Overall, dark web activity has increased by 300% in the past three years.[223] The dark web is reportedly a hub of younger[224] and more extreme content[225] depicting child sexual exploitation and abuse online.

Dark web offender communities have persisted and evolved for over a decade. In this sense they do not represent a new dimension to the threat. What has changed is the availability of anonymity solutions such as Tor and VPNs, which are now mainstream and even built into some web browsers by default.[226]

Tor

'Tor' is an open source privacy network that permits users to browse the web anonymously. The system uses a series of layered nodes to hide web addresses, online data and browsing history. [227]

Individuals now need minimal technical knowledge to obfuscate their online activity. For law enforcement, the challenge is to stay one step ahead of offenders who are more able to use such capabilities, which grant ready anonymity to help them avoid getting caught.[228] [229] [230]

Attempts to access child sexual abuse material are rising. There is evidence to suggest a link between habitual exposure to extreme adult sexual content and viewing child sexual abuse material.

In 2020, 8.8 million attempts to retrieve child sexual abuse material were tracked by three of the IWF's member organisations in just one month.[231] During COVID-19 lockdowns in India, there was a 95% rise in searches for child sexual abuse material.[232] The UN Human Rights Council also reported that the demand for child sexual abuse material increased by up to 25% during the pandemic in some member states of the European Union.[233]

It is conservatively estimated that 1% of the global male population is affected by paedophilia (sexual attraction to prepubescent children).[234] Many such individuals seek and view child sexual abuse material knowingly to address their sexual desires.[235] Advanced policing capabilities are critical to identify such offenders and manage the associated risks – including the possibility that they progress to committing in-person abuse against children.

There are many other pathways to viewing child sexual abuse material. According to the Lucy Faithfull Foundation, only 15-20% of the offenders they currently work with are paedophiles "in that prepubescent children are their primary sexual interest".[236] Several studies have drawn a link between viewing child sexual abuse material and habitual exposure to extreme adult pornography: purportedly because it can cause desensitisation and create an urge to seek out more severe stimuli to continue achieving the same level of sexual arousal.[237] [238] Two particularly problematic areas are so-called 'abuse-themed pornography'[239] and pornography that seeks to portray adults as children. The former makes it easier for viewers "to take the next step of watching real abuse"; the latter has been described by offenders as a gateway to viewing child sexual abuse material.[240]

The link with consumption of extreme pornography is worrying, given that children's exposure to adult sexual content has increased drastically in the digital age. Studies from several East Asian countries suggest that 50% of children and young people have been exposed to 'sexually explicit media', while the United States, Australia and a number of European countries report exposure rates of 80% or higher.[241] Frequent viewing of adult pornography or violent pornography from a young age is associated with viewing child sexual abuse material.[242]

The way in which users are guided to interact with online content also contributes to accelerating pathways to offending. The primary means of driving user engagement on social media platforms is content recommendation. Broadly, there are two models for this. The first is the 'social graph' algorithmic model, which presumes a user's interests by prioritising the activities of their connections. The second is the 'interest graph' model, which infers a user's interests based on past activity and engagement. For users inappropriately seeking content involving children, such algorithms risk encouraging the behaviour by repeatedly recommending similar images and videos.[243] [244] Combined with high video view counts and accompanying threads of troubling comments that often escape the notice of moderators,[245] the total effect is to ease the overcoming of internal inhibitions to abuse.[246] [247] Some major platforms claim to have detection mechanisms and moderation policies in place to support the identification of such behaviour.[248] The timeliness and effectiveness of such measures is critical because, as explained by the UK's National Centre for Social Research, "desensitisation / online disinhibition and validation from other offenders are often reasons for viewing child sexual abuse material and / or moving on to contact offending".[249]

Disrupting searches for child sexual abuse material can deter offending, but the impact of such interventions is hard to measure.

The evidenced link between viewing content and in-person abuse underscores why the disruption of attempts to search for imagery is so important.

The majority (60%) of respondents to a WeProtect Global Alliance / Technology Coalition Tech survey confirmed that they issue some form of deterrence messaging.[250] Search filtering is a popular mechanism used mainly by search engines. User queries are cross-referenced with a list of content to be blocked, so if a match is made no results are returned. In some cases, a warning is also issued to the searcher. When implemented by both Google and Microsoft in one year, the overall number of web-based searches for abuse images reduced by 67%.[251]

A study funded by the Australian government found that online warning messages issued to users seeking to view 'barely legal pornography' increased attrition rates by up to 25%.[252] Similarly, Lucy Faithfull's 'Stop it Now!' campaign in the UK and the Prevention Project Dunkenfeld in Germany both demonstrated that deterrence can promote help-seeking among (potential) offenders.[253] The Oak Foundation recently committed to fund a new research project to identify and evaluate perpetrator prevention initiatives and help build capacity to implement them through an online hub for policymakers and practitioners.[254]

LUCY FAITHFULL FOUNDATION: MINDGEEK (PORNHUB) COLLABORATION

The Lucy Faithfull Foundation (the Foundation) is a UK charity working to prevent child sexual abuse, including by working with adults and young people who have offended sexually or who are at risk of doing so. In February 2021, the Foundation launched a collaboration with Mindgeek to issue deterrence messages on their adult pornography website, Pornhub. Messages are shown when users make searches indicative of attempts to find sexual videos featuring children. Mindgeek had already recognised the need for deterrence messaging on its adult content sites, where it had noted attempts by a small minority of users to seek child sexual abuse material using banned search terms.

The deterrence messages clarify the law and the harm done to children in the creation and viewing of such material. They also direct users towards help to stop any illegal behaviour – including to 'Stop It Now! Get Help', an online self-directed intervention for people concerned about their online sexual behaviour towards children. Between February and early May 2021, the deterrence messages brought more than 35,000 users from across the world to 'Stop It Now! Get Help'. Although a small figure relative to Pornhub's overall traffic volumes, as highlighted by the Lucy Faithfull Foundation, it shows the important role such messages play in education and intervention.

The main difficulty with deterrence lies in measuring effectiveness. In the examples cited, it was achieved by monitoring engagement with help materials and help-seeking behaviour. This is limited – not least because it is impossible to understand if and how offending has actually been deterred. There are also questions about its long-term impact; whether users might become desensitised to warnings over time or simply move to other sites instead.

Deterrence mechanisms are a critical part of a broader response that addresses the range of pathways to viewing child sexual abuse material.

The importance of efforts to remove child sexual abuse material from the internet is indisputable. However, without also working with (potential) offenders to tackle 'demand', there is always a risk that individuals persist in finding new ways to access imagery and evade detection. The importance of balancing effort across 'supply' and 'demand' is exemplified by a current IWF initiative. Responsible for the removal of 153,600 child sexual abuse webpages in 2020 alone,[255] the organisation teamed up with the Lucy Faithfull Foundation to develop the ReThink chatbot, with the support of End Violence Partnership. The tool will engage users showing signs of searching for child sexual abuse material, and signpost support services to try to deter the behaviour before an offence is committed.[256] Deterrence initiatives are also important from a broader societal perspective, because "they are focused on changing the behaviour of adults", not children, and in so doing provide "an important message about whose responsibility it is to prevent child sexual abuse".[257]

SUOJELLAAN LAPSIA RY: REDIRECTION PROJECT

Suojellaan Lapsia Ry is a Finnish Non-Governmental Organisation that helps protect children in all environments through advocacy, research and training programmes.[258]

Its ReDirection project, supported by End Violence Partnership, began in September 2020 and will run until September 2022. It is a research initiative to gather information to inform the development of new and better ways to disrupt and deter offending. The research involves distribution of a 30-question 'Help us to help you' survey, via the dark web search engine 'Ahmia', which processes an estimated 20,000 searches daily. The survey was automatically released in response to more than 20,000 searches for child sexual abuse material over the course of three months. More than 3,100 completed surveys were returned.

On the basis of the research findings, Suojellaan Lapsia plans to design a new self-help programme for individuals searching for and viewing child sexual abuse material. The aim is to identify individuals at risk of offending and direct them to help and support services.

Amplifying our understanding of pathways to viewing child sexual abuse material will be key to ensuring an effective response. This chapter has explored just two relevant motivations: sexual interest in children, and desensitisation caused by habitual exposure to extreme sexual content. Even highly effective deterrence interventions are unlikely to dissuade the most determined individuals, hence the importance of developing law enforcement capabilities to identify persistent and potentially sophisticated offending. Equally, it is arguably neither appropriate nor feasible to pursue a criminal justice resolution for the increasing volume of viewing offences linked to online desensitisation and disinhibition.

06

Harms

Sharing and / or storing child sexual abuse material

The volume of child sexual abuse material available online is increasing. Methods for sharing and storing content are evolving.

From 2019 to 2020, the number of NCMEC Cyber Tipline reports of child sexual abuse material rose by 63% overall.[259] In the same period, the IWF also noted a 16% increase in confirmed reports of such material on both the surface web and the dark web.

The figure includes reports received from members of the public, and discoveries made by the IWF team through active internet searching. Such data would seem to indicate that the volume of child sexual abuse material available online is increasing.[260]

Globally, a large proportion of reports concern resharing material that is 'known' (as opposed to 'first generation' – see definitions below). The international INHOPE network of reporting hotlines estimates that 60% of content flagged to them in 2020 was 'known'.[261]

'Known' and 'first generation' material

'Known' child sexual abuse material is content that has been previously detected and classified by law enforcement and / or moderators. 'First generation' material is 'new' content that has not previously been detected or classified.

Video accounts for an increasing proportion of detected content: the number of video files reported to NCMEC increased tenfold between 2017 and 2020 (Figure 15). In the same period, the number of image files doubled. Given that many police and reporting agencies do not have sufficient bandwidth to process images, this trend could hamper detection unless capabilities are improved – particularly as on-device storage capacity continues to increase.[262]

Image hosts are the most common site type used to share child sexual abuse material.[264] This includes social media platforms that are often used to disseminate material via fake accounts that are then rapidly deleted.[265] Currently there is no formal, established mechanism for platforms to lawfully share identifiers associated with such accounts. This enables offenders to switch freely between platforms and services, operating with relative impunity.[266]

The use of 'hidden services' to distribute child sexual abuse material increased by 155% from 2019 to 2020.[267] These are websites hosted within a proxy network (such as 'Tor' – see glossary definition), so that their location can't be traced.[268]

While some offenders continue to amass material on devices such as laptops, mobile phones and USB sticks,[269] there are signs of movement away from the curation of personal collections, with offenders preferring 'on-demand' access to content via the use of 'file hosts:'[270] internet services that allow users to upload files for remote access.[271] Links to files containing child sexual abuse content are posted across multiple sites and often used as part of peer-to-peer sharing.

This creates a raft of challenges for law enforcement. Material is often published and hosted in different jurisdictions, which complicates evidence-gathering.[272] The volume of content in an offender's possession was historically one of several factors used to assess the level of risk they posed, but this is no longer always indicative.[273]

Cloud sharing apps fuel explosion of user interactions with harmful content.

Offender populations have come to rely on the ease of use, security and privacy of cloud file sharing apps to store and distribute illegal images and videos. Cloud storage makes it possible to share child sexual abuse material by simply posting a link in a forum, on a platform or through direct messaging, to thereby reach more offenders, more quickly.

Crisp's analysis shows that instances of user engagement or interactions with harmful content relating to child sexual exploitation and abuse exploded to nearly 20 million in the first quarter of 2021 — up significantly from more than 5.5 million in the first quarter of 2020.

Over the five quarters from January 2020 to March 2021, Crisp assessed 1,340 items containing content-sharing links deemed high-risk due to the context and communities in which they were shared. Where there was a harmful link in the content, the number of interactions ranged from 20 to 12,746 in extreme cases. Sharing across multiple locations and forums globally greatly increased the number of total user interactions with such links.

Perpetrators typically use cloud file sharing to efficiently exchange images and videos with both known and new offender contacts. To ensure that content remains accessible for as long as possible, determined offenders use multiple cloud platforms simultaneously. The true nature of harmful links is hidden behind a smoke screen of references to other (lesser) illegal activity or legitimate file-sharing uses to evade detection.

Figure 14: User Interactions with harmful content.

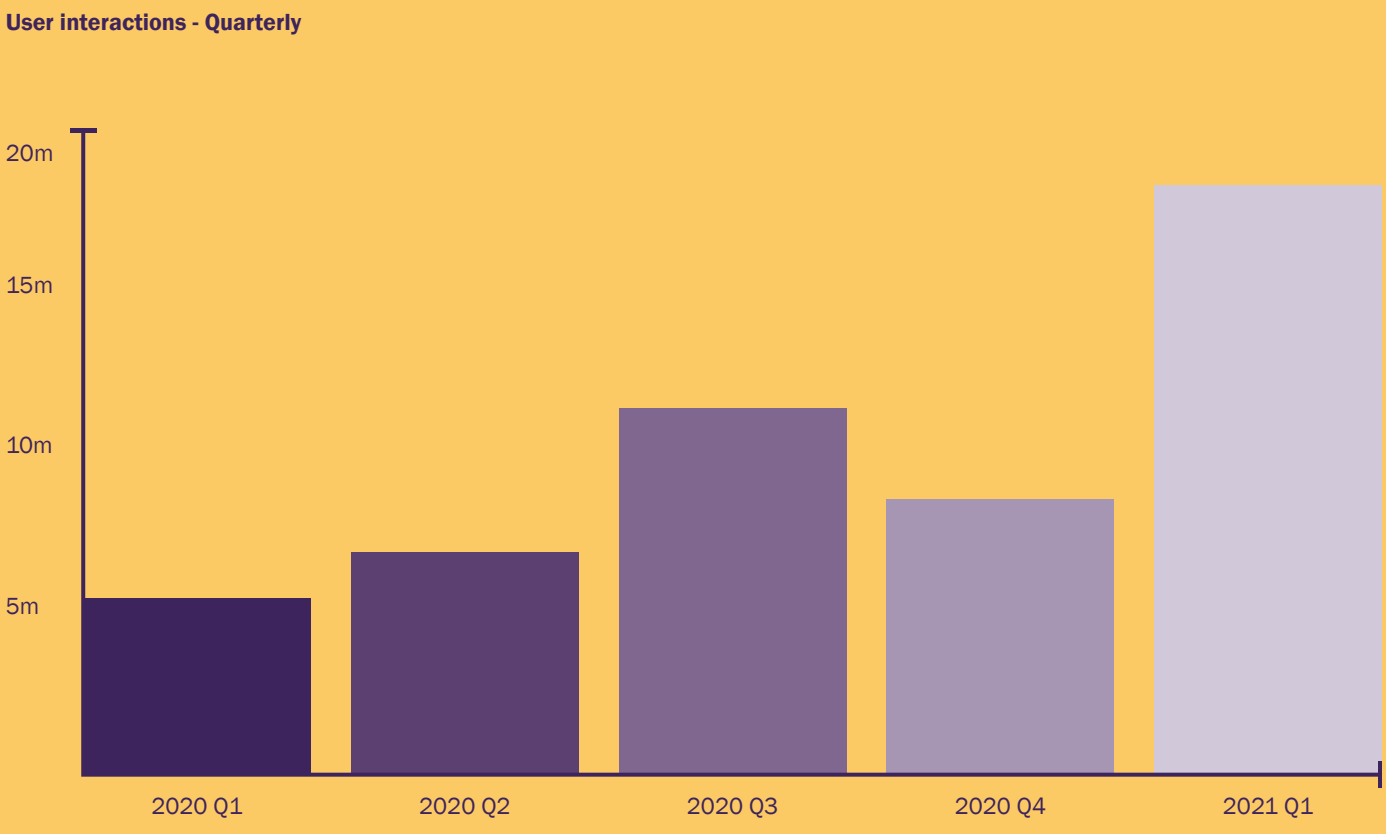


Figure 15: Growth in image vs video-based child sexual abuse material, reproduced with the permission of NCMEC. [263]

NCMEC trends data: Growth in image and video child sexual abuse material		
Year	Images	Video
2020	33.6m	31.6m
2019	27.7m	41.2m
2018	23.2m	22.2m
2017	17.0m	3.4m

Resharing of material is worsening the harm caused by child sexual abuse.

A significant proportion of reports of child sexual abuse material are generated by the resharing of 'known' imagery. Facebook has stated that more than 90% of its reports to NCMEC between October and November 2020 concerned shares or reshares of previously detected content.[274] A study of NCMEC reports logged between 2011 and 2014 found that of a sample of 2,598, imagery was 'actively traded' (had been reported back to NCMEC five or more times) in 7% of cases involving just one offender and one victim, and in 12% of cases with multiple victims and / or offenders.[275] In every case, repeat sharing "serves to re-victimise and thus further exacerbate the psychological damage to the abused",[276] often preventing closure even in cases where the offender is caught and punished.[277] As online re-sharing proliferates, the use of 'opt-in' victim notification policies (such as exist in the US) will be increasingly critical to ensure that harm is not unwittingly reinforced each time a survivor's imagery is re-discovered by police or reporting agencies.[278]

Other issues linked to re-sharing include the harassment and pursuit of specific victims, an activity which also provides offenders with opportunities to connect with like-minded individuals.

> ***In every case, repeat sharing "serves to re-victimise and thus further exacerbate the psychological damage to the abused", often preventing closure even in cases where the offender is caught and punished.***

Facebook has stated that more than

90%

of its reports to NCMEC between October and November 2020 concerned shares or reshares of previously detected content.

A study of NCMEC reports logged between 2011 and 2014 found that of a sample of

2,598

imagery was 'actively traded' (had been reported back to NCMEC five or more times).

Offenders re-traumatise survivors using fake profiles.

In a tactic that re-victimises survivors of child sexual exploitation and abuse, offenders are creating fake online profiles that misappropriate the identities of known survivors. These fraudulent accounts, which typically adopt survivors' names and feature non-harmful imagery at the account /profile level, appear on the surface web across multiple social media sites.

The accounts are used by offender communities to connect with like-minded perpetrators, primarily to exchange contact information. This can lead to trading exploitation tactics, 'tradecraft', and child sexual abuse material in a perceived 'safe space' online.

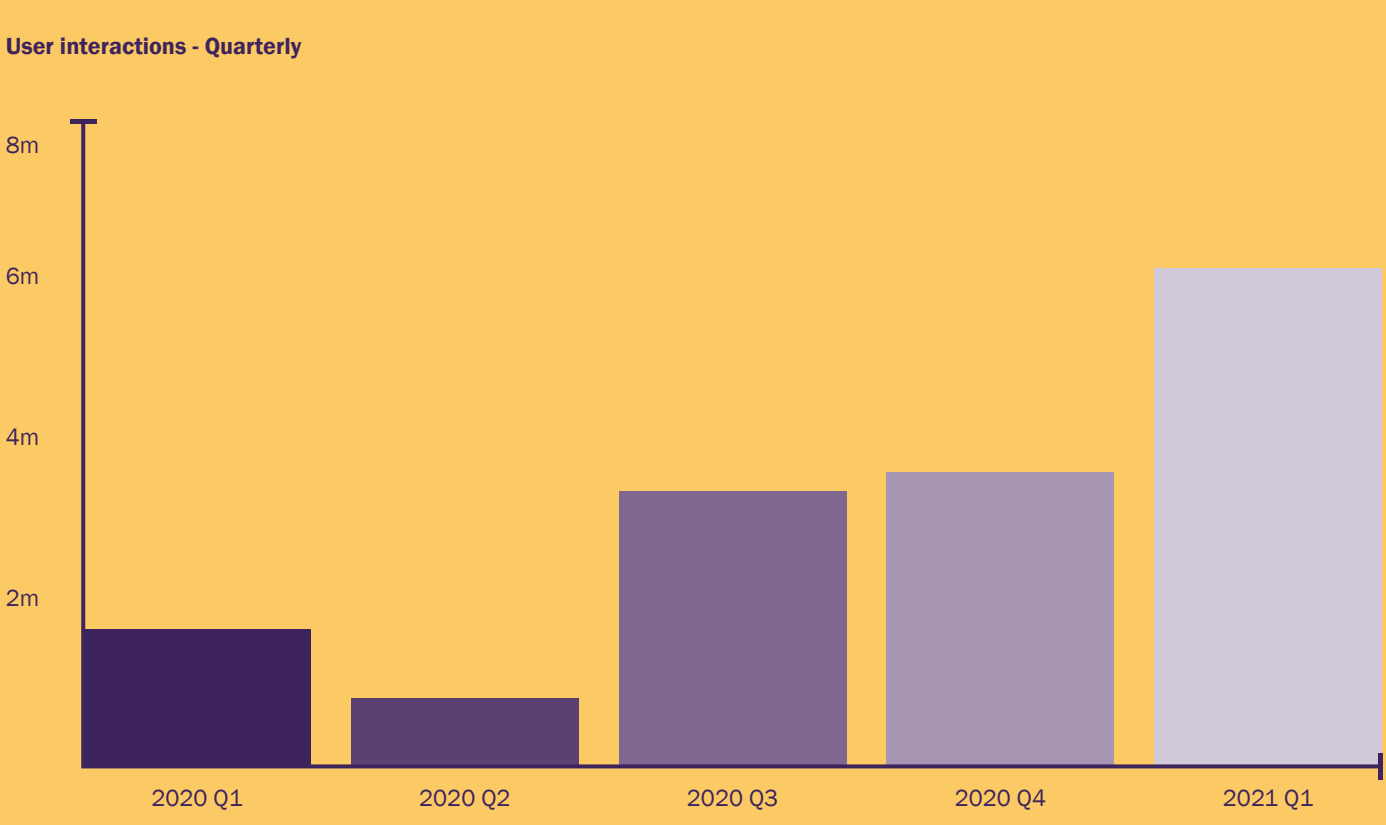
More offenders are using these accounts to publicly convey their preferences or interests, and endorse commercial websites that distribute abusive imagery.

In a disturbing trend, Crisp noted a threefold increase in user interactions with fake profiles from the first quarter of 2020 through to the first quarter of 2021.

For example, between January 2020 and March 2021, Crisp identified 3,324 pieces of content that referenced known survivors or commercial websites. On average each piece of harmful content then generated more than 2,000 interactions (likes, comments, etc.), causing a multiplier effect and reaching many more offenders.

