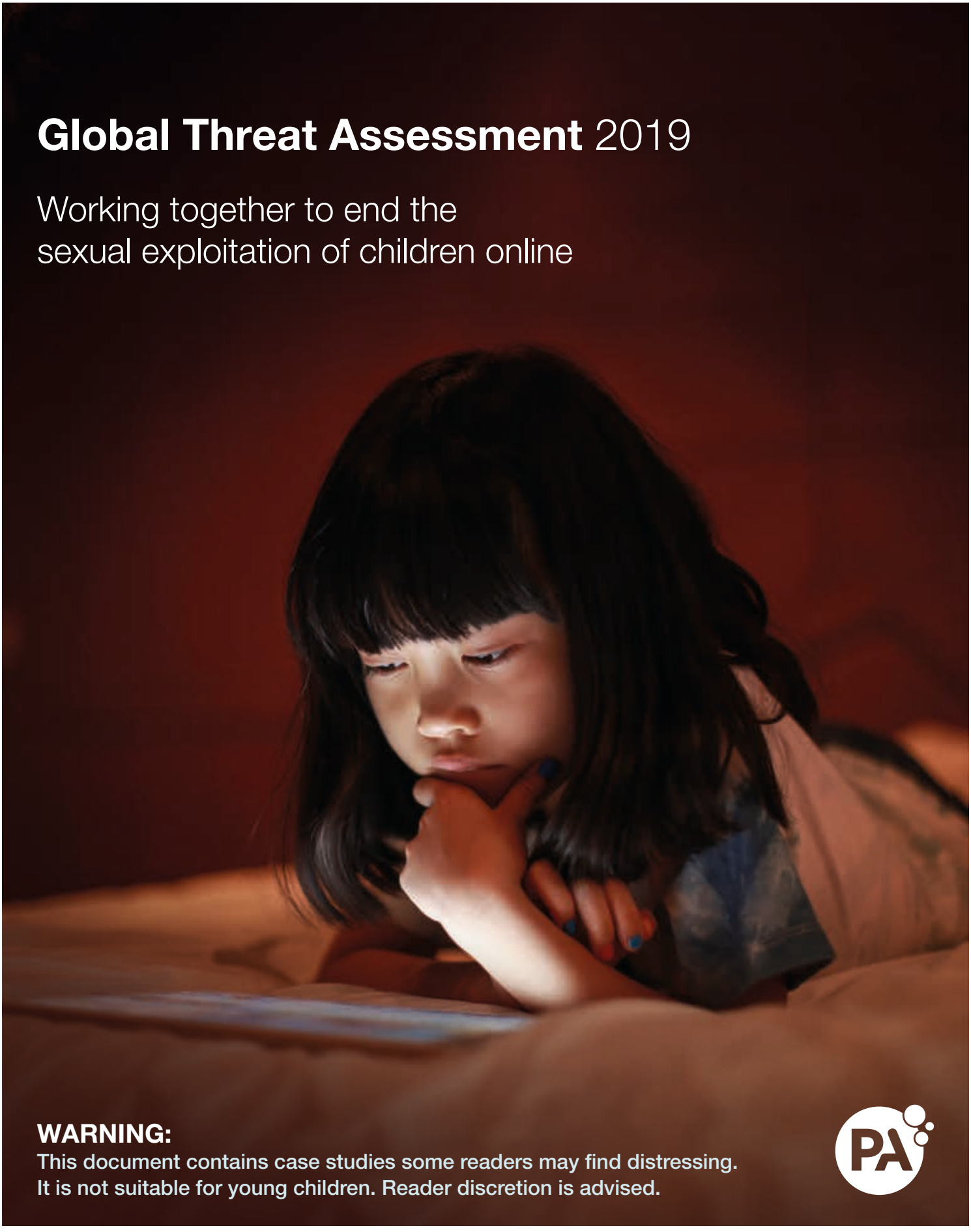
WePROTECT GLOBAL ALLIANCE

Global Threat Assessment 2019

Working together to end the sexual exploitation of children online



WARNING:
This document contains case studies some readers may find distressing.
It is not suitable for young children. Reader discretion is advised.

PA

Acknowledgements

The WePROTECT Global Alliance wish to thank the following organisations for providing specialist advice, and PA Consulting Group for researching and compiling this report:

Aarambh Foundation (India)
ECPAT International
eSafety Commissioner (Australia)
European Commission
Europol
International Justice Mission
Internet Watch Foundation
INTERPOL
National Center for Missing and Exploited Children (US)
National Crime Agency (UK)
The Global Partnership to End Violence Against Children
The Lucy Faithfull Foundation
UNICEF Ghana
US Department of Justice

Contents

01 Foreword

by Ernie Allen, Chair of WePROTECT Global Alliance

At our last Summit, co-hosted with the Global Partnership to End Violence Against Children and the government of Sweden in 2018, the WePROTECT Global Alliance published our inaugural Global Threat Assessment. It was the first of its kind, drawing together experts from across the Alliance to produce a global, publicly available analysis of the scale and nature of the threat facing children online, with the aim of strengthening our international response.