The majority of the accounts included offender discussion and confirmation of consuming child sexual abuse material. Most references to material were linked to offences originating more than a decade prior to the creation of the fake profiles. This memorialising of past sexual abuse has the effect of re-traumatising survivors who once again experience a loss of control of their identities as depicted on social media.

Figure 16: User interactions with content referencing known survivors or commercial websites.



NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN (NCMEC): Ella's Story

Ella* was sexually abused by a family member from the age of five, for a period of seven years. Ella's abuser took images and videos of the abuse and distributed them online. NCMEC traced the location of the abuse to an area in the Western United States and referred the case to local law enforcement. Police located and rescued Ella, and the offender was convicted and sentenced.

Although the offender is now in prison, images and videos of Ella continue to circulate, and other offenders continue to harass her online. Her caregiver described the trauma created by resharing: "There's this sense that the offender going to prison is the end but it's not... At first, I was oddly grateful for the photos because that's what got them caught. But the images are still out there, they don't go away. Tens of thousands of people have seen her... even 10 years later."

Over the years, Ella has received thousands of victim notifications from the government about cases involving her images and videos. Even in adulthood, this re-victimisation has left Ella in need of continuous therapy.

Ella is now drawing on her experience to help others. She serves as a survivor consultant, helping to inform the development of NCMEC's support resources and building new programme services for other survivors.

The National Center for Missing and Exploited Children (NCMEC) is a private, non-profit corporation. Its mission is to find missing children, reduce child sexual exploitation, and prevent child victimisation.

*a pseudonym

Facebook analysed instances of sharing between 2019 and mid-2020 and concluded that 75% was 'non-malicious'. According to Facebook's taxonomy, this is sharing purported to be undertaken through outrage, attempted humour, or vigilante motives.[279] More transparency on the classification of 'non-malicious' sharing, and taxonomies applied by other platforms would be helpful to inform strategies to curb this trend. A proactive approach by online service providers is key to addressing the behaviour and mitigating the attendant risk that child sexual abuse online is increasingly normalised – and even trivialised.

Child sexual abuse material is being distributed for financial gain. This type of sharing creates unique detection challenges.

According to the IWF, while the proportion of commercial web pages containing child sexual abuse material decreased slightly (-4%) from the previous year,[280] the majority (61%) of domains analysed in 2020 were commercial in nature.[281] The IWF has continued to observe new means of monetising content, such as affiliate schemes that enable publishers to earn money every time a link is clicked to access child sexual abuse material.[282]

There has also been a dramatic increase in the recorded use of cryptocurrencies to purchase child sexual abuse material. The total value of Bitcoin and Ethereum payments to addresses linked to providers of such content was USD 930,000 in 2019 – a 212% increase from 2017.[283] This trend correlates with increased use of commercial hidden services to access content. The proportion of such services has been rising since 2016,[284] and cryptocurrencies are the only payment method they accept.[285]

Commercial sharing can pose unique challenges, as distributors often deploy tactics to frustrate attempts to detect and remove imagery. In 2020, an increase in 'commercial disguised websites' was observed. These websites evade detection by displaying illegal imagery only when the site is accessed by a specific 'digital pathway' of links from other sites. Other commercial sites use techniques including 'top level domain hopping' to survive online after the original site has been taken down. This is when a site modifies its domain while retaining its brand name, so users can still locate it.[286]

More innovation and broader uptake of tools is required to detect material, and curb resharing.

Effective detection of 'known' child sexual abuse material is made possible by two linked techniques called 'hashing' and 'hash-matching'. These techniques have significantly accelerated the identification and removal of child sexual abuse material from the internet.

Hashing and hash-matching

'Hashing' is a process used to transform data of any size into much shorter fixed-length data. The shorter sequence represents the original data and becomes the file's unique signature, or its 'hash value'.

'Hash-matching' is the process by which hashes of known child sexual abuse material held on databases are compared with the 'hash' of newly discovered material to determine if the content has already been reported to authorities. If this is the case, the process for removing the content is generally streamlined, and often automated.[287]

A number of databases exist to facilitate 'hash-matching'. One of the most significant is Interpol's, which houses more than 2.7 million 'hashes' of child sexual abuse material and is used by 64 police forces worldwide.[288] Others include the UK's Child Abuse Image Database, IWF's hash-list, and NCMEC's CyberTipline system.

'Hash-matching' does have some limitations. When 'known' imagery is detected, its removal relies on the identification of the host to issue a take-down notice. Sometimes there are challenges in tracing the location of the hosting server, which can delay removal.[289] In some countries, non-compliance with take-down notices is also an issue.[290] Continued close work between governments, industry and law enforcement across the globe is critical to ensure its continued effectiveness.

Wider uptake of the technology is key to enhancing its impact: although the majority of respondents to an Alliance / Tech Coalition survey confirmed that they use both image (87%) and video (76%) 'hash-matching' to proactively remove child sexual abuse material from their platforms,[291] many organisations still neither contribute 'hashes' to existing databases, nor cross-reference them.[292]

Hash-based detection and removal could be streamlined by merging existing hash-lists. However, this is complicated by national differences in how material is classified. Interpol applies a 'baseline' tag to material that is illegal in all countries, which is used by many of its law enforcement partners.[293] But it is harder to achieve global consensus on classifications for lower severity imagery. More international join-up could improve de-duplication and detection to significantly enhance the overall impact of the technology.[294] [295]

The detection and removal of 'first generation' child sexual abuse material poses a different set of challenges. Solutions exist to detect new content, but they are relatively less mature and more technically complex than 'hash-matching'. So-called content 'classifiers' use algorithms informed by machine learning to identify and categorise child sexual abuse material. Difficulties estimating the ages of children in images[296] and assessing severity mean they tend to generate a higher false positive rate than 'hash-matching' – increasing the need for human moderation.[297] More innovation is required to improve accuracy rates, to reduce the burden on moderators and enable wider uptake of these effective and otherwise safe solutions. Work is also required to explore how both classifiers and 'hash-matching' could work effectively with E2EE.

GOOGLE: CONTENT SAFETY API

The Content Safety API is a tool developed by Google that is provided free to NGOs and private companies to support their work protecting children. It uses artificial intelligence to help organisations better prioritise potentially abusive imagery for human review, where the content is not 'known' child sexual abuse material. Quicker identification of new images increases the speed at which victims of abuse can be identified and safeguarded. Effective prioritisation also reduces the strain on moderators and reviewers.

The tool has already processed more than two billion images, helping companies including Yubo, Plugon and Facebook – and NGOs such as Safernet Brazil – to improve their detection and reporting of child sexual abuse material.

06
Harms

Child 'self-generated' sexual material

The volume of child 'self-generated' sexual material has increased during the COVID-19 pandemic.

Child 'self-generated' material comprises an increasing proportion of child sexual abuse content. It creates complex challenges for policymakers and demands a nuanced response.

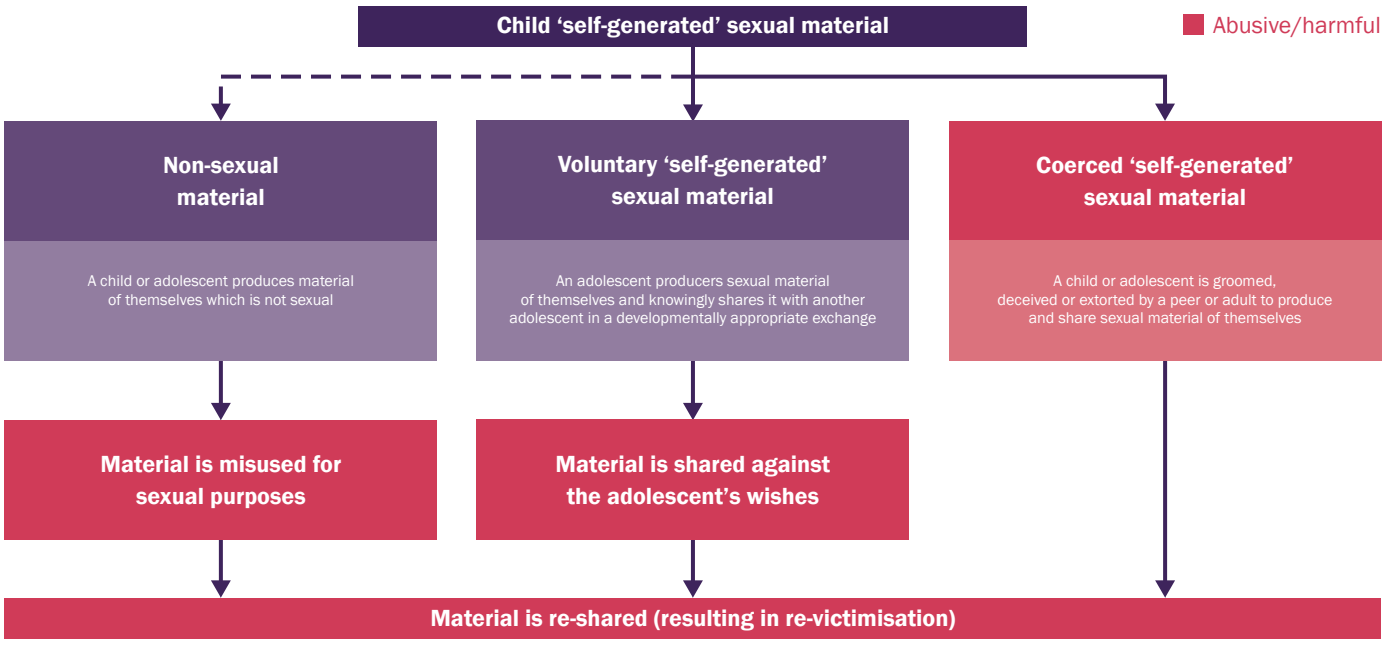
IWF featured a 'snapshot study' of 'self-generated' content in its 2012 Annual Report.[298] In 2017, ECPAT also described it as a "current trend"; attributing the growing volume of 'self-generated' material to the commodified quality of "newly produced, never before seen" imagery, which made it valuable 'currency' for offenders.[299]

Recently the volume of 'self-generated' material has spiked dramatically.

The IWF received 68,000 reports of 'self-generated' sexual material in 2020, a 77% increase from 2019. Overall, 'self-generated' content accounted for 44% of all reports actioned by the IWF in 2020.[300]

This escalation has been partly attributed to the 'perfect storm' created by the COVID-19 pandemic: children spending more time online, and reduced opportunities to commit 'in-person' abuse fuelling online offending and demand for imagery.[301]

Figure 17: Main categories of 'self-generated' sexual material, and associated harms.



Causes of 'self-production' are complex and varied.

There are three broad categories of 'self-generated' material (see Figure 17):

- Non-sexual material is 'self-generated' content that is not sexual in nature but is misappropriated and used in connection with child sexual exploitation and abuse online.[302] Although the victims may be unaware, such material is harmful primarily because it facilitates offender activity. In some cases, direct harm is also caused to victims as a result of offenders manipulating images to appear sexual, and then blackmailing children by threatening to share them.[303]
- Voluntarily 'self-generated' material is usually shared between adolescent peers. This category covers 'self-production' by adolescents only, because younger children cannot consent, and therefore 'self-production' involving them cannot be considered 'voluntary'. In such scenarios, harm is typically caused when imagery is (re)shared against a young person's wishes. Across 39 different studies involving 110,380 participants aged 12 to 17, 12% reported forwarding a 'self-generated' sexual image without consent.[304] The Economist Impact study commissioned alongside this report also found that 29% of respondents reported that someone had shared sexually explicit images and / or videos of them without permission. Harm can also be caused to recipients by the unsolicited sharing of voluntarily 'self-produced' material.[305]
- 'Coerced self-generated' involves the grooming of children to cause the creation of sexual imagery and has been linked to 'capping'.[306] Children involved in 'coerced self-production' may not perceive themselves to be victims, and may potentially view their own actions as voluntary.

The different routes to 'self-production' create a challenge for responders. While the content of the image or video may meet the legal definition of 'child sexual abuse material' – and therefore invoke certain legal processes once discovered – the intent behind the creation or sharing of the images may be unclear. Understanding the context of production and / or sharing is critical to ensure the response can be appropriately tailored; therefore, a case-by-case approach is always required.

INTERNET WATCH FOUNDATION
Sibling 'self-generated' sexual material

The Internet Watch Foundation (IWF) is a child protection organisation that uses technology to find and remove child sexual abuse material from the internet.[307] In 2020, the IWF noted an alarming uptick in the volume of 'self-generated' material discovered online.[308] Within this, analysts observed a particularly disturbing trend of predators tricking children into involving other children in 'self-production'.

Analysis of 'self-generated' sexual images reported to the IWF between September and December 2020 found:

511
images and videos involved siblings

65%
of cases, one or both children engaged in direct sexual contact with the other

46%
of this material was classified as Category A content, depicting the most severe forms of child sexual abuse

In many cases, children had been manipulated or coerced by adults into livestreaming sexual activity and the resulting videos and screenshots were shared across a variety of web platforms. Some adults had posed as children, and occasionally the abuse took the form of a game or 'dare'. The children involved rarely demonstrated any understanding of the sexual nature of what they were being made to do.

While evidence suggests that sharing sexual images is not an uncommon practice for young people (see Figure 18), some children are more likely to be pressured into doing so, which may place them at greater risk of coercion and / or non-consensual sharing.

HAMOGELO:
Maria's Story

Maria* is 15 years old and lives in Greece. She started speaking with Yannis*, a 20-year-old, on a dating platform. She used the platform out of curiosity and boredom: the COVID-19 lockdown restrictions meant she wasn't going to school or partaking in her usual outdoor activities.

Yannis asked her about life during the pandemic, listened to her and seemed to share her feelings. He talked to her every day, and they gradually grew closer.

Yannis eventually coerced Maria into sending 'self-generated' sexual images of herself. He convinced her that it was a step forward in their 'relationship', and that it would be a secret between them. Over time, Yannis began asking her for more, including videos.

Maria tried to refuse but Yannis threatened to publish her photos on social media. Feeling desperate, she searched for help online, and came across Hamogelo's Helpline 1056.

The Helpline provided anonymous support and counselling, and helped Maria talk to her parents about the issue. They contacted the helpline together, and the case was forwarded to the Cyber Crime Division of the Hellenic Police, leading to Yannis eventually being apprehended.

Hamogelo, or 'The Smile of the Child', is a Greek organisation that supports children who face violence, abuse, extortion, poverty and health issues. To date, they have supported more than 1.7 million children and families.

*pseudonyms

A recent survey revealed that Flemish teens identifying as LGBTQ+ were pressured into sharing sexual images more than their heterosexual peers.[309] A study on 'Teens, Sexting and Risks' by UK charity Internet Matters also found that 'vulnerable groups' (children with one or more physical, mental, or social impairments or disabilities) are far more likely to be pressured or blackmailed to share 'nudes'.[310] Sexual harassment in the form of persistent requests for 'self-generated' material is ostensibly not an uncommon experience in some countries. A survey by the UK Office for Standards in Education, Children's Services and Skills (OFSTED) found that of a sample of 900 young people, 80% of girls said they were pressured into sharing sexual images of themselves "a lot" or "sometimes". Other possible contributory causes of 'self-production' include a previous history of abuse, engagement in "more risky online and real-world behaviours", and frequent use of chatrooms.[311] [312]

According to the IWF, girls in early adolescence are far more likely to appear in such imagery: 95% of 'self-produced' sexual content reported to the organisation in 2020 featured girls aged 11-13.[313] However, other studies suggest that an equal or higher proportion of boys are 'self-generating' such content:

- A US survey of 1,000 young people aged 13-17 found that the proportion of boys who had shared their own nudes was one in 10 (for girls the figure was one in five).[314]
- An online survey of 1,001 young people from the UK aged 13-17 found an equal number of boys and girls had taken fully naked pictures of themselves.[315]
- A survey conducted with 500 young people aged 13-24 living in Kathmandu valley, Nepal, found that 18% of boys and 5.2% of girls reported taking naked photos of themselves.[316]

More research is required to understand the role of gender as a risk factor, and how this may differ for the different types of harm linked to child 'self-generated' sexual material (for example, coerced production versus voluntary 'self-production'). Other common risk factors for 'self-production' relate to the characteristics of children's internet usage. Increasing use of mobile devices[317] limits the possibility of parental supervision. Combined with ease of access to adult platforms and content (due to a lack of age verification checks, or checks that are readily bypassed),[318] it is easy to envision how conditions for 'self-production' could arise even in the absence of other risk contributory causes.

'Self-generation' in exchange for payment may increase due to poverty caused by COVID-19.

Commercially motivated 'self-production' is when children create sexual images or videos of themselves in exchange for payment. Reports of commercially motivated 'self-production' are emerging worldwide. In the Philippines, authorities have uncovered instances of teenagers creating groups on social platforms to sell sexual images and videos "to fund expenses in online learning". One such group amassed 7,000 members before it was taken down.[319] In Cambodia, some young people (mostly girls) are using their sexual material to sell cosmetic products online. Surveys conducted with Cambodian youth suggest that such activity can culminate in serious sexual abuse.[320] NCMEC has highlighted cases of missing children later discovered to be selling their sexual material on subscriber platforms, and found evidence of a link to organised exploitation and trafficking.[321]

Regardless of the circumstances, all acts of commercially motivated 'self-production' are almost certainly harmful to the child, and the material produced is most likely illegal. The issue demands an urgent and considered response from policymakers. Netclean's 2020 survey of global law enforcement found that some had already seen a rise in 'self-production' "in exchange for money" during the pandemic, while others predicted a continuation of the trend as conditions of economic hardship worsen, as a way for children "to make money for things they could otherwise not afford".[322]

Harm caused by 'self-generated' material extends to harassment, further sharing and victim-blaming.

The IWF has seen some cases where offenders who view 'self generated' content attempt to identify and track down the victim(s), with the intent of coercing them into creating even more content.[323] In other scenarios, the initial perpetrator(s) may be known; as with 'in-person abuse' they are often "people on whom children rely and depend".[324] Both factors can create a sense of inescapability surrounding the abuse, which is amplified by re-sharing. In 2014, the IWF assessed more than 3,800 'self-generated' sexual images and videos, and found that 90% had been "harvested from the original upload location and were being redistributed on third party websites".[325]

Harm caused by 'self-generated' material is likely to be exacerbated by a tendency towards victim-blaming. According to a survey by Thorn, 60% of children blame the victim when 'self-generated' material is re-shared, while 55% of caregivers also believe the victim is mostly or exclusively to blame for re-sharing.[326] Such attitudes undermine disclosure and reporting by fuelling stigmas that prevent children from coming forward.

Reporting initiatives and technology solutions may curb the rise in 'self-generated' material, but prevention demands a more nuanced approach.

The 'Report Remove' campaign was launched in the UK in 2020 to enable children to anonymously report 'self-generated' material and request for it to be taken down.[327] Such initiatives reduce barriers to disclosure. Device-level controls that prevent children from capturing sexual images and videos may also offer an effective 'stop-gap' to curb the rise in 'self-production'. An example is the 'SafeToWatch' video and image threat detector (see case study overleaf). Such solutions have implications for children's right to privacy, which will need to be carefully considered to support wide uptake and effective deployment.

Long-term sustainable prevention will require considered approaches grounded in the complex experiences of children and young people grappling with self-discovery in the digital age. Given that sharing 'self-produced' sexual images is not uncommon and does not always cause harm, excessive focus on potential negative outcomes risks "providing advice that will be dismissed as it doesn't correspond with the common experiences of young people".[328] Education will be key to protecting children from becoming victims of coercion, and from the potential negative consequences of 'voluntary self-production'. Educational initiatives can also help to promote healthy sexual development and understanding of consent.[329] An example of one such initiative is the NCA's 'Send me a pic' campaign, which aims to promote constructive dialogue with young people around nude image sharing.

SAFETONET: SAFETOWATCH

SafeToNet is a Safety Tech company that deploys artificial intelligence and behavioural analytics to help keep children safe online. SafeToNet believe that child-safe design features should be integrated into technologies at the device and operating system levels.

SafeToNet's latest innovation is SafeToWatch, a video and image threat detector that can disrupt the creation of child sexual abuse material in real-time, and at source. It uses several inputs, such as audio and video, to assess a child's online digital environment, and applies a set of unique algorithms to enable the real-time detection of child sexual abuse material. SafeToWatch functions in the same way regardless of whether the content is being livestreamed by a third party or 'self-generated' by the child themselves. Detection of such images immediately triggers the restriction of cameras and microphones, which can render an app or entire device inoperable and thereby prevent the photo or video being taken. Imagery is not retained, upholding children's right to privacy. Unlike platform-level detection tools, the technology is readily deployable in end-to-end encrypted environments. Critical to the future success of SafeToWatch and similar innovations is reliable access to government and law enforcement data to train algorithms, to optimise the effectiveness of such solutions.