With the help of PA Consulting, who have generously supported the threat assessment pro bono, and the expertise and knowledge of our membership, we have built on these foundations and listened to your feedback. This next iteration of the threat assessment brings new insights into the nature of online child sexual abuse in the Global South and looks ahead to how technological innovation will impact the threat.

Our conclusions are sobering. We assess that the scale of the problem, both in absolute terms and in terms of reports to law enforcement and civil society, is increasing at an alarming rate. And behind every one of these cases there is a child who needs to be safeguarded and supported. This "tsunami" of cases is increasing the burden on every pillar of the WePROTECT Global Alliance: governments, law enforcement, civil society and the technology industry. As internet connectivity grows, particularly in the Global South, offenders are able to find and exploit new victims.

At the same time, we are facing reduced reporting as industry-applied encryption means that technology companies are increasingly unable to identify and flag malicious use of their own platforms. And we are experiencing a widening gap between those nations who have had the time to evolve sophisticated support services in step with their technical evolution and those who are leaping to technology parity faster than their preparations can keep pace. Anonymity and secure networking continue to enable offenders to establish safe spaces online, where they can network and spread tools and techniques to facilitate exploitation. As we develop our understanding of the methodology and motivations of offenders, and of the needs and impact of abuse on victims, it underlines the importance of prevention and protection – stopping the harm before it takes place. Conservative estimates of the financial impact of this crime run into the billions of dollars in terms of health, social services and impact on quality of life. There is an economic, operational and moral case to step up our response.

As more children come online around the world, and as the technology landscape changes and evolves, we now, more than ever, need a forum for collaboration, networking and action. WePROTECT Global Alliance offers a platform, a voice and a toolkit for its members to tackle online child sexual abuse at a global scale. Alongside this threat assessment we are also launching a Global Strategic Response, setting out a framework for action at transnational level, drawing on expert views. We will continue to fight to raise awareness, support action and ultimately put a stop to the sexual exploitation of our children online.

Ernie Allen
Chair, WePROTECT Global Alliance Board

Definitions and scope

The WePROTECT Global Alliance (WPGA) is an international movement dedicated to national and global action to end online child sexual exploitation (OCSE). Throughout this report we have adopted the following terms and abbreviations:

CSEA: Child Sexual Exploitation and Abuse (variously referred to by organisations as CSAE and CSE) is a form of child sexual abuse that occurs when an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity.

The victim may have been sexually exploited even if the sexual activity appears consensual. Child sexual exploitation does not always involve physical contact; it can occur through use of technology. [1]

The WPGA endorses the scope set out in the European Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, known as the 'Lanzarote Convention', which extends to cover all possible kinds of sexual offences against children, including the sexual abuse of a child, exploitation of children through prostitution, grooming and corruption of children through exposure to sexual content, and activities and offences related to child abuse material. The Convention covers sexual abuse within the child's family, or 'circle of trust', as well as acts carried out for commercial or profitmaking purposes. The Lanzarote Convention sets forth the following six criminal offences:

- Article 18: Sexual abuse
- Article 19: Child prostitution
- Article 20: Child pornography* [referred to in this report as Child Sexual Abuse Material]
- Article 21: Participation of a child in pornographic performances
- Article 22: Corruption of children
- Article 23: Solicitation of children for sexual purposes (also known as 'online grooming').

CSAM: While UN agencies and other international institutions describe indecent images and videos of children as 'child pornography', following the Interagency Terminology and Semantics Project completed in June 2016, the WPGA believes the phrase 'child sexual abuse material' (CSAM) accurately captures the heinous nature of sexual violence and exploitation of children while protecting the dignity of victims.

Global North and Global South:
To distinguish between differing levels of wealth and development amongst member countries, in this report we have used the term 'Global North' for the G8 countries, the United States, Canada, all member states of the European Union, Israel, Japan, Singapore, South Korea, as well as Australia, New Zealand and four of the five permanent members of the United Nations Security Council, excluding China. The 'Global South' is made up of Africa, Latin America, the Middle East and developing Asia. It includes three of the four newly advanced economies of the BRIC countries (excluding Russia), which are Brazil, India and China.

This report uses the terms offender and perpetrator interchangeably to denote those who commit online child sexual exploitation and abuse.