SafeToNet has acquired 77 mobile phone stores in Germany, to bring cyber safety to the high street.[330]

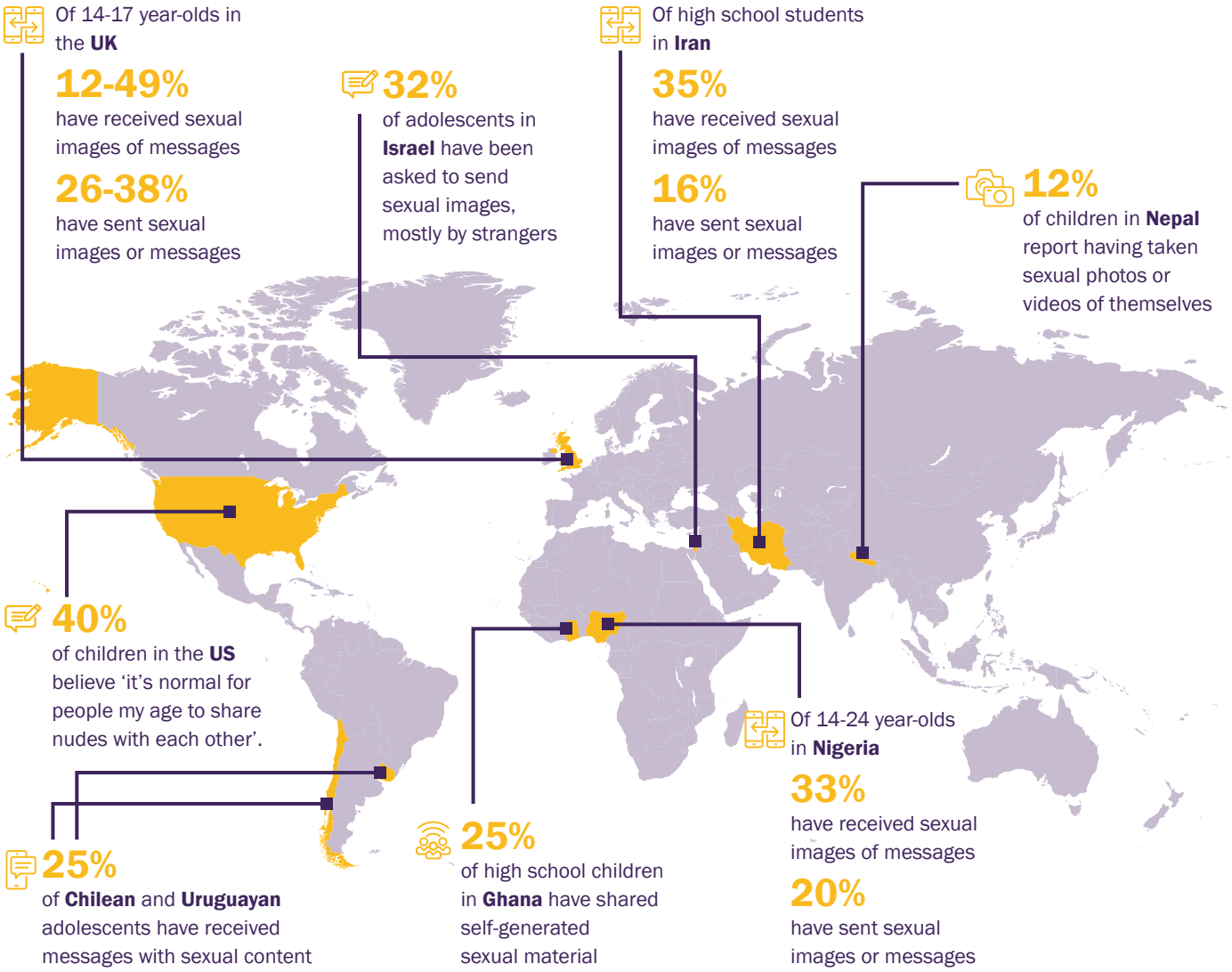
In some countries, changes to legislation would enable a more effective and child-focused response to the issue of voluntarily 'self-produced' sexual material.

Some legal frameworks require urgent reform to prevent the continued criminalisation of children for behaviour that is arguably "part and parcel of the normal discovery of sexuality".[331]

In this vein, parts of Australia have decriminalised 'sexting' between peers.[332] Such approaches are possible under the terms of the Lanzarote Convention, which includes an 'exemption' for criminalising child sexual abuse between children if certain tests are met. This guidance can help nations determine an appropriate response towards children and adolescents involved in generating, viewing or sharing 'self-generated' content.[333] In the UK, the number of young people entering the criminal justice system as a result of 'self-generated' sexual material doubled between 2007 and 2016.[334] The government recently advised education practitioners that "children and young people should not be criminalised for 'sharing nudes and semi-nudes'". [335]

Some young people do cross the line into harmful sexual behaviour and offending. As highlighted by UNICEF, "peers are a significant proportion of those responsible for acts of sexual abuse against other children and adolescents".[336] Such scenarios also expose a gap in the response because "interventions have been mostly designed for adult offenders".[337] Manifesting in many cases as a harm caused by peers, the issue of 'self-generated' sexual material demonstrates the importance of response strategies that can address the needs of children who both experience abuse and engage in harmful sexual behaviour towards their peers.[338]

Figure 18: How common is the sharing of sexual images and messages among young people? [339 340 341 342 343 344 345 346]



06

Harms

Livestreaming child sexual exploitation and abuse

Livestreaming is on the rise, enabled by connectivity and the availability of inexpensive streaming devices.

Livestreaming can involve the 'in-person' abuse of one or more children, transmitted online, or a child / children being forced to 'perform' sexual acts in front of a webcam – usually in exchange for payment.

Livestreaming is on the rise, enabled by connectivity and the availability of inexpensive streaming devices. It often manifests as a cross-border crime that demands a co-ordinated international response.

Unlike 'self-generated' livestreaming (see Harm Chapter: *Child 'self-generated' sexual material*), this type of abuse is normally facilitated by a third party. Although there are cases in which the victim and abusers are in the same locality, most crimes cross national borders. As explained by ECPAT, this type of abuse has "tended to take advantage of economic disparity, with perpetrators from developed countries accessing victims in developing countries".[347] The issue exemplifies the pervasive harm caused by global inequalities in an increasingly connected world.

According to Interpol, livestreaming for payment is increasing.[348] There is evidence to suggest this trend is being exacerbated by the pandemic. In the Philippines, described by UNICEF as the "global epicentre of the live stream sexual abuse trade",[349] a 265% increase in cases was recorded during the quarantine period from March to May 2020. Save the Children has drawn a link with deepening poverty, suggesting that conditions of economic hardship created by COVID-19 are causing more individuals to become involved in livestreaming to make money.[350]

Livestreaming involves a range of offences. Most identified victims are in the Global South but the abuse is happening in many regions of the world.

When livestreaming occurs, the abusers include the individuals who arrange the exploitation, and those who direct and 'consume' the content. Individuals who arrange abuse may be from organised criminal groups, but could equally be part of the victim's circle of trust. Through its analysis of livestreaming cases in the Philippines, IJM reported that the majority of offenders (69%) were financially motivated adult female relatives or close associates of victims.[351] The fact that livestreaming 'facilitators' are primarily financially motivated distinguishes the crime from many other forms of child sexual abuse.

Available data indicates that the individuals who 'consume' livestreamed abuse are predominantly from Europe, North America and Australia.[352] These offenders seek out livestreamed abuse by targeting regions of the world "with high levels of poverty, limited domestic child protection measures and easy access to children".[353] Prosecution of so-called 'demand-side' offenders has tended to focus on the offence of viewing child sexual abuse material, arguably underplaying their overall part in the crime. As the IJM explains, there is a case for processing these individuals as traffickers, because they "abuse their financial power" by 'giving' payments for exploitation, thus fitting the internationally agreed definition of human trafficking as set out in the Palermo Protocol.[354]

The majority of identified livestreaming victims live in South-East Asia, in particular the Philippines,[355] but there are also victims in regions including Europe, Russia and the US.[356] This highlights the importance of avoiding a narrow typification of livestreaming as a crime that only affects children and young people in low-income countries.[357] In addition to causing extensive trauma and suffering for victims, according to a study of cases in South-East Asia, livestreaming can also "be a first step for children to enter 'offline' commercially motivated sexual exploitation".[358]

INTERNATIONAL JUSTICE MISSION: Ruby's Story

At the age of 16, Ruby* was deprived of her freedom and forced to do whatever online offenders asked as they directed the livestreaming of her sexual abuse.

Ruby's ordeal started when a trafficker sent her a private message on social media offering her a staff job in a computer shop, and won her trust by offering free board and lodging while she worked for them. The trafficker and his accomplice also covered Ruby's expenses to travel to them. Ruby soon discovered that the job was not what she had been promised. She wanted to leave but could not do so until she had paid off what had become her travel 'debt'. This became almost impossible due to her 'income' going towards overpriced goods sold to her by her trafficker. At one point she attempted to escape but was threatened with a knife.

Ruby describes the abuse in her own words:

"I'm paid for every disgusting show that I will do in front of the computer camera with the customer. And while doing every disgusting show, I lost every bit of my self-esteem to the point where I felt disgusted with myself as well.

"It's like being trapped in a dark room without any rays of light at all. There's no point in living at all. You do disgusting shows every day, every time, and then after doing that you go to sleep and then repeat the same routine every day and it's like there's no ending at all."

IJM helped Philippine authorities to act on a tip from US Homeland Security Investigations (HSI) to pinpoint Ruby's location and rescue her, along with five other girls. The couple who ran the trafficking operation were later convicted and sentenced, and IJM supported Ruby in her restoration journey. Ruby said of the recovery process: "It wasn't easy at all. It took me years, years to recover from the painful experiences, from the traumatic experiences. You know, at night, when someone suddenly turns off the light, I suddenly get up from my bed and can't sleep without the light on because I was so afraid of the dark. That's where it left me for years."

Today, Ruby is free and safe. She is considering pursuing a law degree with the hope of helping other girls trapped in similar circumstances.

International Justice Mission is an NGO that partners with local justice systems around the world to end violence against people living in poverty. Through its Center to End Online Sexual Exploitation of Children, it strengthens systems to protect children from the production of child sexual abuse material, including via livestreaming.

*a pseudonym

Increasingly blurred boundaries between livestreaming and trafficking will further complicate livestreaming investigations.

Globally, one third of detected trafficking victims are children. Of these, 72% of girls and 23% of boys are trafficked for the purpose of sexual exploitation.[359] Child trafficking often involves forms of online abuse and has been linked to the growth in the volume of child sexual abuse material available. The United Nations Office on Drugs and Crime (UNODC) highlights the case of traffickers in Thailand "sexually exploiting large numbers of children and producing several hundred thousand images for online distribution".[360]

The crossover between livestreaming and trafficking is likely to become increasingly blurred as more traffickers move their business models online to circumvent the impact of COVID-19 restrictions.[361] As highlighted in the 2021 UNODC Global Trafficking Report, the benefit of internet technologies for traffickers is significant, critically: "They allow for exploitation in front of larger audiences than is generally possible with traditional trafficking."[362] There is evidence to suggest livestreaming has increased in popularity through the pandemic as an alternative to in-person child sexual abuse.[363] Arguably, online traffickers will be well positioned to take advantage of this increased demand for 'remote services'.

When livestreaming manifests as part of child trafficking it can create unique challenges that complicate investigations. In the Philippines, UNICEF found that trafficking cases featuring online exploitation "are confused with cybercrime cases" – an issue that can delay referrals.[364] Trafficking victims are also often harder to identify, precisely due to crossover with other forms of abuse.[365]

Globally, one third of detected trafficking victims are children. Of these,

72% OF GIRLS AND 23% OF BOYS

are trafficked for the purpose of sexual exploitation.

More proactive collaboration is needed between police, and online and financial service providers to enhance the detection of livestreamed abuse.

It is technically possible to disrupt livestreaming. As outlined in Harm Chapter: *Sharing and / or storing child sexual abuse materia*l, classifiers do exist to detect child sexual abuse material. However, most livestreamed abuse is transmitted online within private 'conversations' and is therefore not subject to screening or moderator review. Unless an offender records it, the stream usually leaves no trace. The lack of evidence also makes it difficult to prosecute offences – a challenge compounded by the absence of provisions in existing legislation that criminalise the practice.[366] 'Consumers' of livestreamed abuse generally exhibit low technical sophistication (most livestreaming occurs on the surface web),[367] possibly because they perceive the probability of detection and conviction are low.

Monitoring private conversations to detect livestreaming might be considered by some internet users as a justifiable intrusion of privacy. But even if such mechanisms were accepted and implemented by some online service providers, offenders could simply migrate to any one of the increasing number of E2EE platforms. This feature cloaks the content of communications, making the discovery of streams impossible, and thus highlighting the pressing need to diversify disruption methods.

Financial indicators are cited by many as the most effective 'clues' to aid the identification of livestreamed abuse. There is also a history of successful collaboration with the financial sector. A targeted initiative in 2017 achieved the virtual elimination of the use of credit cards in the US for the purchase of child sexual abuse content online.[368] The Australian Transaction Reports and Analysis Centre has also successfully leveraged its public-private partnership the Fintel Alliance to block transactions linked to child exploitation.[369]

Many police agencies and financial service providers already liaise to investigate livestreaming offences. However, there is potential for a more proactive approach. As the IJM explains, while companies "normally oblige" when law enforcement request information, it is more important "that they proactively identify, report and disrupt… money transfers in real-time".[370] The potential for such close collaboration may be complicated by the continued diversification of financial services. More use of cryptocurrencies could also create difficulties, as although it is possible to trace such payments, not all police agencies have the required know- how.[371]

In 2020, the Egmont Group (a consortium of global Financial Intelligence Units) conducted a study into the possible uses of financial intelligence to combat livestreaming. The study highlighted challenges: for example, how it can be difficult to distinguish livestreaming transactions from payment for adult sexual content, scam activity, or other crimes. Overall, it concluded that there is benefit in "combining financial information" with other sources, via data exchange with law enforcement and private sector entities.[372] The project findings demonstrate the importance of a co-ordinated, multi-sector approach to effectively tackle livestreamed abuse. With the appropriate frameworks in place to enable lawful data-sharing, information from online service providers could provide a powerful complement to financial intelligence. This could include, for example, 'signals' (metadata and behavioural indicators) that point to probable nefarious activity by users.

Sustainable livestreaming prevention requires community education and empowerment, police capacity-building, and more consistency in the global approach.

A UNICEF analysis of cases of online child sexual abuse in the Philippines found that livestreaming is in many instances facilitated by the victim's family or community and 'justified' by certain cultural beliefs. For example, the idea that harm is not caused if the child is not touched, as well as the expectation that children should help their families financially.[373] This context complicates safeguarding (as children in such circumstances may not even recognise the abuse), and places a greater burden on overstretched child protection agencies to identify children at risk. Community education and empowerment are critical for sustainable livestreaming prevention, to increase awareness of the damage caused by such abuse, eradicate harmful beliefs, and promote protective practices. Initiatives that give children a voice are also vital, to ensure that they are able to speak up, and seek help.

Currently, there is no internationally agreed definition for the offence of livestreaming child sexual exploitation and abuse. Although in many countries it would fall under existing provisions relating to child sexual exploitation,[374] this creates a barrier to global law enforcement collaboration, and restricts the ability to develop consistent investigative approaches. It also means offenders can potentially escape punishment on the 'double criminality' clause, which states that conduct must be criminalised in both the offender's home country and the country where the offence occurred.[375]

In some countries, investigative limitations also reduce the risk of detection and punishment. For example, in Australia, 90% of successful livestreaming prosecutions rely on the use of covert tactics – but in Cambodia undercover investigations are not permitted by law.[376] In Mexico, efforts to combat the crime are hindered by a lack of subject knowledge on the part of legislators, which prevents holistic consideration of detection and investigation methods.[377]

Currently, there is no internationally agreed definition for the offence of livestreaming child sexual exploitation and abuse.

07

Recommendations

This year's Global Threat Assessment demonstrates that the scale of child sexual exploitation and abuse online continues to grow.

The below recommendations would enable governments, civil society, communities and online service providers to capitalise on positive developments to enhance the threat response, including prevention. These recommendations are aligned to WeProtect Global Alliance's Global Strategic Response framework.[378]

Child sexual exploitation and abuse online is a global issue that demands continued international collaboration and cross-sector dialogue. The Alliance meets this need by facilitating engagement between governments, the private sector and civil society – and generating political commitment and practical approaches to make the digital world safe for children.

To find out more visit: www.weprotect.org

Theme	Recommendation
Funding	**Governments, the private sector and civil society** must commit sufficient funding to tackle the threat of child sexual exploitation and abuse online. Current levels of investment are neither proportionate to the scale and scope of the issue, nor sufficient to deliver the required step change in the global threat response.[379]
Policy / legislation	**Governments** must establish laws that criminalise all offences relating to child sexual exploitation and abuse online, based on approved international frameworks, while seeking to avoid the criminalisation of children themselves. **Governments** must invest in strengthening child protection systems to prevent and respond to the sexual exploitation and abuse of children in all contexts. **Governments** must consider legislative options for strengthening the response to child sexual exploitation and abuse online. Laws should establish standards for industry reporting, the rapid removal of child sexual abuse material, and a basis for the lawful and transparent use of tools to detect child sexual abuse material. International alignment should be sought to enhance global collaboration to combat the threat.

Criminal justice	**Governments** must invest in deterrence and rehabilitation to help those at risk of offending or offenders to change or manage their behaviours. **Governments** must fund specialist law enforcement units to cultivate and maintain threat expertise to improve in-country investigative outcomes. Governments must also invest in building international policing capabilities to strengthen collaboration on cross-border and technologically sophisticated crimes. **Governments** and law enforcement agencies must consult with their international counterparts to develop consistent approaches for investigating cross-border crimes and solving common investigative challenges (for example, gathering evidence dispersed across multiple jurisdictions).
Victim support services and empowerment	To reduce the trauma of repeat victimisation, **policymakers** must work with **industry** to set standards for the timely removal of child sexual abuse material from the internet; reduce image recidivism; and design child-friendly reporting independent of Criminal Justice processes. **Governments** must invest in victim support services and capacity-building for child protection services, to ensure staff are trained in trauma-informed approaches, how to support victims of online abuse, and how to tailor support for children from marginalised groups. **All stakeholders** must consider safe and appropriate engagement with survivors of child sexual abuse to inform the design and evaluation of effective services, policies and support.
Technology	**Online service providers** must take a 'Safety by Design' approach that includes impact assessing all products and services from a child rights perspective. Online service providers should identify and, as appropriate, warn, expel and report actors who pose a risk to children. **Online service providers** should publish regular transparency reports detailing the actions they take to reduce the risk to children online, and the mechanisms used to monitor their effectiveness. **Developers of online safety technologies** should continue working to enhance the accuracy of age estimation tools, classifiers to detect unknown child sexual abuse content (including livestreamed content), and solutions to enable the detection of child sexual abuse online in encrypted environments. Open sourcing (with appropriate controls in place) should be used to encourage collaboration between relevant actors, and help set consistent standards for safety technologies.
Societal	**Governments** must incorporate online safety into school curricula, as a complement to wider programmes that also cover, for example, healthy and harmful sexual behaviours. **All stakeholders involved in the response** – including parents, carers and civil society organisations – must educate communities on the risk and impact of child sexual abuse, and what can be done to prevent it.
Research and insight	**Governments, civil society organisations and online service providers** must invest in research to: • Better understand pathways into offending and, linked to this, the effectiveness of deterrence, self-help and offender management programmes. • Better understand the drivers behind the increase in child 'self-generated' sexual material, and characteristics of adolescent social and sexual development. • Understand the risk and protective factors that may increase or reduce the risk of a child being a victim, including those specific to marginalised groups. • Better understand the extent to which children worldwide are experiencing technology-facilitated child sexual exploitation and abuse. • Evidence how the threat is manifesting in Global South countries (as the evidential picture is currently more developed in respect of the Global North).

08

Acknowledgements

WeProtect Global Alliance would like to thank the following organisations and individuals for their support in the development of the Global Threat Assessment 2021:

STEERING COMMITTEE

Signy Arnason
Canadian Centre for Child Protection

Rinchen Chopel
South Asia Initiative to End Violence Against Children

Sean Coughlan
Human Dignity Foundation

Toby Dagg
INHOPE/Office of the e-Safety Commissioner

Deborah Denis and Donald Findlater
Lucy Faithfull Foundation

Edward Dixon
Rigr AI

Nicole Epps
World Childhood Foundation

Alexandra Evans
TikTok

Guillermo Galarza
International Centre for Missing and Exploited Children

Alexandra Gelber
US Department of Justice

Susie Hargreaves
Internet Watch Foundation

Afrooz Kaviani Johnson
UNICEF

Almudena Lara
Google

Daniela Ligiero
Together for Girls

Remy Malan
Roblox

David Miles
Facebook

Uri Sadeh
Interpol

Michael C. Seto
University of Ottawa Institute of Mental Health Research at the Royal

John Starr and **Melissa Stroebel**
Thorn

Nena Thundu
African Union

*Special thanks also to the **WeProtect Global Alliance Board Members,** and special thanks to **Getty Images.***

OTHER CONTRIBUTORS

Apple
Arpan
Australian Centre to Counter Child Exploitation
Australian Department of Home Affairs
Australian Federal Police
Camera Forensics
ChildSafeNet
Child Rescue Coalition
Crisp
DLT Risk Ltd.
Ethel Quayle
Europol
Global Partnership to End Violence Against Children (End Violence Partnership)
Dr. Hany Farid
Hamogelo
International Justice Mission
LOCATE
Marie Collins Foundation
Microsoft
National Centre for Missing and Exploited Children (US)
National Crime Agency (UK)
Netsweeper
Palantir
Policing Institute for the Eastern Region (UK)
Project VIC International
SafeToNet
SafeBAE
Scotiabank
Sentropy
Stuart Allardyce
Suojellaan Lapsia Ry
Terre des Hommes
The Technology Coalition
UK Home Office
UK Department for Digital, Culture, Media and Sport
Vidintifier
Walk Free
YOTI
ZiuZ Forensic BV

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. This report was researched and written by Chloe Setter, Natalia Greene, Nick Newman and Jack Perry.

09

Glossary of terms

Term	Definition
Child sexual abuse	The involvement of a child (anyone under 18) in sexual activity that he or she does not fully comprehend, is unable to give informed consent to, or for which the child is not developmentally prepared and cannot give consent.[380] This is the definition of child sexual abuse adopted by WeProtect Global Alliance ('the Alliance'), based on World Health Organization (WHO) guidelines.
Child sexual exploitation	A form of child sexual abuse that involves any actual or attempted abuse of position of vulnerability, differential power or trust. This includes, but is not limited to, profiting monetarily, socially or politically from the sexual exploitation of another.[381] This can be perpetrated by individuals or groups of offenders. What distinguishes child sexual exploitation from child sexual abuse is the underlying notion of exchange present in exploitation.[382] There is significant overlap between the two concepts, because exploitation is often a feature of abuse, and vice versa.[383]
Child sexual exploitation and abuse online	Child sexual exploitation and abuse that is partly or entirely facilitated by technology, i.e. the internet or other wireless communications. This concept is also referred to as Online Child Sexual Exploitation and Abuse (OCSEA), and 'technology-facilitated' child sexual exploitation and abuse.
Child sexual abuse material (CSAM)	Any visual or audio content of a sexual nature involving a person under 18 years old,[384] whether real or not real. **Note on alternative terminology:** Some organisations distinguish between child sexual abuse material and child sexual exploitation material (e.g. the Interagency Working Group on the Sexual Exploitation of Children define 'child sexual exploitation material' as a broader category that encompasses both 'material depicting child sexual abuse and other sexualised content depicting children'). 'Child pornography' is also used as an alternative term by some organisations. The Alliance's stated position is to refrain from use of this term: 'Child sexual abuse material' is felt to more accurately capture the heinous nature of sexual violence against children, and to protect the dignity of victims. Some 'self-generated' sexual material would also constitute child sexual abuse material, depending on the circumstances of its production (see Child 'self-generated' sexual material).