We have also used the following terms to define different hosting arrangements for online services:

- the **Surface Web** is the portion of the web readily available to the general public and searchable with standard web search engines
- the **Deep Web** is the portion 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 URL or IP address, and may require password or other security access beyond the public website page
- the **Dark Web** (also referred to as the Dark Net) is a disputed term, but is understood by most authorities, and within this report, as a 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), which 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.

02 Aims of the Global Threat Assessment

The inaugural Global Threat Assessment (GTA) was published in February 2018 and launched at the 2030 Agenda for Children: End Violence Solutions Summit in Stockholm, Sweden. It was the first report of its kind – a global, comprehensive view of technological change, victim vulnerability, offender behaviour and the intersection point at which child sexual exploitation and abuse (CSEA) is most prevalent.

The central conclusion of GTA18 was that "technology is permitting offender communities to attain unprecedented levels of organisation, which in turn creates new and persistent threats as these individuals and groups exploit online 'safe havens' and 'on-demand' access to victims".[2]

This evidence-based discovery served as a call to arms for national governments to redouble their efforts to find new and innovative ways of countering this threat to the most vulnerable in our societies. Their response includes the deployment of sophisticated intelligence capabilities to disrupt the most dangerous offender communities, improved educational and support resources, and new legislative and regulatory measures that improve oversight of technology companies and make clear their responsibilities to keep children safer online through robust action to counter illegal content and activity.

90 countries already members of the WePROTECT Global Alliance

22 of the biggest names in the global technology industry

26 leading international and non-governmental organisations

This year's report has been commissioned with the assistance and expertise of the WePROTECT Global Alliance board members and sets out to build on the wide-reaching success and impact of GTA18. Its purpose is to demonstrate the nature, scale and complexity of online child sexual exploitation (OCSE) in order to support a broad mobilisation – compelling nation states, the global technology industry and the third sector to find new ways of working together to combat this rapidly evolving threat. The WePROTECT Model National Response provides guidance and support to countries and organisations to help them build their response to OCSE.

The assessment considers the same key lenses as GTA18 and retains the same aims, as listed below, focusing on and providing a deeper understanding of each theme. Our goal is to provide a more global perspective on the threat, taking account of different contexts and cultural perspectives beyond the predominantly North American and Western European data and case studies used in our first report. This report sets out to:

- raise further international awareness and understanding of OCSE
- provide a greater understanding of the threat and how it is evolving
- enable a better understanding of the impact on victims and the wider societal impact
- benchmark progress against GTA18 to monitor changes in the nature and scale of the threat, as well as the positive impact that interventions are having
- provide recent case studies to support members in prioritising individual and collective investment decisions and interventions.

Methodology

This report is a meta study, which combines the results from multiple international studies in an effort to increase the power and impact of the individual reports, improve estimates of the scale of OCSE globally, and make an assessment when reports disagree. This secondary research is reinforced by primary research from operational case studies provided by WePROTECT member organisations.

Key data points

18.4 million referrals of child sexual abuse material (CSAM) by US technology companies to the National Center for Missing and Exploited Children (NCMEC) in 2018[3]

2/3 of the total 18.4 million referrals to NCMEC originated in messaging services, at risk of disappearing if end-to-end encryption is implemented[4]

13.3 million+ suspicious images processed by the Canadian Centre for Child Protection (Project Arachnid) have been triggered for analyst review, resulting in 4.6 million takedown notices sent to providers[5]

94% of CSAM material found online by the Internet Watch Foundation (IWF) contains images of children aged 13 or under

39% of CSAM material found online by the IWF contains images of children aged ten or under[6]

46 million unique images or videos relating to CSAM in EUROPOL's repository[7]

750,000 individuals estimated to be looking to connect with children across the globe for sexual purposes online at any one time.[8]

03 Summary conclusions

Emerging trends signal a 'tsunami' of growth in OCSE, leaving ever more victims and survivors in its wake

The scale, severity and complexity of online CSEA is increasing at a faster pace than those aiming to tackle the activity can respond, with referrals from industry and law enforcement partners reaching record highs.[9] This creates an urgent need for governments, law enforcement organisations, the technology industry and third sector organisations to work together to step up their collective response.

The practical impediment to closer international collaboration, sharing and learning is the fragmented nature of each nation's online safety response, typically spanning policing, social services, regulation and education.