Term	Definition
Known child sexual abuse material	Child sexual abuse material that has been previously detected and classified by law enforcement and / or moderators.
'First generation' child sexual abuse material	Child sexual abuse material that has not previously been detected and classified by law enforcement and / or moderators.
Non-photographic child sexual abuse material	This includes computer-generated images cartoons, or drawings which graphically depict children in a sexually abusive way. [385] [386]
Sexualised material of children	Material that does not represent the sexual abuse of a child, but which is used for sexual purposes. An example might be a video of children doing gymnastics, which is inappropriately viewed for sexual gratification. Sexualisation is not always an objective criterion, and the crucial element in judging such a situation is the intent of a person to sexualise a child in an image or to make use of an image for sexual purposes.
Producing child sexual abuse material	Creating child sexual abuse material by in-person photography /video / audio recording, creating textual content or non-photographic (e.g. computer-generated) visual material, or manipulating existing child sexual abuse material to create new unique imagery.
Searching for and / or viewing child sexual Abuse material	Seeking child sexual abuse material on the internet and viewing or attempting to view it.
Sharing and / or storing child sexual abuse material	Downloading, storing, hosting, uploading and / or sharing child sexual abuse material.

Term	Definition
Grooming children online for the purpose of sexual exploitation and abuse	An individual builds a relationship, trust and emotional connection with a child or young person in order to manipulate, exploit and abuse them (facilitated, partly or entirely, by the internet or other wireless communications).[388] There is not always an intent to meet in person. Note on Alternative Terminology: Some organisations use the term 'online enticement' (as defined by NCMEC[389]) when referring to this concept.
Child 'self-generated' sexual material	Content of a sexual nature, including nude or partially nude images and video, that has been produced by children of themselves. Child 'self-generated' sexual material is not a harm per se (it can be produced voluntarily and shared as part of a developmentally appropriate exchange, e.g. between adolescents), but there are production scenarios in which harm is caused, primarily: • When a child or adolescent is coerced into producing 'self-generated' sexual material • When voluntarily 'self-generated' sexual material is shared against an adolescent's wishes This report is focused on examining the characteristics and boundaries of harmful 'self-production'. This phrase appears in quotation marks throughout the report to avoid any implication of willingness on the part of the child or young person involved. While the content may meet the definition of child sexual abuse material, the intent is likely to be unclear and therefore cannot be taken for granted in any circumstances.
Livestreaming child sexual exploitation and abuse	Transmitting child sexual abuse and exploitation in real-time over the internet.
Computer-Generated Imagery (CGI)	In the context of child sexual abuse and exploitation, this refers to wholly or partly artificially or digitally created sexualised images of children.[390]
'Deepfake'	A form of CGI that uses artificial intelligence to replace one person's likeness with another in photos or recorded video.[391]
'Capping'	Offenders capturing footage of livestreamed child sexual abuse and exploitation.[392] Capping may also include offenders capturing innocuous imagery of children and using it for sexual purposes (this imagery would then constitute sexualised images of children).
'Gamification' of abuse	The application of game-like elements (e.g. point scoring, competition with others, rules of play) to encourage participation in abuse and exploitation.

Term	Definition
Child displaying harmful sexual behaviour	A child or young person under the age of 18 years old exhibiting behaviours that are developmentally inappropriate, may be harmful towards themselves or others and / or abusive towards another child, young person or adult.[393]
Risk factors	Factors at the individual, relationship, community, and societal level that may make a child more likely to experience sexual abuse and exploitation.
Protective factors	Factors at the individual, relationship, community, and societal level that may reduce the risk of a child being a victim of sexual abuse and exploitation.
Re-victimisation	When a victim faces any sexual abuse or assault subsequent to a first abuse or assault.[394] This includes the further distribution and viewing of imagery on the internet: a single image of a victim can be shared hundreds or thousands of times.[395] Re-victimisation may be caused by the same or a different offender to the initial victimisation.
Child trafficking	The recruitment, transportation, transfer, harbouring or receipt of a child for the purpose of exploitation.[396]
Global North	The G8 countries, the United States, Canada, all member states of the European Union, Israel, Japan, Singapore, South Korea, Australia, New Zealand and four of the five permanent members of the United Nations Security Council, excluding China.[397]
Global South	Africa, Latin America, the Middle East and developing Asia. This includes three of the four newly advanced economies of the BRIC countries (excluding Russia), which are Brazil, India and China.[398]
Surface web	The portion of the web readily available to the general public and searchable with standard web search engines.[399]
Deep web	The portion of the web whose contents are not indexed by standard web search engines, and includes many common uses such as webmail, online banking, and subscription services. Content can be located and accessed by a direct link or IP address, and may require a password or other security access beyond the public webpage.[400]
Dark web	The layer of information and pages that you can only get access to through so-called 'overlay networks' (such as Virtual Private Networks (VPN) and peer-to-peer (P2P) file sharing networks), that obscure public access. Users need special software to access the dark web because a lot of it is encrypted, and most dark web pages are hosted anonymously.[401]

Term	Definition
Safety Technology (Safety Tech)	Solutions to facilitate safer online experiences, and to protect users from harmful content, contact or conduct.[402]
Safety-by-design	The embedding of the rights and safety of users into the design and functionality of online products and services from the outset.[403]
Peer-to-peer (P2P)	In a P2P network, the "peers" are computer systems which are connected to each other via the internet. Files can be shared directly between systems on the network without the need of a central server. In other words, each computer on a P2P network becomes a file server as well as a client.[404]
Virtual Private Network (VPN)	An arrangement that creates an encrypted connection over the Internet from a device to a network, known as a tunnel.[405]
Hashing	A process whereby a binary hash is created by a mathematical algorithm that transforms data of any size into much shorter fixed-length data. This shorter sequence represents the original data and becomes this file's unique signature, or its hash value – often called its digital fingerprint.[406]
Hash-matching	A process of using databases of hashed child sexual abuse material to detect when the material is re-shared, by matching its hash value against those of already known files.[407]
Artificial Intelligence (AI) classification or AI moderation	Automated or partly-automated moderation systems that identify harmful content by following rules and interpreting many different examples of content which is and is not harmful.[408]
Encryption	The process of encoding information into an alternative form that can only be decrypted by authorised individuals who possess the decryption key.[409]
End-to-end Encryption	A form of encryption wherein the content of each message is visible only to the sender and recipient. Unscrambling the message requires a private decryption key exchanged between correspondents, so that while the message may be intercepted, it cannot be viewed or monitored by the service provider, law enforcement or any other third party.[410]
'Hidden services'	Websites that are hosted within a proxy network (such as Tor), so their location can't be traced.[411]
Metadata	Data that describes other data.[412] Examples of metadata would include the time and duration of a phone-call (as opposed to the content of the communication itself).
Tor	An open source privacy network that permits users to browse the web anonymously. The system uses a series of layered nodes to hide web address, online data, and browsing history.[413]

Term	Definition
Secure tooling	Software / applications used to aid anonymity online by hiding user location and identity.
Secure Operating Systems	The use of operating systems that can be booted from a USB. Because they do not write to the hard drive, once shut down everything is deleted. Encryption software can then be used to protect the contents of a file and parts of the drive, which can only be accessed with the user's decryption key.
Tradecraft	An ever-evolving host of cloaking techniques and evasion strategies offenders use to avoid individual detection, and their techniques and strategies for identifying and engaging children.
Virtualising & emulation	Virtual machines allow users to run an operating system that behaves like a full, separate computer in an app window on their desktop. Some emulators can create a virtual smartphone interface on a computer. This allows the user to install and use apps on their computer that would otherwise not be available. Emulators are often used in conjunction with 'capping' tools, as they can prevent a 'screenshot' notification from being sent to the victim, and the offender can use 'capping' software installed on their computer to capture clearer images.
UN Convention on the Rights of the Child	An international human rights treaty comprising 54 articles that cover all aspects of a child's life and set out the civil, political, economic, social and cultural rights that all children everywhere are entitled to. It also explains how adults and governments must work together to make sure all children can enjoy all their rights.[414] [415]
UN Committee on the Rights of the Child General Comment 25	Authoritative guidance that sets out how children's rights apply in the digital environment. It helps states understand what steps are necessary to respect, protect and fulfil children's rights in the digital environment.[416]
Voluntary Principles to Combat Child Sexual Exploitation and Abuse	A set of principles aiming to provide a framework to combat child sexual exploitation and abuse online and intended to drive collective action. They were developed by five Governments (Australia, Canada, New Zealand, UK and US), in consultation with a wide range of stakeholders including a leading group of industry representatives.[417]
WeProtect Global Alliance Model National Response (MNR)	A framework providing guidance and support on the MNR to countries and organisations to help them deliver on it. The Model is focused on helping countries to build their response to child sexual exploitation online.[418]
WeProtect Global Alliance Global Strategic Response (GSR)	A framework providing guidance and support on the GSR to countries and organisations to help them deliver on it. The Model is focused on enhancing global collaboration on the response to child sexual exploitation online.
Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (also known as the 'Lanzarote Convention')	A convention that requires criminalisation of all kinds of sexual offences against children. It sets out that states in Europe and beyond shall adopt specific legislation and take measures to prevent sexual violence, to protect child victims and to prosecute perpetrators. The 'Lanzarote Committee' is the body established to monitor whether Parties effectively implement the Lanzarote Convention and with identifying good practice.[419]
European e-Privacy Directive	Legislation that concerns the processing of personal data and the protection of privacy in the electronic communications sector.[420] The Directive does not contain an explicit legal basis to continue current voluntary practices to detect, report and remove child sexual abuse.[421]

10

Annex A:

Findings from WeProtect Global Alliance / Technology Coalition survey of technology companies

SUMMARY OF FINDINGS

Many of the companies surveyed have capabilities to detect child sexual abuse and exploitation online, and reporting mechanisms, but there are opportunities to enhance collaboration and focus more on deterrence and prevention.

	Reporting	Detection	Deterrence and prevention	Tool development	Transparency reporting
Key findings	Most reports are at least partly automated, and almost all companies have some form of reporting mechanism	The majority of companies are using hash-based tools to detect both image and video child sexual abuse materia. Use of advanced classifiers to detect video and livestream content, is less common despite the fact this category is becoming more prevelent	Prevention measures such as deterrence messaging and child safety resources are widely provided, but these are less common than use of hash-based detection, despite their potential to prevent abuse before it occurs	Many companies use tools developed by others, but it is less common for them to develop tools in-house and share them	Most companies do not yet publish transparency reports. However, of companies that do, a large majority publish specific data on child sexual abuse and exploitation
Recommendations	Diversify reporting pathways to gain a more holistic picture of the threat	Share information and intelligence (e.g. hashes and keywords) to help stay ahead of what is a rapidly evolving space	Invest in deterrence and prevention measures, and diversify the targeting of online safety resources to avoid over-realiance on one group, to help prevent abuse before it occurs	Collaborate and share tools across indrustry to help maximise thier benefit. Ensure regulatory frameworks empower rather than hinder companies utilising key tools	Develop universal reporting frames to ensure data is consistent and encourage more companies to make it publicly available

METHODOLOGY

Between February and March 2021, WeProtect Global Alliance and the Technology Coalition carried out a 20-question survey of their respective industry members to understand the scope of activities undertaken by technology companies to combat the issue of child sexual abuse online. In total 32 companies responded, ranging in size from less than 250 employees to more than 5,000.

LIMITATIONS

The sample is small relative to the size of the global technology sector, and is more representative of Global North-based companies. However, the wide range of company sizes and types arguably provide a representative sample of the industry. Due to the survey being fully anonymised and aggregated, it was not possible to trace one respondent's answers to multiple questions, limiting potential comparisons between responses – for example, for different company sizes. Finally, some of the questions may not have been relevant to all respondents. This was mitigated by including a 'not relevant' option or allowing for questions to be skipped.

FULL RESULTS

Reporting:

84% of companies surveyed have at least partly automated processes for forwarding reports of child sexual abuse online, suggesting that report management is relatively efficient.

This question did not focus on proactive detection mechanisms companies may have in place, so does not provide a full picture in this regard. However, outside of this the most popular reporting mechanism for companies is direct user reports. Least popular are reporting paths for NGOs and law enforcement, suggesting that there may be scope for greater cross-sector collaboration. Diversifying reporting pathways will also avoid over-reliance on user reporting which, given that rates of self-reporting are low, may help to provide a more complete picture of offending.

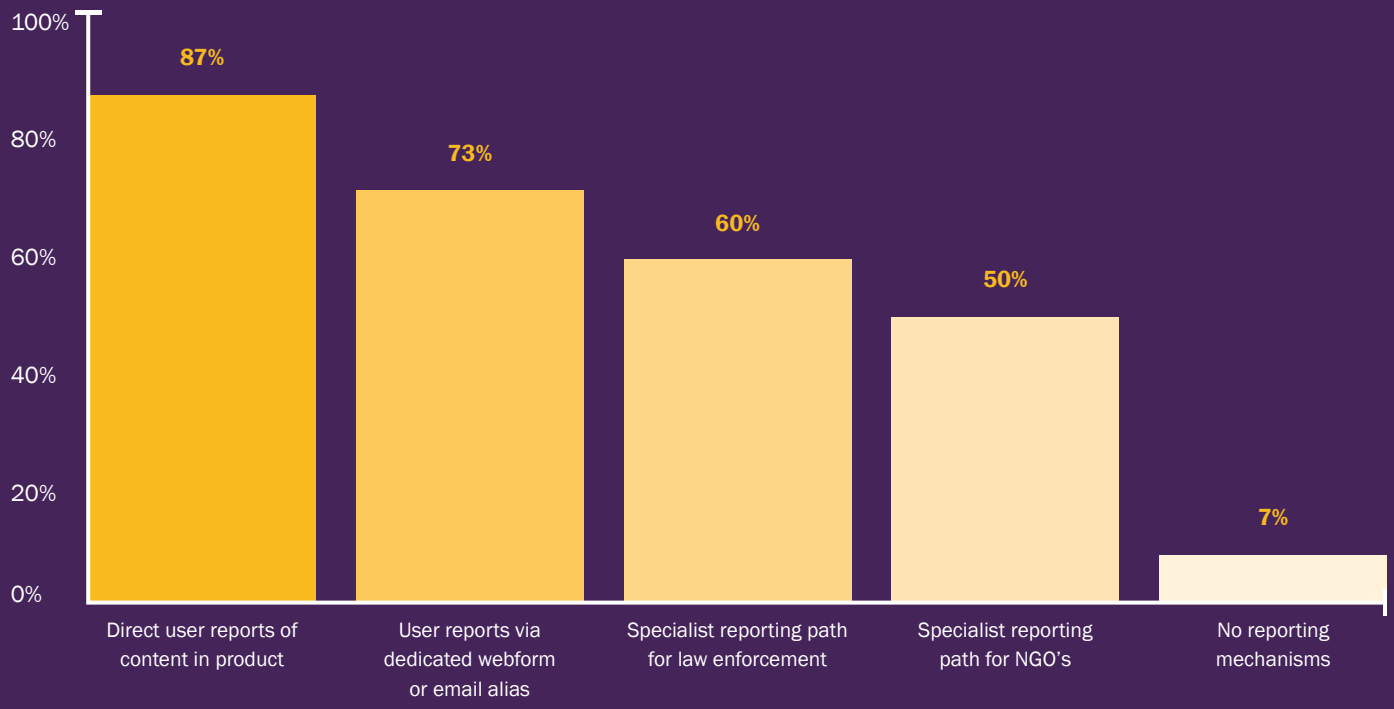
REPORT HANDLING

84%

PARTLY OR FULLY AUTOMATED

Figure 19: Mechanisms companies provide to enable reporting.

What mechanisms do companies provide to enable reporting of child sexual abuse material?

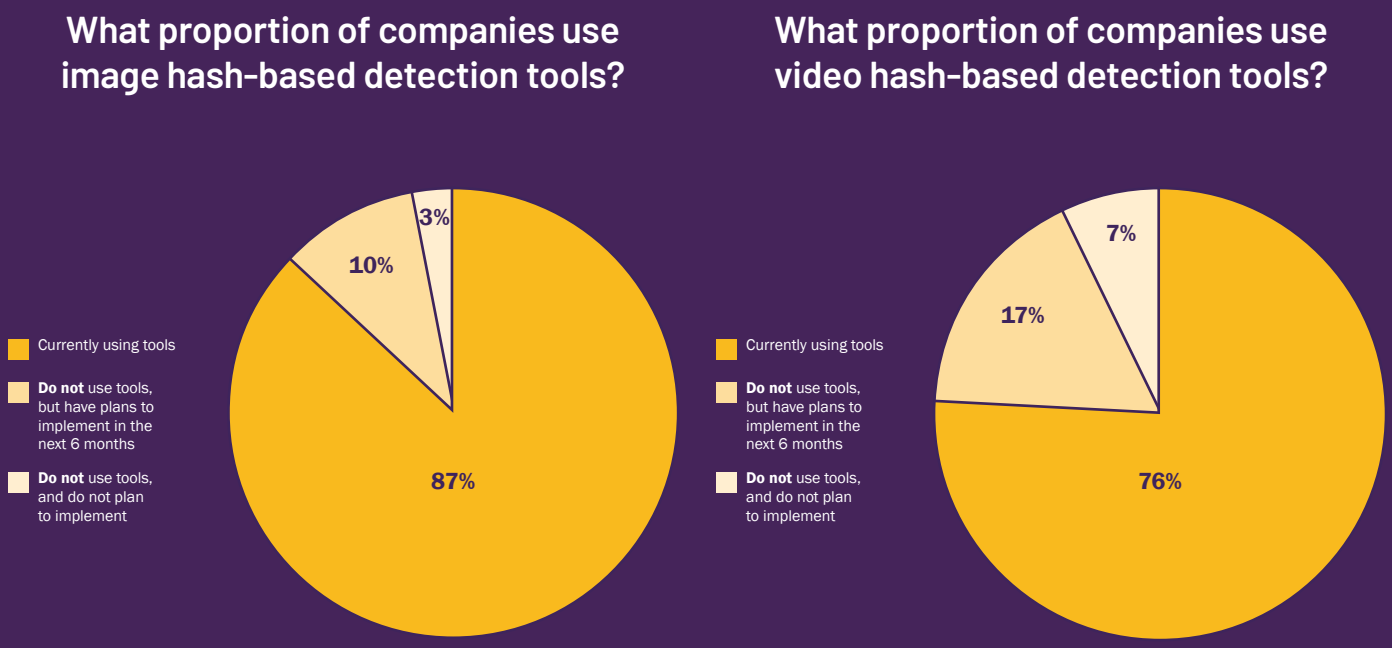


DETECTION

Hash-based Detection

Most respondents use hash-based tools to detect image and video-based child sexual abuse material on their platforms. Most of those not already using hash-based tools plan to implement them in the next six months, as shown in Figure 20 below.

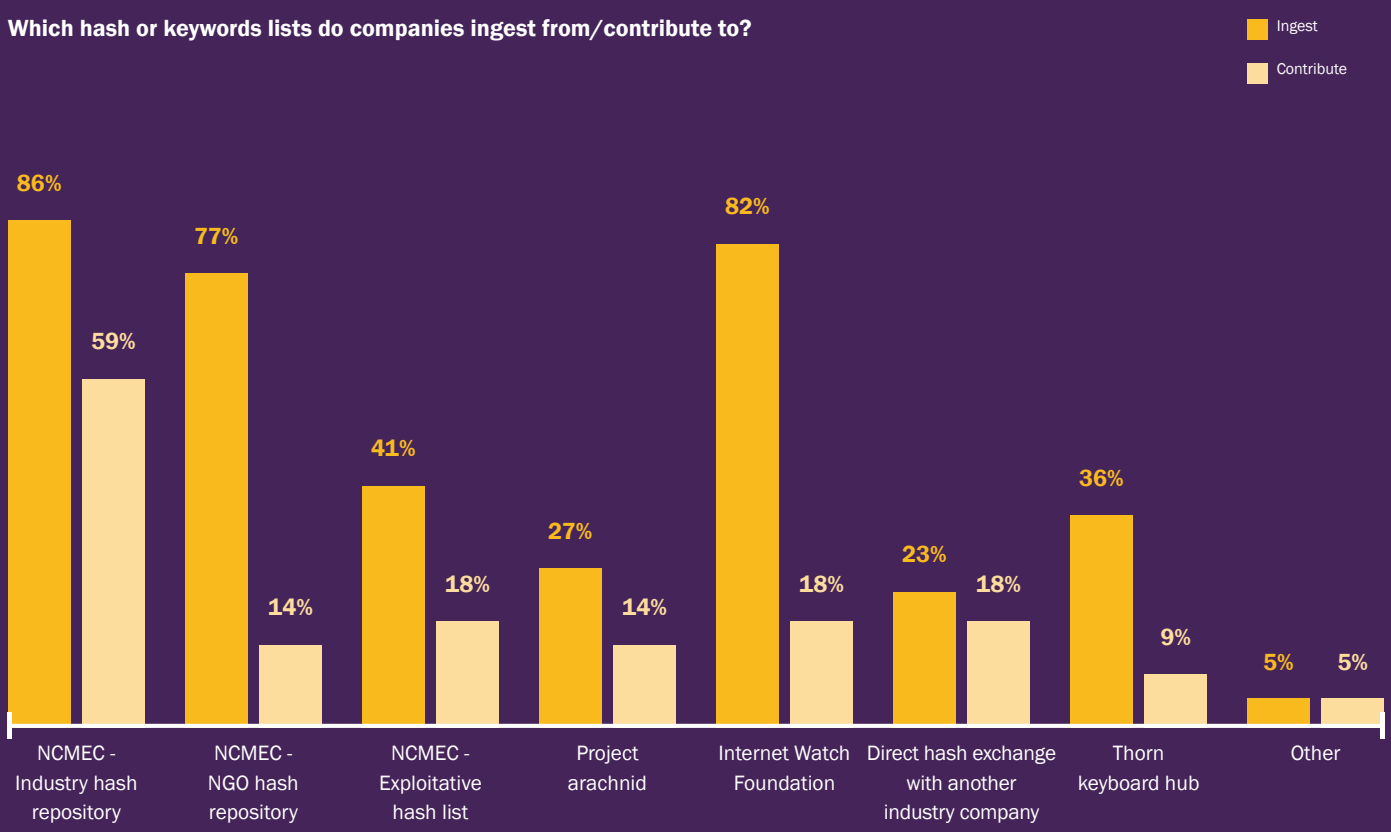
Figure 20: Company use of hash-based detection tools.



To effectively use hash-based detection tools, companies need access to hashes of known child sexual abuse material. Another important element of detection is the ability to block search terms relating to child sexual abuse, for which companies need access to keyword lists.

Most companies ingest hashes and keywords from at least one repository, as shown in Figure 21 below. However, a much smaller proportion contribute hashes or keywords. Assuming companies are not purely detecting known content, limited external intelligence sharing may impact the ability to keep up with the evolving threat.

Figure 21: Company use of hash/keyword lists.

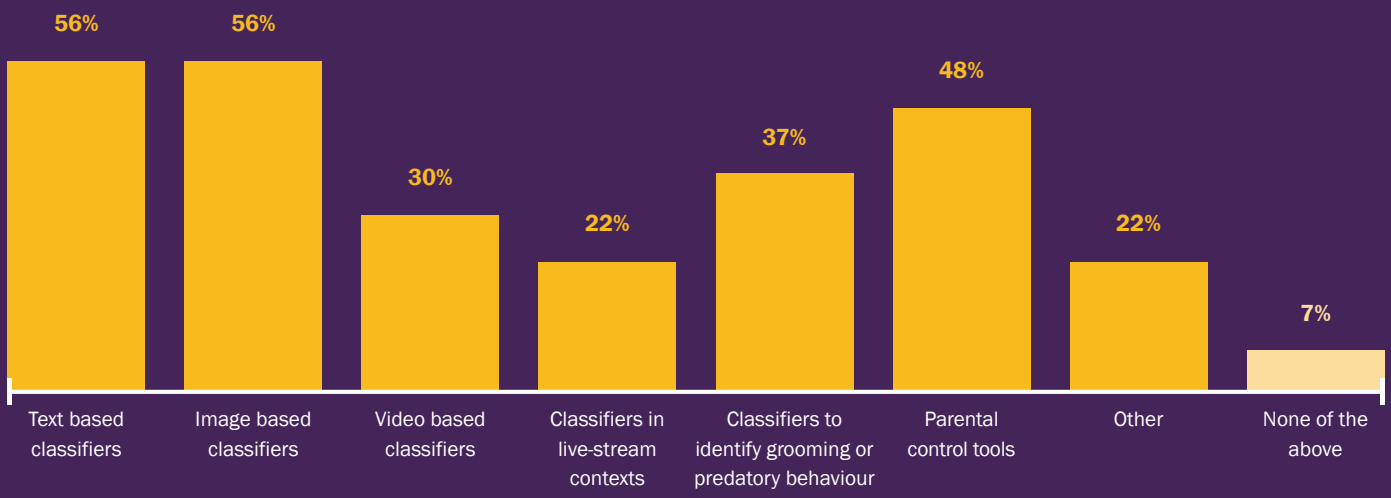


ADVANCED DETECTION:

Advanced detection refers to technologies such as artificial intelligence classifiers. These advanced detection measures are less commonly used than hash-based detection measures. Despite evidence indicating the increasing prevalence of video and livestreaming content, classifiers to detect such material are only used by 30% and 22% of respondents respectively.

Figure 22: Additional measures to combat child sexual exploitation and abuse online.

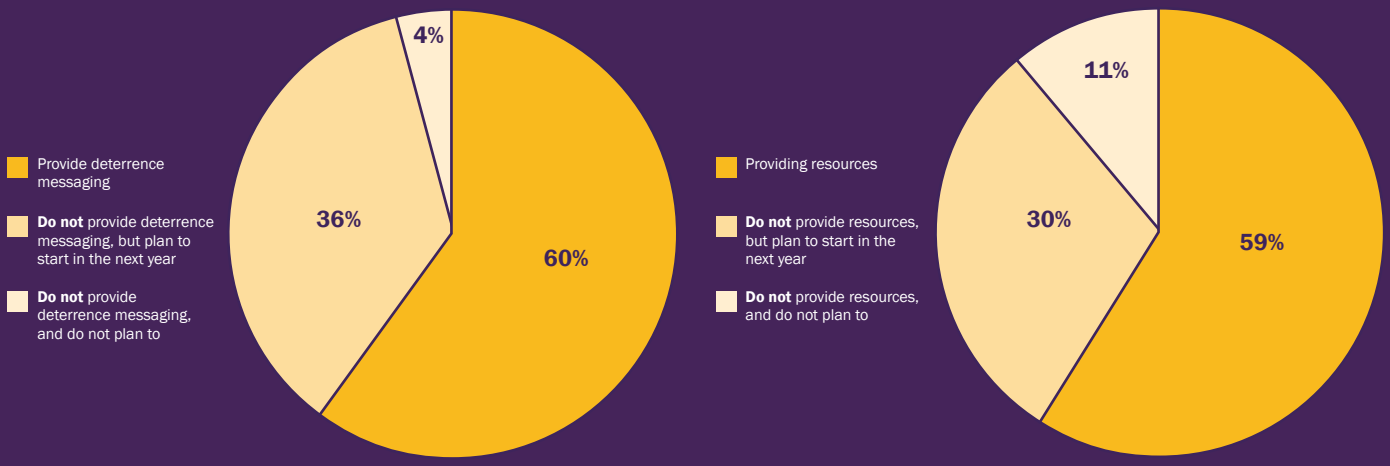
What additional measures do companies use to combat child sexual exploitation and abuse online?



DETERRENCE AND PREVENTION:

Most respondents issue deterrence messaging to potential offenders and provide online child safety resources to help prevent abuse before it occurs, but both are less common than mechanisms to detect child sexual abuse material.

Figure 23: Company use of deterrence messaging and online child safety resources.



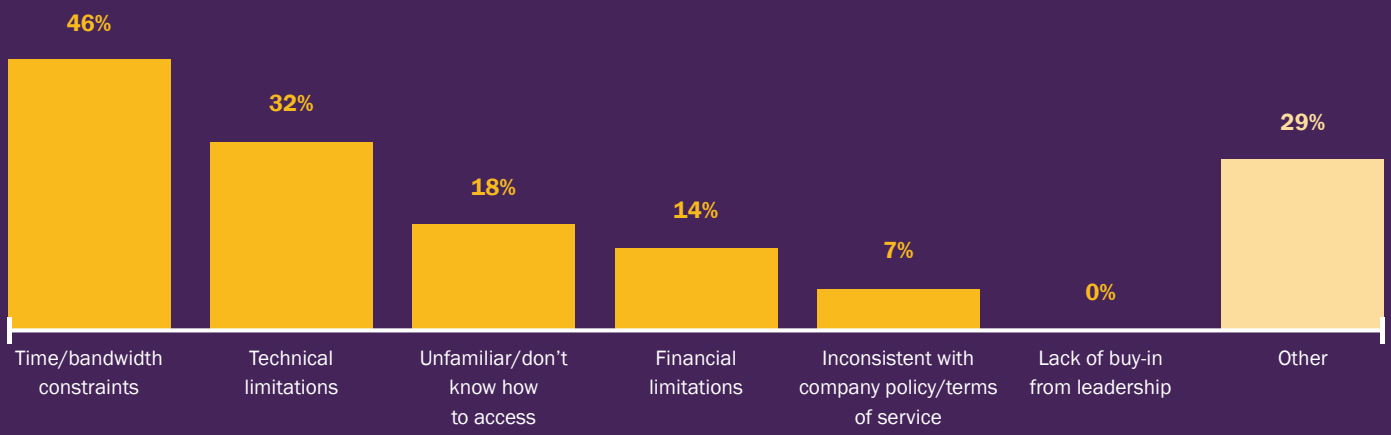
The survey found that most online child safety resources are targeted at parents, which is positive given they are generally the first point of contact for a child experiencing distress online.[422] However, there is also evidence to suggest that child sexual exploitation and abuse is often perpetrated by family members.[423] To support such victims and avoid over-reliance on one group to safeguard children, there is scope to provide more resources for children themselves, educators and other audiences.

TOOL DEVELOPMENT:

Almost 50% of respondents use content classifiers developed by other companies, but only 26% make accessible to others the tools they develop themselves. Further investigation would be required to understand the reasons for this. More collaboration and sharing of tools where possible could arguably help to maximise the benefit of tools overall.

Figure 24: Barriers to use of tools for combatting child sexual abuse online.

What barriers do companies face to using technical resources to combat child sexual exploitation and abuse online?



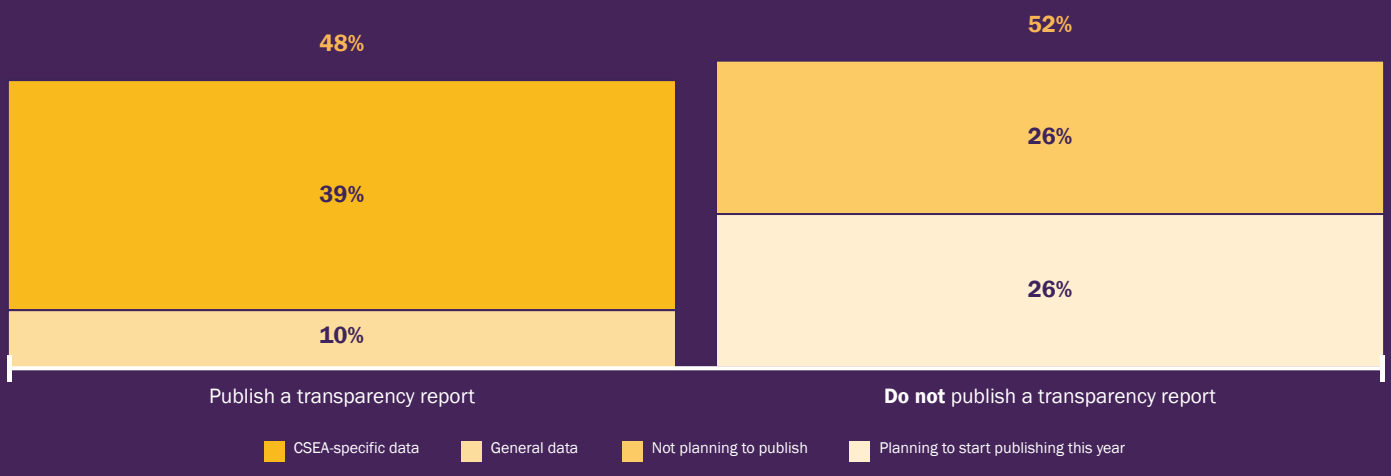
Time and bandwidth constraints are the primary barrier to companies developing and deploying tools to combat child sexual abuse online. A lack of buy-in from leadership was not cited as a challenge by any respondents.

TRANSPARENCY:

A culture of transparency is crucial to enable a joined-up and informed response to child sexual exploitation and abuse online. However, only 49% of respondents regularly publish a transparency report. Of these, 80% publish specific data on child sexual exploitation and abuse, which is critical to understanding the scale and scope of the threat.

Figure 25: Company transparency reporting.

What proportion of companies publish regular transparency reports on child sexual exploitation and abuse on their platform?



The data reported by companies can be very varied as shown in Figure 26 below. More work is needed to develop universal reporting frameworks. This would ensure data is consistent and comparable, and encourage companies that do not yet publish data to make it publicly available.

Figure 26: Data types included in transparency reports.

Of companies that publish a transparency report, what type of data relating to child sexual exploitation and abuseonline do they include?

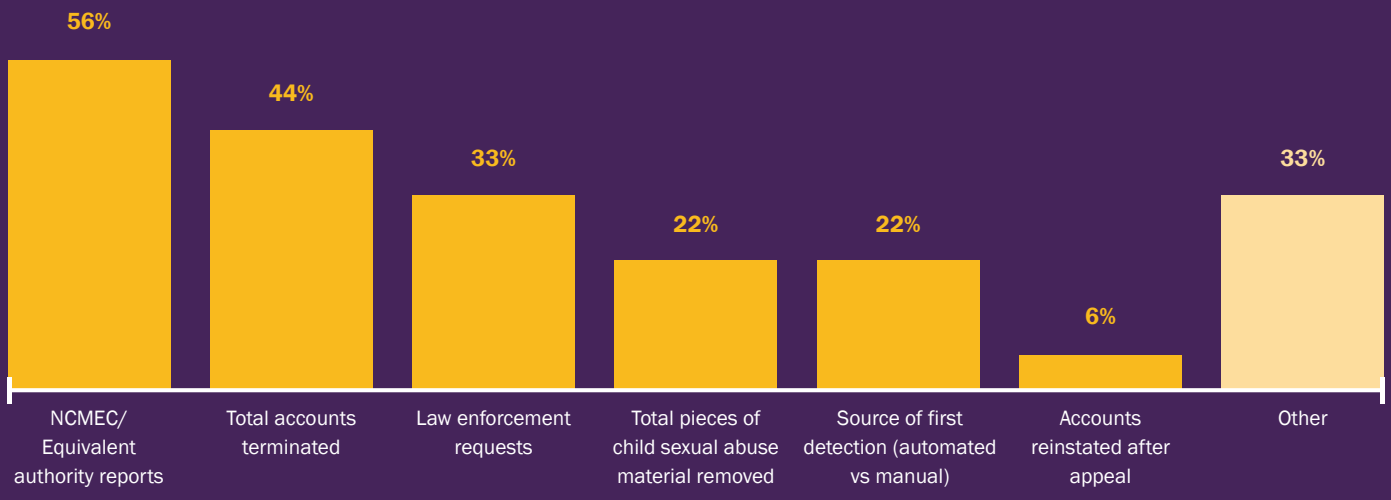


Figure 26 shows it is common for companies to report aggregate data, such as total pieces of child sexual abuse material removed. However, data in transparency reports is rarely broken down to show the prevalence of different types of child sexual abuse, such as grooming or livestreaming. Reporting on these figures would provide greater insight into where different harms are proliferating, with a view to targeting specific interventions where they are most needed.

11

References

1 Annual Report 2020 (INHOPE, 2021) Accessed from: https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf 06/05/2021

2 4 arrested in takedown of dark web child abuse platform with some half a million users (Europol, 2021) Accessed from: https://www.europol.europa.eu/newsroom/news/4-arrested-in-takedown-of-dark-web-child-abuse-platform-some-half-million-users 04/05/2021

3 NetClean Report COVID-19 Impact 2020 (NetClean, 2020) Accessed from: https://www.netclean.com/netclean-report-2020/# 04/05/2021

4 Fighting Child Exploitation with Big Data (Freethink, 2020) Accessed from: https://www.freethink.com/videos/child-exploitation 16/06/2021

5 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: https://www.ijmuk.org/images/EMBARGO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf 15/02/2021

6 Online child sexual abuse activity has increased (NetClean, 2021) Accessed from: https://www.netclean.com/netclean-report-2020/insight-2/ 26/01/2021

7 Online enticement reports skyrocket in 2020 (NCMEC, 2021) Accessed from: https://www.missingkids.org/blog/2021/online-enticement-reports-skyrocket-in-2020 24/02/2021

8 IWF Annual Report: 2020 Trends and Data (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends 22/04/2021

9 Research report: The impact of COVID-19 on the risk of online child sexual exploitation and the implications for child protection and policing (University of New South Wales, Sydney, 2021) Accessed from: https://www.arts.unsw.edu.au/sites/default/files/documents/eSafety-OCSE-pandemic-report-salter-and wong.pdf?utm_source=ActiveCampaign&utm_medium=email&utm_content=New+briefings+and+reports+-from+the+Alliance+and+our+members&utm_campaign=-May+2021+newsletter 07/06/2021

10 COVID-19: Child sexual exploitation and abuse threats and trends (Interpol, 2020) Accessed from: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse 26/01/2021

11 By the Numbers (NCMEC, 2021) Accessed from: https://www.missingkids.org/gethelpnow/cybertipline 16/06/2021

12 IWF Annual Report: Self-generated child sexual abuse (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/selfgenerated 06/05/2021

13 Acion to end Child Sexual Abuse and Exploitation (UNICEF, 2020) Accessed from: https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf 23/07/2021

14 Survey of Technology Companies (WeProtect Global Alliance and Technology Coalition, 2021) See Annex A: Findings from WeProtect Global Alliance/Technology Coalition Survey of Technology Companies

15 IWF Annual Report: Hidden Services (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/Trends/International/Other/Hidden 22/04

16 PA Consulting engagement with Australian Centre to Counter Child Exploitation, 01/03/2021

17 Violencia sexual a menores ya deja mas de mil victimas en lo corrido de 2021 (LAFM, 2021) Accessed from: https://www.lafm.com.co/colombia/violencia-sexual-menores-ya-deja-mas-de-mil-victimas-en-lo-corrido-de-2021 11/03/2021

18 Abuso sexual en internet y redes de trata (Infobae, 2020) Accessed from: https://www.infobae.com/america/mexico/2020/07/27/abuso-sexual-en-internet-y-redes-de-trata-los-crimenes-contra-la-ninez-que-aumentaron-durante-la-pandemia/ 25/02/2021

19 Production and distribution of child sexual abuse material by parental figures (Australian Institute of Criminology, 2021) Accessed from: https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf 09/03/2021

20 Los casos de abuso sexual contra menores en espana se multiplican por 4 en la ultima decada (Levante, 2021) Accessed from: https://protect-eu.mimecast.com/s/WuEPCWnWgFxLBY3Hxchqm?domain=levante-emv.com 23/02/2021

21 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: https://www.ijmuk.org/images/EMBARGO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf 15/02/2021

22 A Global Strategic Response to Online Child Sexual Exploitation and Abuse (WeProtect Global Alliance, 2021) Accessed from: https://www.weprotect.org/wp-content/uploads/WeProtectGA-Global-Strategic-Response-EN.pdf 17/06/2021

23 Action to end Child Sexual Abuse and Exploitation (UNICEF/ End Violence Against Children, 2020) Accessed from https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf 13/05/2021

24 Guidelines for Medico-Legal Care for Victims of Sexual Violence: Child Sexual Abuse (World Health Organisation, 2003) Accessed from: https://www.who.int/violence_injury_prevention/publications/violence/med_leg_guidelines/en/ 19/04/2021

25 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf 25/05/2021

26 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Interagency Working Group on Sexual Exploitation of Children, 2016) Accessed from: https://www.ecpat.org/wp-content/uploads/2016/12/Terminology-guidelines_ENG.pdf (23/07/2021)

27 Global Threat Assessment 2019 (WeProtect Global Alliance, 2019) Accessed from: https://www.weprotect.org/issue/global-threat-assessment/ 26/01/2021

28 Grooming (NSPCC) Accessed from: https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/ 25/05/2021

29 Online Enticement (NCMEC) Accessed from: https://www.missingkids.org/netsmartz/topics/onlineenticement 25/05/2021

30 Netclean Annual Report; Comment to insight 4 – Simon Bailey (Netclean, 2020) Accessed from: https://www.netclean.com/netclean-report-2020/insight-6/ 17/06/2021

31 Netclean Annual Report; Insight 2: Online Child Sexual Abuse Activity has increased (Netclean, 2020) Accessed from: https://www.netclean.com/netclean-report-2020/insight-2/ 07/06/2021

32 Netclean Annual Report; Comment to insight 4 – Rob Jones (Netclean, 2020) Accessed from: https://www.netclean.com/netclean-report-2020/insight-6/ 17/06/2021

33 Impact of coronavirus disease on different manifestations of sale and sexual exploitation of children (United Nations, 2021) Accessed from: https://reliefweb.int/sites/reliefweb.int/files/resources/A_HRC_46_31_E.pdf 07/06/2021

34 Protection of children should always trump protection of privacy (eSafety Commissioner, 2020) Accessed from: https://www.esafety.gov.au/about-us/blog/protecting-children-should-always-trump-protecting-privacy 07/06/2021

35 Abuso sexual infantil crece en un 50% durante la pandemia por coronavirus (El Imparcial, 2021) Accessed from: https://www.elimparcial.com/mundo/Abuso-sexual-infantil-crece-en-un-50-durante-la-pandemia-por-coronavirus-20210216-0011.html 07/06/2021

36 Online sexual abuse of children rising amid COVID 19 pandemic – Save the Children Philippines (Relief Web, 2021) Accessed from: https://reliefweb.int/report/philippines/online-sexual-abuse-children-rising-amid-covid-19-pandemic-save-children 22/04/2021

37 La pornografia infantile crecio 117% en Mexico (Jornada, 2020) Accessed from: https://www.jornada.com.mx/2020/08/10/politica/010n1pol 07/06/2021

38 Ending Violence Against Children and COVID-19 (Child Rights Now!, 2020) Accessed from: https://www.wvi.org/sites/default/files/2020-07/2020_06_JF_CRN_Ending%20Violence%20Against%20Children%20and%20COVID%2019%20ENG.pdf 07/06/2021

39 COVID-19 Conversations: The Crisis of Online Child Sexual Exploitation (Equality Now, 2020) Accessed from: https://www.equalitynow.org/covid_19_online_exploitation 07/06/2021

40 Keeping Children Safe in Uganda's COVID-19 Response (Save the Children, 2020) Accessed from: https://resourcecentre.savethechildren.net/node/17615/pdf/Joining%20Forces%20-%20Protecting%20children%20during%20Covid-19%20in%20Uganda.pdf 08/06/2021

41 La violencia contra los niños aumenta con la covid (Inter Press Service, 2021) Accessed from: https://ipsnoticias.net/2021/04/la-violencia-los-ninos-aumenta-la-covid/ 11/06/2021