The rapid global proliferation of mobile device ownership and internet access is creating an asymmetry between the Global North and South. All nations are equally challenged by the rapid evolution of technology, but entry into the digital world is different between those societies who have adopted internet services progressively while learning to protect their infrastructure and citizens online, and those who instantaneously receive the finished product without the time to develop and evolve their educational and support services, law enforcement and regulatory responses. The chain of response is only as strong as its weakest link. As one INTERPOL investigator described it:

> "It's like the difference between cautiously entering a swimming pool from the shallow end, with the tools and education to learn how to swim, and being thrown in at the deep end.[10]"

The growing availability of advanced anonymisation tools and end-to-end encryption peer-to-peer (P2P) file-sharing networks is enabling offenders to have easier, more secure access both to vulnerable children and to the networks of people who share a sexual interest in children. There appears to be a link between large-scale membership of these online 'safe-havens' (the UK's National Crime Agency has identified 2.88 million registered accounts across the ten most harmful Dark Web sites) and the growing commodification and industrialisation of child sexual abuse material (CSAM).[11]

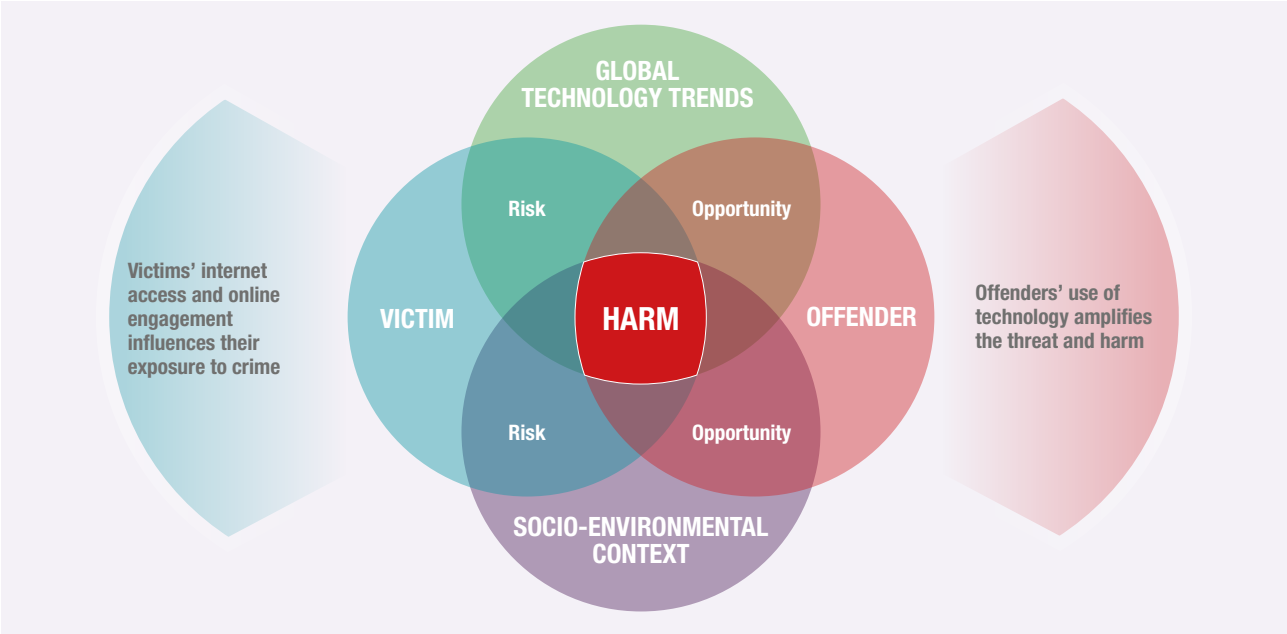
At the same time, increasing device ownership and unsupervised internet access by children increases their exposure to the risk of exploitation and abuse online. This is compounded by their maturity levels, limited understanding of online risks, and changing attitudes to online behaviour, with one in four teens having received sexually explicit texts and emails, and one in seven having sent them.[12]

There is an expanding sphere of harm in which the proliferation of indecent images and videos of children online is fast exceeding the capacity of organisations charged with the proactive identification and removal of this material. The following chapters present evidence that these threats and challenges will continue to grow without decisive, collective action.

Last year's inaugural Global Threat Assessment identified the damaging convergence of four elements that have the greatest influence on the sphere of harm and help explain the increase in online CSEA:

- global technology trends;
- changing offender behaviours;
- victims' online exposure;
- the socio-environmental context.

Figure 1: Four lenses create the sphere of harm: technology, offenders, victims and socio-environmental factors



Fresh global research and new case studies have validated our previous conclusions and highlighted new factors contributing to an expanding sphere of harm. Collectively, these signal a tsunami of growth in online CSEA, and an equal increase in potential victims who need safeguarding and survivors who need appropriate support.

A summary of the four lenses discussed in this report and in Figure 1 are outlined below.