42 Child Sexual Exploitation Materials Hotline Annual Report 2020 (EOKM, 2021) Accessed from: https://www.eokm.nl/wp-content/uploads/2021/04/EOKM-Jaarveslag-2020-DEF-ENG.pdf 17/06/2021

43 National Strategic Assessment of Serious and Organised Crime (National Crime Agency, 2021) Received by email from the NCA, 25/05/2021

44 Pedophilia and Sexual Offending Against Children: Theory, Assessment, and Intervention, Second Edition (Michael Seto, 2018)

45 Research report: The impact of COVID-19 on the risk of online child sexual exploitation and the implications for child protection and policing (University of New South Wales, Sydney, 2021) Accessed from: https://www.arts.unsw.edu.au/sites/default/files/documents/eSafety-OCSE-pandemic-report-salter-and-wong.pdf?utm_source=ActiveCampaign&utm_medium=email&utm_content=New+briefings+and+reports+-from+the+Alliance+and+our+members&utm_campaign=-May+2021+newsletter 07/06/2021

46 IWF Annual Report 2020: Hidden Services (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/other/hidden 07/06/2021

47 Europol Serious and Organised Crime Threat Assessment (SOCTA) 2021 (Europol, 2021) Accessed from: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment 20/04/2021

48 Why Children are at risk of sexual exploitation during COVID-19 (ECPAT International, 2020) Accessed from: https://ecpat.exposure.co/covid19?embed=true 07/06/2021

49 Europol Serious and Organised Crime Threat Assessment (SOCTA) 2021 (Europol, 2021) Accessed from: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment 20/04/2021

50 Netclean Annual Report 2020; Insight 4: Moderate increase in actual investigations and cases (Netclean, 2020) Accessed from: https://www.netclean.com/netclean-report-2020/insight-4/ 06/05/2021

51 COVID-19 to add as many as 150 million extreme poor by 2021 (World Bank, 2020) Accessed from: https://www.worldbank.org/en/news/press-release/2020/10/07/covid-19-to-add-as-many-as-150-million-extreme-poor-by-2021 06/07/2021

52 Joint Leaders' statement – Violence against children: A hidden crisis of the COVID-19 pandemic (World Health Organisation, 2020) Accessed from: https://www.who.int/news/item/08-04-2020-joint-leader-s-statement---violence-against-children-a-hidden-crisis-of-the-covid-19-pandemic 07/06/2021

53 Children's screen time has soared in the pandemic, alarming parents and researchers (NY Times, 2021) Accessed from: https://www.nytimes.com/2021/01/16/health/covid-kids-tech-use.html 16/07/2021

54 Children at increased online risk during COVID-19 pandemic (UNICEF, 2020) Accessed from: https://www.unicef.org/bhutan/press-releases/children-increased-online-risk-during-covid-19-pandemic 16/07/2021

55 The impact of the coronavirus pandemic on child welfare: sexual abuse (NSPCC, 2020) Accessed from: https://learning.nspcc.org.uk/media/2280/impact-of-coronavirus-pandemic-on-child-welfare-sexual-abuse.pdf 16/07/2021

56 Aumentan casos de abuso infantil tras relajar medidas en Paraguay (Prensa Latina, 2021) Accessed from: https://www.prensa-latina.cu/index.php?o=rn&id=437283 07/06/2021

57 Impact of coronavirus disease on different manifestations of sale and sexual exploitation of children (United Nations, 2021) Accessed from: https://reliefweb.int/sites/reliefweb.int/files/resources/A_HRC_46_31_E.pdf 07/06/2021

58 Child protection in the time of COVID-19 (Australian Institute of Health and Welfare, 2021) Accessed from: https://www.aihw.gov.au/reports/child-protection/child-protection-in-the-time-of-covid-19/summary 16/06/2021

59 Protecting children from violence in the time of COVID-19: Disruptions in prevention and response services (Unicef, 2020) Accessed from: https://www.unicef.org/reports/protecting-children-from-violence-covid-19-disruptions-in-prevention-and-response-services-2020 07/06/2021

60 Netclean Annual Report; Insight 5: COVID-19 has affected the capacity to investigate child sexual abuse crimes (Netclean, 2021) Accessed from: https://www.netclean.com/netclean-report-2020/insight-5/ 07/06/2021

61 Summary paper on online child sexual exploitation (ECPAT, 2020) Accessed from: https://www.ecpat.org/wp-content/uploads/2020/12/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf 22/04/2021

62 States divert funds, cut expenditure to foot COVID-19 bill (Economic Times, 2021) Accessed from: https://economictimes.indiatimes.com/news/india/states-divert-funds-cut-expenditure-to-foot-covid-19-bill/articleshow/82448577.cms?from=mdr 07/06/2021

63 Policy Responses to COVID-19: Iraq (International Monetary Fund, 2021) Accessed from: https://www.imf.org/en/Topics/imf-and-covid19/Policy-Responses-to-COVID-19#top 07/06/2021

64 UK's drastic cut to overseas aid risks future pandemics, say Sage experts (Guardian, 2021) Accessed from: https://www.theguardian.com/education/2021/mar/20/uks-drastic-cut-to-overseas-aid-risks-future-pandemics-say-sage-experts 16/07/2021

65 100+ Internet Statistics and Facts for 2021 (Website Hosting Rating, 2021) Accessed from: https://www.websitehostingrating.com/internet-statistics-facts/ 29/04/2021

66 Worldwide digital population as of January 2021 (Statista, 2021) Accessed from: https://www.statista.com/statistics/617136/digital-population-worldwide/ 29/04/2021

67 In-depth analysis of changes in world internet performance (GSMA, 2019) Accessed from: https://www.gsma.com/membership/resources/in-depth-analysis-of-changes-in-world-internet-performance-using-the-speedtest-global-index/ 29/04/2021

68 Number of mobile devices worldwide 2020-2024 (Statista, 2020) Accessed from: https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/ 29/04/2021

69 Children in a digital world (Unicef, 2017) Accessed from: https://www.unicef.org/media/48601/file 29/04/2021

70 Africa Is the Next Frontier For The Internet (Forbes, 2020) accessed from: https://www.forbes.com/sites/miriamtuerk/2020/06/09/africa-is-the-next-frontier-for-the-internet/?sh=e8ecd3b49001 04/05/2021

71 Strong mobile growth predicted for sub-Saharan Africa (Connecting Africa, 2020) Accessed from: http://www.connectingafrica.com/author.asp?section_id=761&doc_id=764310 04/05/2021

72 Child Online Safety: Minimising the Risk of Violence, Abuse and Exploitation Online (Broadband Commission, 2019) Accessed from: https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf 02/04/2021

73 Mobile technology the key to bringing 'education to all', says UN Broadband Commission (Unesco, 2014) Accessed from: https://en.unesco.org/news/mobile-technology-key-bringing-education-all-says-broadband-commission 14/05/2021

74 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf 23/02/2021

75 The Internet of Toys: Implications of increased connectivity and convergence of physical and digital play in young children (LSE, 2017) Accessed from: https://blogs.lse.ac.uk/parenting4digitalfuture/2017/07/19/the-internet-of-toys-implications-of-increased-connectivity-and-convergence-of-physical-and-digital-play-in-young-children/ 20/07/2021

76 Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking (Thorn, 2021) Accessed from: https://www.thorn.org/thorn-research-minors-perspectives-on-disclosing-reporting-and-blocking/ 15/07/2021

77 Exposure to sexually explicit media in early adolescence (Lin et al., 2020) Accessed from: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0230242 16/02/2021

78 Growing up in a connected world (UNICEF, 2019) Accessed from: https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf 30/04/2021

79 Child and adolescent pornography exposure (Hornor, 2020) Accessed from: https://www.jpedhc.org/article/S0891-5245(19)30384-0/fulltext 30/04/2021

80 Working with Children and Young People Who Have Displayed Harmful Sexual Behaviour (Allardyce and Yates, 2020)

81 Action to End Child Sexual Abuse and Exploitation (UNICEF, 2020) p.50 Accessed from: https://www.unicef.org/media/89026/file/CSAE-Report.pdf 17/05/2021

82 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf 23/02/2021

83 Growing up in a connected world (UNICEF, 2019) Accessed from: https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf 30/04/2021

84 Impact of online and offline child sexual abuse: "Everyone deserves to be happy and safe" (NSPCC, 2017) Accessed from: https://learning.nspcc.org.uk/research-resources/2017/impact-online-offline-child-sexual-abuse 17/05/2021

85 Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking (Thorn, 2021) Accessed from: https://www.thorn.org/thorn-research-minors-perspectives-on-disclosing-reporting-and-blocking/ 15/07/2021

86 How Everyone's Invited's 'rape culture' claims sparked a #MeToo movement in UK schools (Evening Standard, 2021) Accessed from: https://www.standard.co.uk/insider/everyones-invited-rape-culture-metoo-movement-schools-b925924.html 18/05/2021

87 #MeToo in school: too many children are sexually harassed by classmates (The Guardian, 2018) Accessed from: https://www.theguardian.com/commentisfree/2018/feb/11/metoo-school-children-teens-sexual-harassment (18/05/2021)

88 Everyone's Invited (Everyone's Invited, 2020) Accessed from: https://www.everyonesinvited.uk/ 18/05/2021

89 Children and parents: Media use and attitudes report 2019 (Ofcom, 2019) Accessed from: https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf 18/05/2021

90 PA Consulting Engagement with Edward Dixon (Rigr AI), 18/03/2021

91 'End Online Violence: Learnings from Sri Lanka' Conference (End Violence Against Children, 25/02/2021)

92 Darknet Cybercrime Threats to South East Asia (UNODC, 2021) Accessed from: https://www.unodc.org/documents/southeastasiaandpacific/Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf 29/04/2021

93 PA Consulting engagement with Interpol, 25/03/2021

94 Interpol: International police coordination required to combat global cyberthreats (CSO, 2021) Accessed from: https://www.csoonline.com/article/3624992/interpol-international-police-coordination-required-to-combat-global-cyberthreats.html 20/07/2021

95 Child sexual abuse material: Model legislation and global review (ICMEC, 2021) Accessed from: https://www.icmec.org/csam-model-legislation/ 29/04/2021

96 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: https://www.ijmuk.org/images/EMBARGO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf 15/02/2021

97 PA Consulting engagement with Europol, 17/03/2021

98 'Legality of Child Pornography' (Wikipedia, 2021) Accessed from: https://en.wikipedia.org/wiki/Legality_of_child_pornography 17/05/2021

99 PA Consulting engagement with United States Department of Justice, 22/03/2021

100 Safer Technology, Safer Users: The UK as a world-leader in Safety Tech (UK Government, 2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/887349/Safer_technology__safer_users-_The_UK_as_a_world-leader_in_Safety_Tech.pdf 18/05/2021

101 The UK Safety Tech Sector: 2021 Analysis (DCMS, 2021) Provided by DCMS on 19/05/2021

102 The UK Safety Tech Sector: 2021 Analysis (DCMS, 2021) Provided by DCMS on 19/05/2021

103 Child Online Safety: Minimising the Risk of Violence, Abuse and Exploitation Online (Broadband Commission, 2019) Accessed from: https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf 2/4/2021

104 Child Online Safety: Minimising the Risk of Violence, Abuse and Exploitation Online (Broadband Commission, 2019) Accessed from: https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf 2/4/2021

105 Metadata-based detection of child sexual abuse material (Periera, Dodhia and Brown, 2020) Accessed from: https://arxiv.org/pdf/2010.02387.pdf 29/04/2021

106 PA Consulting engagement with Terre des Hommes, 25/02/2021

107 Safer Technology, Safer Users: The UK as a world-leader in Safety Tech (UK Government, 2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/887349/Safer_technology__safer_users-_The_UK_as_a_world-leader_in_Safety_Tech.pdf 18/05/2021

108 The UK Safety Tech Sector: 2021 Analysis (DCMS, 2021) Provided by DCMS on 19/05/2021

109 Together to #ENDviolence: Global Policy Briefing; Key Messages (The End Violence Partnership, 2020) Received via email from the End Violence Partnership on 13/07/2021

110 Technology, privacy and rights: keeping children safe from child sexual exploitation and abuse online (WeProtect Global Alliance, 2021) Accessed from: https://www.weprotect.org/wp-content/uploads/Technology-privacy-and-rights-roundtable-outcomes-briefing.pdf 02/06/2021

111 Handbook for policy makers on the rights of the child in the digital environment (Council of Europe, 2020) Accessed from: https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8 06/05/021

112 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf 23/02/2021

113 Germany's Network Enforcement Act and its impact on social networks (Taylor Wessing, 2018) Accessed from: https://www.taylorwessing.com/download/article-germany-nfa-impact-social.html 10/06/21

114 Email received from the Office of the e-Safety Commissioner, 13/07/2021

115 UK to introduce world first online safety laws (GOV.UK, 2019) Accessed from: https://www.gov.uk/government/news/uk-to-introduce-world-first-online-safety-laws 10/06/2021

116 The EU unveils its plan to rein in big tech (Economist, 2020) Accessed from: https://www.economist.com/business/2020/12/15/the-eu-unveils-its-plan-to-rein-in-big-tech 10/06/2021

117 Online Safety and Media Regulation Bill (GOV.IE, 2020) Accessed from: https://www.gov.ie/en/publication/d8e4c-online-safety-and-media-regulation-bill/ 10/06/2021

118 Communication from the Commission to the European parliament, the council, the European economic and Social Committee and the Committee of the Regions: EU Strategy for a more effective fight against child sexual abuse (European Commission, 2020) Accessed from: https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf 10/06/2021

119 End-to-End Encryption: Understanding the impacts for child safety online (NSPCC, 2021) Accessed from: https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf 10/06/2021

120 Encryption, Privacy and Children's Right to Protection from Harm (Unicef, 2020) Accessed from: https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf 21/07/2021

121 Google is testing end-to-end encryption in android messages (Wired, 2020) Accessed from: https://www.wired.com/story/google-is-testing-end-to-end-encryption-in-android-messages/ 10/06/2021

122 NSPCC urges Facebook to stop encryption plans (BBC News, 2020) Accessed from: https://www.bbc.co.uk/news/technology-51391301 10/06/2021

123 End-to-End Encryption (NSPCC, 2021) Accessed from: https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf 25/05/2021

124 Briefing on the future of digital tools to detect child sexual exploitation and abuse online in Europe (WeProtect Global Alliance, 2021) Accessed from: https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/600086ba8f223010c1b4b756/1610647258029/WPGA+European+ePrivacy+briefing+Jan+21.pdf 10/06/2021

125 A battle won, but not the war in the global fight for child safety (NCMEC, 2021) Accessed from: https://www.missingkids.org/childsafetyfirst#:~:text=As%20NCMEC%20has%20recently%20reported%2C%20we%20have%20seen,to%20offer%20permanent%20solutions%20for%20child%20safety%20online. 10/06/2021

126 Provisional agreement on temporary rules to detect and remove online child abuse (News, European Parliament, 2021) Accessed from: https://www.europarl.europa.eu/news/en/press-room/20210430IPR03213/provisional-agreement-on-temporary-rules-to-detect-and-remove-online-child-abuse 22/06/2021

127 Project Beacon: EU comes to political agreement to continue the use of online tools against CSAM (ECPAT, 2021) Accessed from: https://www.ecpat.org/news/tag/project-beacon/ 21/07/2021

128 The EU Strategy on the Rights of the Child and the European Child Guarantee (European Commission, 2021) Accessed from: The EU Strategy on the Rights of the Child and the European Child Guarantee | European Commission (europa.eu) 21/07/2021

129 Fighting against child sexual abuse: join the stakeholder consultation (European Commission, 2021) Accessed from: https://ec.europa.eu/home-affairs/news/fighting-against-child-sexual-abuse-join-stakeholder-consultation_en 21/07/2021

130 NCMEC's Statement Regarding End-to End Encryption (NCMEC, 2019) Accessed from: https://www.missingkids.org/blog/2019/post-update/end-to-end-encryption 10/06/2021

131 Encryption, Privacy and Children's Right to Protection from Harm (Unicef, 2020) Accessed from: https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf 21/07/2021

132 Statement on end-to-end encryption and public safety (Australian Government Department of Home Affairs, 2021) Shared by the Australian Department of Home Affairs by email, 19/05/2021

133 VGT position on End-to-End Encryption (Virtual Global Taskforce, 2021 Received via email from the NCA on 14/06/2021

134 NCA National Strategic Assessment of Serious and Organised Crime (National Crime Agency, 2021) Received via email from the NCA on 25/05/2021

135 PA Consulting Engagement with Dr. Hany Farid, 15/03/2021

136 Opinion: Facebook's encryption makes it harder to detect child abuse (Berkeley, 2019) Accessed from: https://www.ischool.berkeley.edu/news/2019/opinion-facebooks-encryption-makes-it-harder-detect-child-abuse 10/06/2021

137 PA Consulting Engagement with Dr. Hany Farid, 15/03/2021

138 PA Consulting Engagement with Dr. Hany Farid, 15/03/2021

139 Opinion: Facebook's encryption makes it harder to detect child abuse (Berkeley, 2019) Accessed from: https://www.ischool.berkeley.edu/news/2019/opinion-facebooks-encryption-makes-it-harder-detect-child-abuse 10/06/2021

140 Encryption, Privacy and Children's Right to Protection from Harm (Unicef, 2020) Accessed from: https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf 21/07/2021

141 PA Consulting Engagement with Dr. Hany Farid, 15/03/2021

142 End-to-End Encryption (NSPCC, 2021) Accessed from: https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf 25/05/2021

143 Encryption, Privacy and Children's Right to Protection from Harm (Unicef, 2020) Accessed from: https://www.unicef-irc.org/publications/pdf/Encryption_privacy_and_children%E2%80%99s_right_to_protection_from_harm.pdf 21/07/2021

144 Project Arachnid: Online Availability of Child Sexual Abuse Material (Canadian Centre for Child Protection, 2021) Accessed from: https://protectchildren.ca/en/resources-research/project-arachnid-csam-online-availability/ 10/06/2021

145 Webinar: The Online Harms Bill – more harm than good? (11KBW, 20/05/2021)

146 Protection of children should always trump protection of privacy (Julie Inman Grant, eSafety Commissioner, 2020) Accessed from: https://www.esafety.gov.au/about-us/blog/protecting-children-should-always-trump-protecting-privacy 10/06/2021

147 The Decentralised Web of Hate: White Supremacists are starting to use peer-to-peer technology; are we prepared? (Rebellious Data LLC, 2020) Accessed from: https://rebellious-data.com/wp-content/uploads/2020/10/P2P-Hate-Report.pdf 10/06/2021

148 Messaging services are providing a more private internet (Economist, 2021) Accessed from: https://www.economist.com/international/2021/01/23/messaging-services-are-providing-a-more-private-internet 10/06/2021

149 Technology, privacy and rights: keeping children safe from child sexual exploitation and abuse online (WeProtect Global Alliance, 2021) Accessed from: https://www.weprotect.org/wp-content/uploads/Technology-privacy-and-rights-roundtable-outcomes-briefing.pdf 02/06/2021

150 Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (WeProtect Global Alliance, 2020) Accessed from: https://www.weprotect.org/library/voluntary-principles-to-counter-online-child-sexual-exploitation-and-abuse/ 10/06/2021

151 Tech giants list principles for handling harmful content (Axios, 2021) Accessed from: https://www.axios.com/tech-giants-list-principles-for-handling-harmful-content-5c9cfba9-05bc-49ad-846a-baf01abf5976.html 10/06/2021

152 The Technology Coalition Announces Project Protect (Technology Coalition, 2020) Accessed from: https://www.technologycoalition.org/2020/05/28/a-plan-to-combat-online-child-sexual-abuse/ 24/06/2021

153 Online enticement reports skyrocket in 2020 (NCMEC, 2021) Accessed from: https://www.missingkids.org/blog/2021/online-enticement-reports-skyrocket-in-2020 24/02/2021

154 Online enticement (NCMEC) Accessed from: https://www.missingkids.org/netsmartz/topics/onlineenticement 19/04/2021

155 Online child sexual abuse activity has increased (NetClean, 2021) Accessed from: https://www.netclean.com/netclean-report-2020/insight-2/ 26/01/2021

156 Trends identified in CyberTipline sextortion reports (NetClean, 2016) Accessed from: https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/sextortionfactsheet.pdf 01/03/2021

157 Child Online Safety: Minimising the Risk of Violence, Abuse and Exploitation Online (Broadband Commission, 2019) Accessed from: https://broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Report.pdf 02/04/2021

158 Out of the Shadows (Economist Impact, 2018) Accessed from: https://outoftheshadows.eiu.com/ 25/01/2021

159 Online grooming of children for sexual purposes (ICMEC, 2017) Accessed from: https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf 04/02/2021

160 Kids & Tech: Evolution of Today's Digital Natives (Influence Central, 2017) Accessed from: https://influence-central.com/trendspotting/launching-the-new-influence-central-trend-report 12/04/2021

161 Technology working group report (Child Dignity Foundation, 2018) Accessed from: https://johnc1912.files.wordpress.com/2018/11/1d5b1-cdatechnicalworkinggroupreport.pdf 26/02/2021

162 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf 23/02/2021

163 Online grooming: What it is, how it happens, and how to defend children (Thorn, 2020) Accessed from: https://www.thorn.org/blog/online-grooming-what-it-is-how-it-happens-and-how-to-defend-children/ 07/04/2021

164 The impact of the Coronavirus pandemic on child welfare: Online abuse (NSPCC, 2020) Accessed from: https://learning.nspcc.org.uk/media/2390/impact-of-coronavirus-pandemic-on-child-welfare-online-abuse.pdf 10/03/2021

165 Trends identified in cybertipline sextortion reports (NetClean, 2016) Accessed from: https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/sextortionfactsheet.pdf 01/03/2021

166 The impact of the Coronavirus pandemic on child welfare: Online abuse (NSPCC, 2020) Accessed from: https://learning.nspcc.org.uk/media/2390/impact-of-coronavirus-pandemic-on-child-welfare-online-abuse.pdf 11/03/2021