1. Global technology trends: the industrialisation of secure online services

GTA18 highlighted the emergence of offender communities using Dark Web services to share images and tips for grooming children and evading detection.[13] These persist, and are amplified by the industrialisation of easily accessible, 'consumer-ready' Surface Web services that enable greater privacy, security and anonymity. These include secure P2P file-sharing networks, hosting services which disguise CSAM on mainstream websites, and mobile payment services and messaging services that bypass the need for registration and identification.

2. Offender behaviours: the vicious cycle

Our understanding of offender pathways needs further analysis and academic study. Not all offenders will gravitate towards web forums; not all who view CSAM online will manipulate or coerce children to engage in sexually explicit conduct; and not all offenders who commission the live streaming of 'on-demand' abuse will escalate to directly abusing a child in person. Online abuse, through its physical distance from the victim, can heighten the risk of offender deviancy, and there are indications that those joining online 'special interest groups' are encouraged to greater violence and younger children in a quest for status within their offender community.[14]

3. Victim vulnerability: normalisation of risky online behaviour

Young people are increasingly vulnerable to harmful online interactions as a result of a continuing reduction in the age at which they have access to devices and unsupervised access to social media and online gaming. A concerning trend is the normalisation of sexual behaviour online, with large numbers (and a falling age-range) of children sharing self-generated indecent images (SGII), whether through deception and coercion, consensual online activity with an age-appropriate peer, or for social affirmation. This increases the volume of material available to offenders and increases children's vulnerability to exploitation and abuse by adults as well as cyberbullying by other children. There are cases of organised criminals or scammers targeting children to acquire sexualised images and videos, and of contact offenders sharing CSAM more rapidly and widely than before.[15]

4. The socio-environmental context: the leap to technology parity

There were 367 million new internet users globally in the 12 months to January 2019, of which INTERPOL estimates that 1.8 million men with a sexual interest in children are newly online (noting that not all will become sexual offenders).[16] Entry into the digital world is different between those societies who have adopted internet services progressively and those who are leaping to technology parity, who are receiving the full spectrum of internet services instantaneously without the time to evolve their educational and support arrangements, law enforcement or regulatory responses to match. It is noteworthy that, since GTA18, the Broadband Commission for Sustainable Development's work and global influence has placed a greater emphasis on OCSE.[17]

Growth since GTA18

367 million new internet users, a 9% increase[18]

122 million more children have come online, based on UNICEF estimates that 1 in 3 internet users is a child[19]

80% increase in CSAM-related reports to the INHOPE global network of hotlines[20]

100% increase in the number of photos of children being sexually abused reported by tech companies[21]

33% increase in URLs containing CSAM removed by the Internet Watch Foundation.[22]

04 Technology trends

Increased online access, new technology and the rise of 'encryption by default' are fuelling offending rates

The number of mobile devices and internet users continues to grow. There are over five billion unique mobile users and over four billion internet users in the world today, representing a 2% and 9% increase respectively since 2018. There has also been a 9% increase in the number of social media users, to 3.5 billion.[23]

Increasing mobile internet access is facilitating greater use of online gaming, cashless payments, e-commerce and Internet of Things (IOT), devices such as baby monitors, internet-connected toys and webcam-enabled devices. These products are becoming cheaper and longer-lasting, with second-hand devices becoming more accessible to low-income consumers in developing nations.

These developments are enabling nations in the Global South to achieve technology parity with the Global North. Whilst the North has experienced a comparatively gentle evolution of domestic internet and mobile technologies over the past two decades, nations of the South are moving rapidly from limited access to reliable, high-speed internet services and to 4G and 5G mobile networks, bypassing the need to establish costly fixed-line and broadband infrastructure.

The number of absolute users in India grew by around 100 million (21%) over the last year. For internet growth relative to population size, eight of the top ten countries were African countries. Djibouti, Tanzania, Niger and Afghanistan each more than doubled their number of internet users compared with the previous year. In fact, of the top 20 countries for relative internet growth last year, 19 were from the Global South.[24]

The WePROTECT Model National Response provides a valuable framework for these nations to assess their capabilities to fight OCSE.

An estimated 1.8 million new male internet users over the last year have a sexual interest in children

A consequence of this rapid growth in device and internet access is the proportionate increase in the number of adults with a sexual interest in children who are now online, and in the number of children at risk of exposure to these individuals through unsupervised online interactions.

Figure 2: Digital growth Jan 2018 – Jan 2019[25]

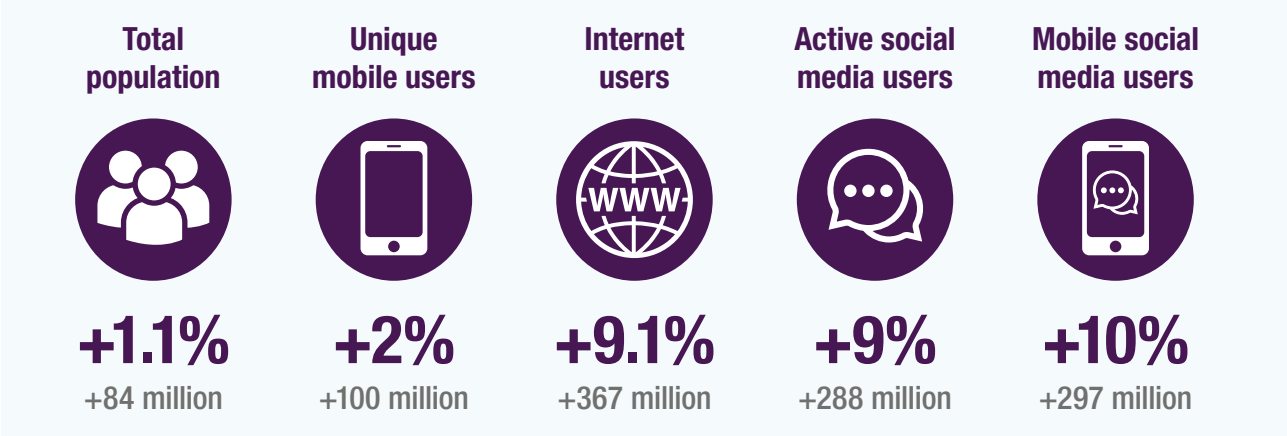
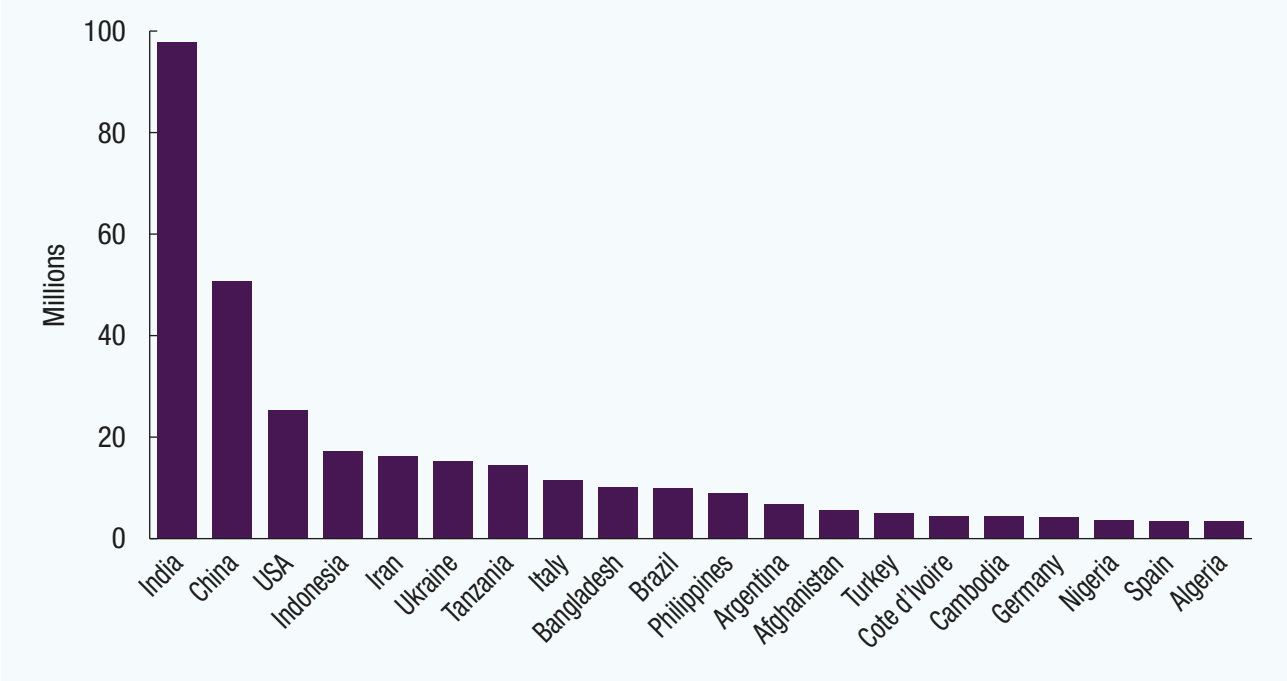


Figure 3: 20 countries with highest rate of absolute internet growth (2018-19)