167 COVID-19: Child Sexual Exploitation (Europol, 2020) Accessed from: https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation 28/01/2021

168 COVID-19 accelerates global video gaming market to $170bn (Consultancy-me.com, 2020) Accessed from: https://www.consultancy-me.com/news/3041/covid-19-accelerates-global-gaming-market-to-170-billion 16/02/2021

169 The Marie Collins Foundation, Accessed from: https://www.mariecollinsfoundation.org.uk/ 29/04/2021

170 Survey of Technology Companies (WeProtect Global Alliance and Technology Coalition, 2021) See Annex A: Findings from WeProtect Global Alliance/Technology Coalition Survey of Technology Companies

171 Online grooming of children for sexual purposes (ICMEC, 2017) Accessed from: https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf 04/02/2021

172 Safety-by-design overview (eSafety Commissioner, 2019) Accessed from: https://www.esafety.gov.au/sites/default/files/2019-10/SBD%20-%20Overview%20May19.pdf 11/02/2021

173 Digital Age Assurance Tools and Children's Rights Online across the Globe (UNICEF, 2021) Accessed from: https://www.unicef.org/media/97461/file/Digital%20Age%20Assurance%20Tools%20and%20Children%E2%80%99s%20Rights%20Online%20across%20the%20Globe.pdf 07/05/2021

174 Video games and online chats are 'hunting grounds' for sexual predators (New York Times, 2019) Accessed from: https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html 21/04/2021

175 Case study submission from TikTok, received on 10/05/2021

176 Continuing to Make Instagram Safer for the Youngest Members of Our Community (Instagram, 2021) Accessed from: https://about.instagram.com/blog/announcements/continuing-to-make-instagram-safer-for-the-youngest-members-of-our-community 21/04/2021

177 What is a supervised experience on YouTube? (Google, 2021) Accessed from: https://support.google.com/youtube/answer/10314940?hl=en 20/07/2021

178 Perpetrators of sexual violence: statistics (RAINN) Accessed from: https://www.rainn.org/statistics/perpetrators-sexual-violence 16/04/2021

179 The sexual exploitation and abuse of deaf and disabled children online (WeProtect Global Alliance, 2021) Accessed from: https://www.weprotect.org/wp-content/uploads/Intelligence-briefing-2021-The-sexual-exploitation-and-abuse-of-disabled-children.pdf 23/02/2021

180 Ending violence against children: key messages and statistics (End Violence Against Children) https://www.end-violence.org/sites/default/files/paragraphs/download/Key Messages_Long_0.pdf 12/04/2021

181 CyberTipline: 2019 & 2020 Reports by country (NCMEC, 2020) accessed from: https://www.missingkids.org/gethelpnow/cybertipline 19/04/2021

182 Online sexual exploitation of children in the Philippines (International Justice Mission, 2020) Accessed from: https://www.ijm.org/documents/studies/Final-Public-Full-Report-5_20_2020.pdf 17/02/2021

183 Annual Report 2020 (INHOPE, 2021) Accessed from: https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf 06/05/2021

184 IWF Annual Report: International Overview (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/overview 21/04/2021

185 Self-generated child sexual abuse (IWF Annual Report, 2020) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/selfgenerated 29/07/2021

186 Impact of coronavirus disease on different manifestations of sale and sexual exploitation of children (United Nations, 2021) Accessed from: https://reliefweb.int/sites/reliefweb.int/files/resources/A_HRC_46_31_E.pdf 04/03/2021

187 Violencia sexual a menores ya deja mas de mil victimas en lo corrido de 2021 (LAFM, 2021) Accessed from: https://www.lafm.com.co/colombia/violencia-sexual-menores-ya-deja-mas-de-mil-victimas-en-lo-corrido-de-2021 11/03/2021

188 Abuso sexual en internet y redes de trata (Infobae, 2020) Accessed from: https://www.infobae.com/america/mexico/2020/07/27/abuso-sexual-en-internet-y-redes-de-trata-los-crimenes-contra-la-ninez-que-aumentaron-durante-la-pandemia/ 25/02/2021

189 Production and distribution of child sexual abuse material by parental figures (Australian Institute of Criminology, 2021) Accessed from: https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf 09/03/2021

190 Los casos de abuso sexual contra menores en espana se multiplican por 4 en la ultima decada (Levante, 2021) Accessed from: https://protect-eu.mimecast.com/s/WuEPCWnWgFxLBY3Hxchqm?domain=levante-emv.com 23/02/2021

191 Production and distribution of child sexual abuse material by parental figures (Australian Institute of Criminology, 2021) Accessed from: https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf 09/03/2021

192 Online enticement of children: an in-depth analysis of CyberTipline reports (National Center for Missing and Exploited Children, 2017) Accessed from: https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Online%20Enticement%20Pre-Travel1.pdf 11/02/2021

193 The cycle of child sexual abuse stops now (Project Arachnid) Accessed from: https://projectarachnid.ca/en/ 07/04/2021

194 PA Consulting engagement with United States Department of Justice, 22/03/2021

195 PA Consulting engagement with United Kingdom National Crime Agency, 18/02/2021

196 Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic (Europol, 2020) Accessed from: https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic 26/01/2021

197 Child abuse predator 'handbook' lists ways to target children during coronavirus lockdown (The Guardian, 2020) Accessed from: https://www.theguardian.com/society/2020/may/14/child-abuse-predator-handbook-lists-ways-to-target-children-during-coronavirus-lockdown 23/02/2021

198 Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic (Europol, 2020) Accessed from: https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic 26/01/2021

199 PA Consulting engagement with Australian Centre to Counter Child Exploitation, 01/03/2021

200 South Korea confronts its voyeurism epidemic (The Guardian, 2018) Accessed from: https://www.theguardian.com/world/2018/jul/03/a-part-of-daily-life-south-korea-confronts-its-voyeurism-epidemic-sexual-harassment 08/03/2021

201 Netclean Report 2019: A report about child sexual abuse crime (Netclean, 2019) Accessed from: https://www.netclean.com/netclean-report-2019/ 28/01/2021

202 A deepfake porn bot is being used to abuse thousands of women (WIRED, 2020) Accessed from: https://www.wired.co.uk/article/telegram-deepfakes-deepnude-ai 19/03/2021

203 Cybersex, erotic tech and virtual intimacy are on the rise during COVID-19 (The Conversation, 2020) Accessed from: https://theconversation.com/cybersex-erotic-tech-and-virtual-intimacy-are-on-the-rise-during-covid-19-141769 19/03/2021

204 Immersive Technologies – Position Statement (e-Safety Commissioner, 2021) Accessed from: https://www.esafety.gov.au/about-us/tech-trends-and-challenges/immersive-tech 14/07/2021

205 CGI (Computer Generated Imagery) (TechTarget, 2016) Accessed from: https://whatis.techtarget.com/definition/CGI-computer-generated-imagery 08/04/2021

206 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Interagency Working Group on Sexual Exploitation of Children, 2016) Accessed from: https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf 17/03/2021

207 What is deepfake? (Business Insider, 2021) Accessed from: https://www.businessinsider.com/what-is-deepfake?r=US&IR=T#:~:text=Recently%2C%20deepfake%20technology%20has%20been,with%20another%20in%20recorded%20video 08/04/2021

208 PA Consulting engagement with Terre des Hommes, 25/02/2021

209 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT France, 2017) Accessed from: https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf 09/08/2021

210 Non-photographic visual depictions (Internet Watch Foundation, 2007) Accessed from: https://www.iwf.org.uk/what-we-do/who-we-are/consultations/non-photographic-visual-depictions 17/03/2021

211 Child Sexual Abuse Material: Model Legislation and Global Review (International Center for Missing and Exploited Children, 2018) Accessed from: https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf 05/03/2021

212 Computer-generated 'Sweetie' catches online predators (BBC News, 2013) Accessed from: https://www.bbc.co.uk/news/uk-24818769 08/03/2021

213 Child sexual abuse in the digital era: Rethinking legal frameworks and transnational law enforcement collaboration (Universiteit Leiden, 2020) Accessed from: https://scholarlypublications.universiteitleiden.nl/access/item%3A2966712/view 07/05/2021

214 National Strategic Assessment of Serious and Organised Crime 2020 (National Crime Agency, 2020) Accessed from: https://www.nationalcrimeagency.gov.uk/news/nsa2020 24/03/2021

215 Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic (Europol, 2020) Accessed from: https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic 26/01/2021

216 PA Consulting engagement with Interpol, 25/03/2021

217 PA Consulting engagement with Ethel Quayle, 04/03/2021

218 The Internet: Investigation Report (Independent Inquiry into Child Sexual Exploitation and Abuse, 2020) Accessed from: https://www.iicsa.org.uk/publications/investigation/internet 02/02/2021

219 Internet Organised Crime Threat Assessment (IOCTA) 2020 (Europol, 2020) Accessed from: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020 30/03/2021

220 Europol Serious and Organised Crime Threat Assessment (SOCTA) 2021 (Europol, 2021) Accessed from: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment 20/04/2021

221 Child Rescue Coalition (CRC): Protecting Innocence Through Technology (CRC, 2021) Email received from CRC, 30/03/2021

222 Global Threat Assessment 2019 (WeProtect Global Alliance, 2019) Accessed from: https://www.weprotect.org/issue/global-threat-assessment/ 26/01/2021

223 Hackers leaked 22 million records on the dark web in 2020 (ID Agent, 2020) Accessed from: https://www.idagent.com/hackers-leaked-22-million-records-on-the-dark-web-in-2020 29/04/2021

224 Trends in Online Child Sexual Abuse Material (ECPAT, 2017) Accessed from: https://www.ecpat.org/wp-content/uploads/2016/05/Emerging-Issues-and-Global-Threats-Children-online-2017-1.pdf 25/03/2021

225 COVID-19: Child Sexual Exploitation (Europol, 2020) Accessed from: https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation 20/04/2021

226 Brave.com now has its own Tor onion service, providing more users with secure access to Brave (Brave.com, 2020) Accessed from: https://brave.com/new-onion-service/ 20/04/20

227 Tor (Investopedia, 2019) Accessed from: https://www.investopedia.com/terms/t/tor.asp 07/05/2021

228 PA Consulting engagement with United States Department of Justice, 07/04/2021 NCMEC Engagement

229 PA Consulting engagement with United Kingdom National Crime Agency, 18/02/2021

230 PA Consulting engagement with United States National Centre for Missing and Exploited Children, 16/03/2021

231 Millions of attempts to access child sexual abuse online during lockdown (Internet Watch Foundation, 2020) Accessed from: https://www.iwf.org.uk/news/millions-of-attempts-to-access-child-sexual-abuse-online-during-lockdown 08/02/2021

232 COVID-19 conversations: The Crisis of Online Child Exploitation (Equality Now, 2021) Accessed from: https://www.equalitynow.org/covid_19_online_exploitation 07/06/2021

233 Impact of coronavirus disease on different manifestations of sale and sexual exploitation of children (United Nations, 2021) Accessed from: https://reliefweb.int/sites/reliefweb.int/files/resources/A_HRC_46_31_E.pdf 04/03/2021

234 The Motivation-Facilitation Model of Sexual Offending (Michael C. Seto, 2017) Accessed from: https://journals.sagepub.com/doi/full/10.1177/1079063217720919 29/07/2021

235 Internet Sex Offenders (Seto, Michael C., 2013)

236 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: https://www.ijmuk.org/images/EMBARGO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf 15/02/2021

237 Sexual interests of child sexual exploitation material (CSEM) consumers (Fortin and Proulx, 2018) Accessed from: https://journals.sagepub.com/doi/10.1177/0306624X18794135 11/02/2021

238 Prevention, disruption and deterrence of online child sexual exploitation and abuse (Quayle, 2020) Accessed from: https://www.research.ed.ac.uk/en/publications/prevention-disruption-and-deterrence-of-online-child-sexual-explo 05/03/2021

239 How extreme porn has become a gateway drug into child abuse (The Guardian, 2020) Accessed from: https://www.theguardian.com/global-development/2020/dec/15/how-extreme-porn-has-become-a-gateway-drug-into-child-abuse 15/02/2021

240 Effects of automated messages on internet users attempting to access 'barely legal' pornography (Prichard, Wortley, Watters, Spiranovic, Hunn, Krone, 2020) Received from Donald Findlater (Lucy Faithfull Foundation), 16/02/2021

241 Exposure to sexually explicit media in early adolescence (Lin et al., 2020) Accessed from: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0230242 16/02/2021

242 Working with Children and Young People Who Have Displayed Harmful Sexual Behaviour (Allardyce and Yates, 2020)

243 On Youtube's Digital Playground, an Open Gate for Pedophiles (The New York Times, 2019) Accessed from: https://www.nytimes.com/2019/06/03/world/americas/youtube-pedophiles.html?module=inline 04/03/2021

244 Prevention, disruption and deterrence of online child sexual exploitation and abuse (Quayle, 2020) Accessed from: https://www.research.ed.ac.uk/en/publications/prevention-disruption-and-deterrence-of-online-child-sexual-explo 05/03/2021

245 On Youtube, a network of paedophiles is hiding in plain sight (WIRED, 2019) Accessed from: https://www.wired.co.uk/article/youtube-pedophile-videos-advertising 31/03/2021

246 Barriers Abusers Overcome In Order To Abuse (Psychology Tools) Accessed from: https://www.psychologytools.com/resource/barriers-abusers-overcome-in-order-to-abuse/ 29/03/2021

247 Child Sexual Abuse (Finkelhor, 1984)

248 The Four Rs of Responsibility, Part 1: Removing Harmful Content (Youtube, 2019) Accessed from: https://blog.youtube/inside-youtube/the-four-rs-of-responsibility-remove/ 27/07/2021

249 Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation (NatCen Social Research, 2017) Accessed from: https://natcen.ac.uk/media/1535277/Behaviours-and-characteristics-of-perpetrators-of-online-facilitated-child-sexual-abuse-and-exploitation.pdf 09/02/2021

250 Survey of Technology Companies (WeProtect Global Alliance and Technology Coalition, 2021) See Annex A: Findings from WeProtect Global Alliance/Technology Coalition Survey of Technology Companies

251 Online sexual exploitation of children in the Philippines (International Justice Mission, 2020) Accessed from: https://www.ijm.org/documents/studies/Final-Public-Full-Report-5_20_2020.pdf 23/02/2021

252 Effects of automated messages on internet users attempting to access 'barely legal' pornography (Pritchard et al., 2020)

253 Prevention, disruption and deterrence of online child sexual exploitation and abuse (Quayle, 2020) Accessed from: https://www.research.ed.ac.uk/en/publications/prevention-disruption-and-deterrence-of-online-child-sexual-explo 05/03/2021

254 Ground-breaking research on perpetrator prevention (Oak Foundation, 2021) Accessed from: https://oakfnd.org/groundbreaking-research-on-perpetration-prevention/ 13/07/2021

255 IWF Annual Report: About Our Year (IWF, 2020) Accessed from: https://annualreport2020.iwf.org.uk/about/year/ceo 21/04/2021

256 Game-changing chatbot to target people trying to access child sexual abuse online (IWF, 2020) Accessed from: https://www.iwf.org.uk/news/game-changing%E2%80%99-chatbot-to-target-people-trying-to-access-child-sexual-abuse-online 20/04/2021

257 Prevention, disruption and deterrence of online child sexual exploitation and abuse (Quayle, 2020) Accessed from: https://www.research.ed.ac.uk/en/publications/prevention-disruption-and-deterrence-of-online-child-sexual-explo 05/03/2021

258 Suojellaan Lapsia, Accessed from: https://suojellaanlapsia.fi/ 29/04/2021

259 COVID-19 and Missing and Exploited Children (NCMEC, 2021) Accessed from: https://www.missingkids.org/blog/2020/covid-19-and-missing-and-exploited-children 22/04).

260 IWF Annual Report: 2020 Trends and Data (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends 22/04/2021

261 Annual Report 2020 (INHOPE, 2021) Accessed from: https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf 06/05/2021

262 PA Consulting engagement with NCMEC, 16/03/2021

263 PA Consulting Engagement with NCMEC, 22/04/2021

264 IWF Annual Report: Site types analysis (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/sitetypes 22/04/2021

265 COVID-19: Child Sexual Exploitation (Europol, 2020) Accessed from: https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation 28/01/2021

266 PA Consulting engagement with Interpol, 25/03/2021

267 IWF Annual Report: Hidden Services (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/Trends/International/Other/Hidden 22/04

268 IWF Annual Report: Glossary (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/glossary 10/05/2021

269 How child sexual abuse material is stored (Netclean, 2019) Accessed from: https://www.netclean.com/netclean-report-2019/insight-4/ 22/04/2021

270 Annual Report 2020 (INHOPE, 2021) Accessed from: https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf 06/05/2021

271 PA Consulting engagement with Edward Dixon (Rigr AI), 18/03/2021

272 PA Consulting engagement with United States Department of Justice, 22/03/2021

273 PA Consulting engagement with Edward Dixon (Rigr AI), 18/03/2021

274 Preventing Child Exploitation on our Apps (Facebook, 2020) Accessed from: https://about.fb.com/news/2021/02/preventing-child-exploitation-on-our-apps/#:~:text=Using%20our%20apps%20to%20harm,authorities%20to%20keep%20children%20safe. 22/04/2021

275 Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims (Thorn, 2018) Accessed from: https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Production%20and%20Active%20Trading%20of%20CSAM_FullReport_FINAL.pdf 15/07/2021

276 Study on the effects of new information technologies on the abuse and exploitation of children (United Nations Office on Drugs and Crime, 2015) Accessed from: https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf 22/04/2021

277 Crime investigations of 'child abuse material' - Challenges and opportunities posed by digital technology (Marie Eneman, 2020) Accessed from: https://www.researchgate.net/publication/344072738_Crime_investigations_of_'child_abuse_material'_-_Challenges_and_opportunities_posed_by_digital_technology 10/05/2021

278 Production of child sexual abuse material by parental figures (Australian Government, Institute of Criminology, 2021) Accessed from: https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf 16/07/2021

279 Understanding the intentions of Child Sexual Abuse Material (CSAM) sharers (Facebook Research, 2021) Accessed from: https://research.fb.com/blog/2021/02/understanding-the-intentions-of-child-sexual-abuse-material-csam-sharers/ 29/06/2021

280 IWF Annual Report: Commercial content (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/Trends/International/Commercial 22/04/2021

281 IWF Annual Report: Domain analysis (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/domain 22/04/2021

282 IWF Annual Report: Commercial content (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/Trends/International/Commercial 22/04/2021

283 Cryptocurrency and the trade of online child sexual abuse material (ICMEC, 2021) Accessed from: https://cdn.icmec.org/wp-content/uploads/2021/03/Cryptocurrency-and-the-Trade-of-Online-Child-Sexual-Abuse-Material_03.17.21-publish-1.pdf 22/04/21

284 IWF Annual Report: Other Trends (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/other 22/04/2021

285 IWF Annual Report: Other Trends (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/other 22/04/2021

286 IWF Annual Report: Other Trends (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/other 22/04/2021

287 Hash Values: Fingerprinting Child Sexual Abuse Material (NetClean, 2018) Accessed from: https://www.netclean.com/2018/10/30/hash-values/ 22/04/2021

288 International Child Sexual Exploitation Database (INTERPOL, 2018) Accessed from: https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database 22/04/2021

289 IWF Annual Report: Hidden Services (IWF, 2020) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/other/hidden 10/05/2021

290 IWF Annual Report: Geographical hosting (IWF, 2020) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/geographic 10/05/2021

291 Survey of Technology Companies (WeProtect Global Alliance and Technology Coalition, 2021) See Annex A: Findings from WeProtect Global Alliance/Technology Coalition Survey of Technology Companies

292 PA Consulting engagement with IWF, 01/03/2021

293 PA Consulting engagement with Interpol, 25/03/2021

294 PA Consulting engagement with IWF, 01/03/2021

295 Technology working group report (Child Dignity Foundation, 2018) Accessed from: https://johnc1912.files.wordpress.com/2018/11/1d5b1-cdatechnicalworkinggroupreport.pdf 26/02/2021

296 Child Dignity Alliance: Technical Working Group Report (Child Dignity Alliance, 2017) Accessed from: https://static1.squarespace.com/static/5a4d5d4e7131a5845cdd690c/t/5c17cdf4032be42f613e28e4/1545063925977/Child+safety+Report+vD+for+web.pdf 22/04/2021

297 PA Consulting engagement with Edward Dixon (Rigr AI), 18/03/2021

298 IWF Annual Report: Self-generated content study (IWF, 2012) Accessed from: https://www.iwf.org.uk/sites/default/files/reports/2016-02/IWF%202012%20Annual%20and%20Charity%20Report%20%28web%29.pdf 06/05/2021

299 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT, 2017) Accessed from: https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf 22/04/2021

300 IWF Annual Report: Self-generated child sexual abuse (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/selfgenerated 06/05/2021

301 PA Consulting engagement with Internet Watch Foundation, 01/03/2021

302 Interim code of practice on online child sexual exploitation and abuse (accessible version)(GOV.UK, 2020) Accessed from: https://www.gov.uk/government/publications/online-harms-interim-codes-of-practice/interim-code-of-practice-on-online-child-sexual-exploitation-and-abuse-accessible-version 19/07/2021

303 Initial Situational Analysis on Online Child Sexual Exploitation in Cambodia (Royal Government of Cambodia, 2019) Accessed from: https://aplecambodia.org/wp-content/uploads/2020/04/Research-on-Online-Child-Sexual-Exploitation-in-Cambodia_ENG.pdf 06/05/2021

304 Prevalence of Multiple Forms of Sexting Behaviour Among Youth (Madigan et al., 2018) Accessed from: https://jamanetwork.com/journals/jamapediatrics/fullarticle/2673719?resultClick=1 06/05/2021

305 'Staying Safe Online' survey: wat unwanted sexual images are being sent to teenagers on social media? (University College London, 2019) Accessed from: https://blogs.ucl.ac.uk/ioe/2020/06/19/staying-safe-online-survey-what-unwanted-sexual-images-are-being-sent-to-teenagers-on-social-media/ 20/07/2021