Based on academic estimates that 1% of the male population is predisposed to a sexual interest in pre-pubescent children, INTERPOL estimates that there are likely to be approximately 1.8 million more men in this category using the internet now compared with a year ago (assuming a 50:50 male to female adoption ratio).[26] This is a conservative estimate, since the 1% estimate refers only to paedophiles with a sexual interest in pre-pubescent children. Other studies estimate that 2.2-4.4% of adult men have knowingly viewed CSAM of pre-pubescent children online.[27]

With a large proportion of the increase in internet access coming from the Global South, the risk these 'new entrants' represent is magnified by a general lack of coordinated online safety education and less developed police and child protective services, meaning more children are falling victims to offenders and are not receiving safeguarding support.

Technology is creating lower barriers to entry for OCSE

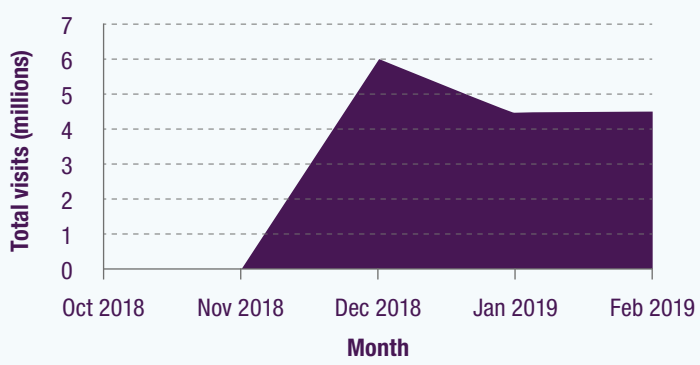
In 2018, US technology companies (with global users) reported over 45 million online photos and videos of children being sexually abused — more than double what they found the previous year.[28]

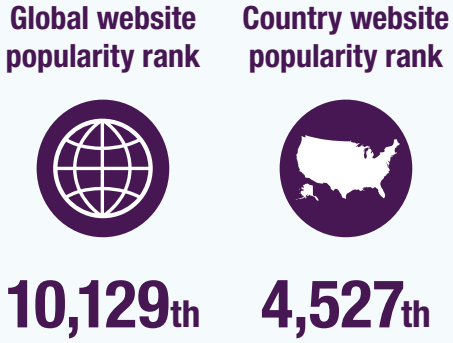
The level of availability of CSAM is significant, and websites hosting this material can be set up and accessed faster than they can be identified and taken down. Between 2014 and 2018, the number of child sex abuse URLs removed per annum has more than tripled, rising from from 31,226 to 105,047 in 2018. Between 1996 and 2019 the UK's Internet Watch Foundation (IWF) has removed almost half a million webpages showing child sex abuse.[29]

One CSAM-hosting website received 6.5 million views in its first month of operation

INTERPOL identified a website on the surface web that, from its appearance in November 2018, received 6.5 million views in its first month of operation, stabilising at 4.67 million views per month. In February 2019 it was ranked as the 4,527th most popular website in the USA and the 10,129th most popular website globally.[30]

Figure 4: Traffic Overview of popular CSAM-hosting website (February 2019)





Our 2018 Global Threat Assessment highlighted similar websites on the Dark Web with around one million visitors.[31]

On the Dark Web, offenders can pursue more niche material. In 2018, 2.88 million accounts were registered globally across the ten most harmful CSEA Dark Web sites.[32] The Dark Web can amplify existing offender behaviours, with these perceived 'safe havens' enabling offenders to discuss their sexual interests more freely and share more extreme images. However, the use of Dark Web and Surface Web activity is not binary, with Canadian authorities noticing large compilations of material encrypted and stored in file-lockers on the Surface Web, and their links shared on Dark Web forums.[33]

The rise of encryption

We tend to associate the Dark Web as an online environment that supports attributes such as anonymity, encryption and security from detection with its use for concealing criminal activity. With the Surface Web, we tend to think of ease of access and general availability of mainstream consumer services. The impact of the end-to-end encryption of popular, mainstream social media and messaging services, when coupled with weak registration and the use of 'Virtual Private Networks' (VPNs) is creating a hybrid environment with the most favourable attributes for offenders, where users can apply Dark Web standard security and anonymity to their Surface Web interactions.