306 PA Consulting engagement with United Kingdom National Crime Agency, 18/02/2021

307 IWF Annual Report: Who we are (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/about/us 11/05/2021

308 IWF Annual Report: Self-generated child sexual abuse (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/selfgenerated 06/05/2021

309 An Exploratory Study of Sexting Behaviours Among Heterosexual and Sexual Minority Early Adolescents (Van Ouytsel et al., 2019) Accessed from: https://pubmed.ncbi.nlm.nih.gov/31473082/ 14/05/2021

310 Look at me: Teens, Sexting, and Risks (Internet Matters, 2021) Accessed from https://www.internetmatters.org/wp-content/uploads/2020/06/Internet-Matters-Look-At-Me-Report-1.pdf 06/05/2021

311 Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation (National Centre for Social Research, 2018) Accessed from: https://www.iicsa.org.uk/key-documents/3720/download/rapid-evidence-assessment-behaviour-characteristics-perpetrators-online-facilitated-child-sexual-abuse-exploitation.pdf 06/05/2021

312 Online harmful sexual behaviours in children and young people under 18 (eSafety Commissioner, 2020) Accessed from: https://www.esafety.gov.au/sites/default/files/2020-09/Online%20harmful%20sexual%20behaviours%20Position%20statement.pdf 13/07/2021

313 IWF Annual Report: Self-generated child sexual abuse (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/selfgenerated 06/05/2021

314 Self-Generated Child Sexual Abuse Material: Attitudes and Experiences (Thorn, 2019) Accessed from: https://info.thorn.org/hubfs/Research/08112020_SG-CSAM_AttitudesExperiences-Report_2019.pdf 28/07/2021

315 A quantitative and qualitative examination of the impact of online pornography on the values, attitudes, beliefs and behaviours of children and young people (NSPCC, Children's Commissioner, Middlesex University London, 2016) Accessed from: https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/MDX-NSPCC-OCC-Online-Pornography-Report.pdf 28/07/2021

316 A Rapid Assessment of Live Streaming of Online Sexual Abuse and Exploitation of Children and Young People in Kathmandu (ECPAT Luxembourg, ChildSafeNet) Draft, due to be published in 2021. Received by email from ChildSafeNet Nepal, 04/03/2021

317 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf 23/02/2021

318 Online Nation: 2021 Report (Ofcom, 2021) Accessed from: https://www.ofcom.org.uk/__data/assets/pdf_file/0013/220414/online-nation-2021-report.pdf 24/06/2021

319 Faster Takedown of Online Sexual Abuse Sought (Manila-Standard.Net, 2021) Accessed from: https://manilastandard.net/mobile/article/349129 06/05/2021

320 Initial Situational Analysis on Online Child Sexual Exploitation in Cambodia (Royal Government of Cambodia, 2019) Accessed from: https://aplecambodia.org/wp-content/uploads/2020/04/Research-on-Online-Child-Sexual-Exploitation-in-Cambodia_ENG.pdf 06/05/2021

321 The children selling explicit videos on OnlyFans (BBC News, 2021) Accessed from: https://www.bbc.co.uk/news/uk-57255983 07/07/2021

322 Netclean Annual Report 2020; Insight 4: Moderate increase in actual investigations and cases (Netclean, 2020) Accessed from: https://www.netclean.com/netclean-report-2020/insight-4/ 06/05/2021

323 'Grave threat' to children from predatory internet groomers as online child sexual abuse material soars to record levels (IWF, 2021) Accessed from: https://www.iwf.org.uk/news/%E2%80%98grave-threat%E2%80%99-children-predatory-internet-groomers-online-child-sexual-abuse-material-soars 07/05/2021

324 Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation (National Centre for Social Research, 2018) Accessed from: https://www.iicsa.org.uk/key-documents/3720/download/rapid-evidence-assessment-behaviour-characteristics-perpetrators-online-facilitated-child-sexual-abuse-exploitation.pdf 06/05/2021

325 Emerging Patterns and Trends Report: Online-Produced Sexual Content (IWF, 2015) p.3 Accessed from: https://www.iwf.org.uk/sites/default/files/inline-files/Online-produced_sexual_content_report_100315.pdf 19/05/2021

326 Self-Generated Child Sexual Abuse Material: Attitudes and Experiences (Thorn, 2019) Accessed from: https://f.hubspotusercontent00.net/hubfs/7145355/Research/08112020_SG-CSAM_AttitudesExperiences-Report_2019.pdf?__hstc=208625165.851aa734d938b21fee07aa6d05-bc-9e7.1604505256798.1614622415296.1614700924025.7&__hssc=208625165.2.1614700924025&__hsfp=723267087 06/05/2021

327 The Internet: Investigation Report (Independent Inquiry into Child Sexual Exploitation and Abuse, 2020) Accessed from: https://www.iicsa.org.uk/publications/investigation/internet 02/02/2021

328 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf 23/02/2021

329 PA Consulting Engagement with SafeBAE, 02/03

330 SafeToNet acquires German mobile phone stores to safeguard children online (PR Newswire, 2021) Accessed from: https://www.prnewswire.com/news-releases/safetonet-acquires-german-mobile-phone-stores-to-safeguard-children-online-301247334.html 14/05/2021

331 Handbook for policy makers on the rights of the child in the digital environment (Council of Europe, 2020) Accessed from: 1680a069f8 (coe.int) 06/05/021

332 Teen sexting is decriminalised between partners of similar age (news.com.au, 2018) Accessed from: https://www.news.com.au/national/nsw-act/courts-law/teen-sexting-is-decriminalised-between-partners-of-similar-age/news-story/3fdceb4adbd2c6028eab1f76a86ba5ab 06/05/2021

333 Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (Council of Europe, 2007) Accessed from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/699615/MS4.2018_Lanzarote_CM9602_WEB.pdf 22/06/2021

334 Police Response to Youth Offending Around the Generation and Distribution of Indecent Images of Children and its Implications (University of Suffolk/ Marie Collins Foundation, 2019) Accessed from: https://www.uos.ac.uk/sites/www.uos.ac.uk/files/FOI-Report-Final-Outcome-21_2.pdf 13/05/2021

335 Sharing nudes and semi-nudes: advice for education settings working with children and young people (GOV.UK, 2020) Accessed from: https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people 01/06/2021

336 Action to end Child Sexual Abuse and Exploitation (UNICEF/ End Violence Against Children, 2020) Accessed from https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf 13/05/2021

337 Action to end Child Sexual Abuse and Exploitation (UNICEF/ End Violence Against Children, 2020) Accessed from https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf 13/05/2021

338 Action to end Child Sexual Abuse and Exploitation (UNICEF/ End Violence Against Children, 2020) Accessed from https://www.unicef.org/media/89206/file/CSAE-Brief-v3.pdf 13/05/2021

339 Sexting among high school students in a metropolis in Ghana: an exploratory study (Baiden et al., 2019) Accessed from: https://www.tandfonline.com/doi/abs/10.1080/17482798.2020.1719854 07/05/2021

340 Sexting: Prevalence, Predictors, and Associated Sexual Risk Behaviors among Postsecondary School Young People in Ibadan, Nigeria (Olatunde and Balogun, 2017) Accessed from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5420550/ 07/05/2021

341 Self-Generated Child Sexual Abuse Material: Attitudes and Experiences (Thorn, 2019) Accessed from: https://f.hubspotusercontent00.net/hubfs/7145355/Research/08112020_SG-CSAM_AttitudesExperiences-Report_2019.pdf?__hstc=208625165.851aa734d938b21fee07aa6d05bc9e7.1604505256798.1614622415296.1614700924025.7&__hssc=208625165.2.1614700924025&__hsfp=723267087 06/05/2021

342 A Rapid Assessment of Live Streaming of Online Sexual Abuse and Exploitation of Children and Young People in Kathmandu (ECPAT Luxembourg, ChildSafeNet) Draft, due to be published in 2021. Received by email from ChildSafeNet Nepal, 04/03/2021

343 The reception of sexual messages among young Chileans and Uruguayans (Alfaro et al., 2020) Accessed from: https://www.researchgate.net/publication/347336149_The_reception_of_sexual_messages_among_young_Chileans_and_Uruguayans 28/05/2021

344 Online Harms White Paper (UK Government, 2019) Accessed from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf 07/05/2021

345 Teenage Sexting and Sexual Behaviours in an Iranian Setting (Ghorashi, 2019) Accessed from: https://www.researchgate.net/publication/333826458_Teenage_Sexting_and_Sexual_Behaviors_in_an_Iranian_Setting 19/05/2021

346 Demystifying Sexting: Adolescent Sexting and its Associations With Parenting Styles and Sense of Parental Social Control in Israel (Dolev-Cohen and Ricon, 2020) Accessed from: https://cyberpsychology.eu/article/view/11878/11340 19/05/2021

347 Summary paper on online child sexual exploitation (ECPAT, 2020) Accessed from: https://www.ecpat.org/wp-content/uploads/2020/12/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf 22/04/2021

348 COVID-19: Child sexual exploitation and abuse threats and trends (Interpol, 2020) Accessed from: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-highlights-impact-of-COVID-19-on-child-sexual-abuse 26/01/2021

349 Safe from harm: Tackling webcam child sexual abuse in the Philippines (UNICEF, 2016) Accessed from: https://www.unicef.org/stories/safe-from-harm-tackling-webcam-child-sexual-abuse-philippines 09/08/21

350 Online sexual abuse of children rising amid COVID 19 pandemic – Save the Children Philippines (Relief Web, 2021) Accessed from: https://reliefweb.int/report/philippines/online-sexual-abuse-children-rising-amid-covid-19-pandemic-save-children 22/04/2021

351 Technical and Financial Sector Indicators of Livestreaming (IJM, 2020) Shared by IJM, 11/03/2021

352 Technical and Financial Sector Indicators of Livestreaming (IJM, 2020) Shared by IJM, 11/03/2021

353 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT, 2017) Accessed from: https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf 22/04/2021

354 Falling short: demand side sentencing for online sexual exploitation of children (International Justice Mission, 2020) Accessed from: https://www.ijmuk.org/images/EMBARGO-8-NOV-20-IJM-REPORT-FALLING-SHORT-Demand-Side-Sentencing-for-Online-Sexual-Exploitation-of-Children.pdf 15/02/2021

355 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT, 2017) Accessed from: https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf 22/04/2021

356 Victims of livestreamed child sexual abuse (Netclean, 2019) Accessed from https://www.netclean.com/netclean-report-2019/insight-2/ 22/04/2021

357 Summary paper on online child sexual exploitation (ECPAT, 2020) Accessed from: https://www.ecpat.org/wp-content/uploads/2020/12/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf 22/04/2021

358 UNICEF: What works to prevent online and offline child sexual exploitation and abuse: Review of national education strategies in East Asia and the Pacific (UNICEF, 2020) Accessed from https://www.sddirect.org.uk/media/1874/what-works-to-prevent-online-and-offline-csae-in-east-asia-and-the-pacific.pdf 22/04/2021

359 UNODC Global Trafficking Report (UNODC, 2021) Accessed from: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Chapter5.pdf 22/04/2021

360 UNODC Global Trafficking Report (UNODC, 2021) Accessed from: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Chapter5.pdf 22/04/2021

361 Impact of the COVID 19 pandemic on trafficking in persons (UNODC, 2021) Accessed from: https://www.unodc.org/documents/Advocacy-Section/HTMSS_Thematic_Brief_on_COVID-19.pdf 22/04/2021

362 UNODC Global Trafficking Report (UNODC, 2021) Accessed from: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Chapter5.pdf 22/04/2021

363 Europol Serious and Organised Crime Threat Assessment (SOCTA) 2021 (Europol, 2021) Accessed from: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment 20/04/2021

364 National Study of Online Sexual Abuse and Exploitation of Children in the Philippines (UNICEF, 2020) Accessed from: UNICEF Philippines study 22/04/2021

365 Why are human trafficking cases difficult to identify and prosecute (John Vanek, 2018) Accessed from: https://johnvanek.com/2018/01/25/why-are-human-trafficking-cases-difficult-to-identify-and-prosecute/ 11/05/2021

366 Summary paper on online child sexual exploitation (ECPAT, 2020) Accessed from: https://www.ecpat.org/wp-content/uploads/2020/12/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf 22/04/2021

367 Online sexual exploitation of children in the Philippines (IJM, 2020) Accessed from: https://ijmstoragelive.blob.core.windows.net/ijmna/documents/studies/Final-Public-Full-Report-5_20_2020.pdf 22/04/2021

368 Cryptocurrency and the Blockchain (International Centre for Missing and Exploited Children, 2017) Accessed from: https://www.icmec.org/wp-content/uploads/2017/05/ICMEC-FCACPCryptocurrencyPaperFINAL5-17.pdf 22/04/2021

369 Case Study: The Fintel Alliance – a public private partnership (AUSTRAC, 2021) Shared by the Australian Department of Home Affairs, 19/05/2021

370 IJM Composite Case Study - 'Follow the Money' – Trafficking for livestreamed Online Child Sexual Exploitation. Received by email 31/03

371 Cryptocurrency and the Blockchain (International Centre for Missing and Exploited Children, 2017) Accessed from: https://www.icmec.org/wp-content/uploads/2017/05/ICMEC-FCACPCryptocurrencyPaperFINAL5-17.pdf 22/04/2021

372 Combatting Online Child Sexual Abuse and Exploitation Through Financial Intelligence: Public Bulletin (Egmont Group, 2020) Accessed from: https://egmontgroup.org/sites/default/files/filedepot/20200901_CSAE%20Public%20Bulletin.pdf 16/07/2021

373 National Study of Online Sexual Abuse and Exploitation of Children in the Philippines (UNICEF, 2020) Accessed from: UNICEF Philippines study 22/04/2021

374 Online child sexual abuse and exploitation: Current forms and good practice for prevention and protection (ECPAT, 2017) Accessed from: https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf 22/04/2021

375 Child Dignity Alliance: Technical Working Group Report (Child Dignity Alliance, 2017) Accessed from: https://static1.squarespace.com/static/5a4d5d4e7131a5845cdd690c/t/5c17cdf4032be42f613e28e4/1545063925977/Child+safety+Report+vD+for+web.pdf 22/04/2021

376 Cambodia feared lagging behind predators in cybersex trafficking crackdown (Reuters, 2019) Accessed from: https://www.reuters.com/article/us-cambodia-sexcrimes-children/cambodia-feared-lagging-behind-predators-in-cybersex-trafficking-crackdown-idUSKCN1VW00B 22/04/2021

377 Informe de monitoreo de país sobre la explotación sexual comercial de niños, niñas y adolescentes (ECPAT, 2014) Accessed from: https://www.ecpat.org/wp-content/uploads/2016/04/IMP%20MEXICO.pdf 22/04/2021

378 A Global Strategic Response to Online Child Sexual Exploitation and Abuse (WeProtect Global Alliance, 2021) Accessed from: https://www.weprotect.org/wp-content/uploads/WeProtectGA-Global-Strategic-Response-EN.pdf 17/06/2021

379 Together to #ENDviolence: Global Policy Briefing; Key Messages (The End Violence Partnership, 2020) Received via email from the End Violence Partnership on 13/07/2021

380 Guidelines for Medico-Legal Care for Victims of Sexual Violence: Child Sexual Abuse (World Health Organisation, 2003) Accessed from: https://www.who.int/violence_injury_prevention/resources/publications/en/guidelines_chap7.pdf 25/05/2021

381 Glossary on Sexual Exploitation and Abuse (United Nations, 2017) Accessed from: https://hr.un.org/sites/hr.un.org/files/SEA%20Glossary%20%20%5BSecond%20Edition%20-%202017%5D%20-%20English_0.pdf 25/05/2021

382 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf 25/05/2021

383 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Interagency Working Group on Sexual Exploitation of Children, 2016) Accessed from: https://www.ecpat.org/wp-content/uploads/2016/12/Terminology-guidelines_ENG.pdf (23/07/2021)

384 Child Sexual Abuse Material (NCMEC) Accessed from: https://www.missingkids.org/theissues/csam 25/05/2021

385 IWF Annual Report: Glossary (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/selfgenerated 06/05/2021

386 Non-Photographic Visual Depictions (IWF, 2007) Accessed from: https://www.iwf.org.uk/what-we-do/who-we-are/consultations/non-photographic-visual-depictions 25/05/2021

387 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf 25/05/2021

388 Grooming (NSPCC) Accessed from: https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/ 25/05/2021

389 Online Enticement (NCMEC) Accessed from: https://www.missingkids.org/netsmartz/topics/onlineenticement 25/05/2021

390 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf 25/05/2021

391 What is a deepfake? Everything you need to know about the AI-powered fake media (Business Insider, 2021) Accessed from: https://www.businessinsider.com/what-is-deepfake?r=US&IR=T#:~:text=Recently%2C%20deepfake%20technology%20has%20been,with%20another%20in%20recorded%20video. 25/05/2021

392 Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic (Europol, 2020) Accessed from: https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic 26/01/2021

393 Working with Children and Young People Who Have Displayed Harmful Sexual Behaviour (Allardyce and Yates, 2020)

394 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (ECPAT, 2016) Accessed from: https://www.ohchr.org/Documents/Issues/Children/SR/TerminologyGuidelines_en.pdf 25/05/2021

395 IWF Annual Report: Glossary (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/selfgenerated 06/05/2021

396 Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children (United Nations, 2000) Accessed from: https://www.ohchr.org/en/professionalinterest/pages/protocoltraffickinginpersons.aspx

397 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: https://www.weprotect.org/issue/global-threat-assessment/ 25/01/2021

398 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: https://www.weprotect.org/issue/global-threat-assessment/ 25/01/2021

399 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: https://www.weprotect.org/issue/global-threat-assessment/ 25/01/2021

400 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: https://www.weprotect.org/issue/global-threat-assessment/ 25/01/2021

401 Global Threat Assessment 2019 (WePROTECT Global Alliance, 2019) Accessed from: https://www.weprotect.org/issue/global-threat-assessment/ 25/01/2021

402 Safer Technology, Safer Users: The UK as a world-leader in Safety Tech (UK Government, 2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/887349/Safer_technology__safer_users-_The_UK_as_a_world-leader_in_Safety_Tech.pdf 25/05/2021

403 Safety by Design (Australian eSafety Commissioner, 2019) Accessed from: https://www.esafety.gov.au/sites/default/files/2019-10/LOG%207%20-Document8b.pdf 25/05/2021

404 The Decentralised Web of Hate (Bevensee & Rebellious Data LLC, 2020) Accessed from: https://rebelliousdata.com/wp-content/uploads/2020/10/P2P-Hate-Report.pdf 25/05/2021

405 What is a VPN? – Virtual Private Network (Cisco) Accessed from: https://www.cisco.com/c/en_uk/products/security/vpn-endpoint-security-clients/what-is-vpn.html 25/05/2021

406 Hash Values: Fingerprinting Child Sexual Abuse Material (NetClean, 2018) Accessed from: https://www.netclean.com/2018/10/30/hash-values/ 25/05/2021

407 Hash Values: Fingerprinting Child Sexual Abuse Material (NetClean, 2018) Accessed from: https://www.netclean.com/2018/10/30/hash-values/ 25/05/2021

408 Use of AI in Online Content Moderation (Cambridge Consultants, 2019) Accessed from: https://www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf 25/05/2021

409 Darknet Cybercrime Threats to Southeast Asia (UNODC, 2020) Accessed from: https://www.unodc.org/documents/southeastasiaandpacific/Publications/2021/Darknet_Cybercrime_Threats_to_Southeast_Asia_report.pdf 25/05/2021

410 End-to-End Encryption (NSPCC, 2021) Accessed from: https://www.nspcc.org.uk/globalassets/documents/news/e2ee-pac-report-end-to-end-encryption.pdf 25/05/2021

411 IWF Annual Report: Glossary (IWF, 2021) Accessed from: https://annualreport2020.iwf.org.uk/trends/international/selfgenerated 06/05/2021

412 Metadata (WhatIs.com, 2021) Accessed from: https://whatis.techtarget.com/definition/metadata 24/06/2021

413 Tor (Investopedia, 2019) Accessed from: https://www.investopedia.com/terms/t/tor.asp 07/05/2021

414 Convention on the Rights of the Child (United Nations, 1989) Accessed from: https://www.ohchr.org/en/professionalinterest/pages/crc.aspx 25/05/2021

415 How we protect children's rights with the UN Convention on the Rights of the Child (UNICEF) Accessed from: https://www.ohchr.org/en/professionalinterest/pages/crc.aspx 25/05/2021

416 Explanatory Notes: General Comment no.25 on children's rights (5Rights Foundation, 2021) Accessed from: https://5rightsfoundation.com/uploads/ExplanatoryNotes_UNCRCGC25.pdf 25/05/2021

417 Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse (WePROTECT Global Alliance, 2020) Accessed from: https://www.weprotect.org/response/technology/ 25/05/2021

418 Preventing and Tackling Child Sexual Exploitation and Abuse: A Model National Response (WePROTECT Global Alliance, 2016) Accessed from: https://www.weprotect.org/wp-content/uploads/WePROTECT-Model-National-Response.pdf 25/05/2021

419 Lanzarote Convention (Council of Europe) Accessed from: https://www.coe.int/en/web/children/lanzarote-convention 25/05/2021

420 Glossary: E-privacy Directive 2009/136/EC (European Data Protetion Supervisor) Accessed from: https://edps.europa.eu/data-protection/data-protection/glossary/e_en#e-privacy_directive2009-136-ec 25/05/2021

421 The EU will continue to protect children from child sexual abuse online (European Commission, 2020) Accessed from: https://ec.europa.eu/home-affairs/news/20200910_eu-continue-protect-children-from-child-sexual-abuse-_en 25/05/2021

422 EU Kids Online 2020: Survey Results from 19 Countries (EU Kids Online, 2020) Accessed from: https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf

423 Production and distribution of child sexual abuse material by parental figures (Australian Institute of Criminology, 2021) Accessed from: https://www.aic.gov.au/sites/default/files/2021-02/ti616_production_and_distribution_of_child_sexual_abuse_material_by_parental_figures.pdf 28/05/2021

WeProtect Global Alliance brings together experts from government, the private sector and civil society.

We break down complex problems and develop policies and solutions to protect children from sexual abuse online.

WeProtect
GLOBAL ALLIANCE