Europol Internet Organised Crime Threat Assessment (IOCTA) states that the majority of CSAM is still shared via P2P file-sharing-networks[34]. Publicly-accessible social media and communications platforms remain the most common methods for meeting and grooming children online. In 2018, Facebook Messenger was responsible for nearly 12 million of the 18.4 million worldwide reports of CSAM.[35] These reports risk disappearing if end-to-end encryption is implemented by default, since current tools used to detect CSAM do not work in end-to-end encrypted environments. In addition, P2P file-sharing networks provide a cloak of cover for perpetrators to access and share CSAM.[36]

The growth of 'encryption by default' is further enabling Surface Web offending, with increased public awareness of online security risks and the desire to protect the privacy of private communications leading many e-mail and messaging service providers towards default encryption. This enables more offenders, including those who are less technically aware, to share CSAM, tips and tradecraft securely and anonymously. WhatsApp, which provides users with end-to-end encryption, was the most popular messaging service in 133 countries and territories in 2018.[37]

As more mainstream services move towards end-to-end encryption or provide ephemeral services (such as auto-deleting messages and images), government leaders are urging their industry counterparts to ensure that online

privacy and security does not come at the expense of making us more vulnerable in the real world. There is an ongoing public debate on protecting users' privacy and protecting people, particularly children and vulnerable adults, from criminal harm.

Child's Play Dark Web forum

An American and a Canadian offender were arrested for running two of the largest dark web sites for CSAM, called 'Child's Play' and 'Giftbox', in 2017. At their peak, these sites had over one million user profiles registered (users may have more than one registered profile each), with posts of the most serious category of abuse being viewed over 770,000 times.

Following a joint investigation by US, Canadian, Australian and European police forces, supported by the NCA Joint Operations Team, two offenders were arrested in Virginia, USA after the Canadian offender travelled to meet their American counter-part. Upon arrest and questioning, the offenders provided law enforcement with the site's usernames, passwords and encryption keys.

With permission from European police partners, the passwords and servers were passed to an Australian law enforcement agency. They continued to run Child's Play under legal authority in Australia, with an officer acting as the site administrator. The evidence gathered resulted in a dozen children being identified and rescued in Canada alone, over 100 victim cases referred globally and with one country identifying approximately 900 suspects.

The two offenders were both sentenced to 35 years for administering a child exploitation enterprise, having both been sentenced to life imprisonment in 2017 for the rape of a minor.[38]

The world's most popular messenger apps

WhatsApp
The most used messaging app in the world, with end-to-end encryption by default

Facebook Messenger
Facebook's separate messaging app allows users to share files, location, and to send money in some markets. Expected to incorporate end-to-end conversation

WeChat
The most popular app in China with more than one billion users; enables photo sharing, video and voice calls, location sharing, digital payments and games. This app employs transport encryption so that the message is encrypted between the user and WeChat's servers

Viber
More than one billion users; encrypted messaging and self-destructing chats available

Line
Very popular in Asia, boasting over 600 million users. Calls to landlines, and free line-to-line video or voice calls. Supports encrypted chats

Telegram
Millions of active users and highly secure encrypted chats[39]

End-to-end encryption creates a risk to children as it prevent online platforms and their moderators from identifying, removing and reporting harmful content from critical parts of their own networks. However, many service providers appear to be accelerating their implementation of end-to-end encryption and applying additional technology that also encrypts the name of the website that a perpetrator is requesting.[40] Protocol technology (referred to as domain name system (DNS) over HTTPS, or 'DoH') works by taking a domain name that a user has typed in their browser and sending a query to a DNS server to learn the numerical IP address of the web server that hosts that specific site. This is how normal DNS works too. However, DoH takes the DNS query and sends it to a DoH-compatible DNS server (resolver) via an encrypted HTTPS connection, rather than plaintext. This way, DoH hides DNS queries inside regular HTTPS traffic, so third-party observers will not be able to monitor traffic and tell what DNS queries users have run and infer what websites they are about to access. This could impact existing mechanisms for blocking web addresses that host CSAM and render parental or school web filtering ineffective. The technology world is still debating the advantages and disadvantages, but DoH has already been implemented in at least one leading web browser, with plans to roll it out as 'default' in the US, and other browsers are making similar plans.

While Surface Web applications offer CSAM access to low-tech offenders, the Dark Web is attractive to more sophisticated offenders and those seeking to use extra measures to attempt to evade detection. These services can only be accessed via secure 'overlay networks' which require special software to access. These may include virtual private networks (VPN), P2P networks and the so-called 'onion router' method used by Tor, where user data is encrypted and then transferred through different relays to create multi-layered encryption – protecting the identity and location of the user.[41] The US Department of Justice (DoJ) indicates that Dark Web sites are growing at a rate of 40,000 users per month, remaining in place for several years.

The "devastating consequences" for children of encryption

Last year, law enforcement authorities in the EU received more than 600,000 reports of instances of OCSE.

The rescue of a nine-year-old girl abused by her father for more than a year, and of 11 children exploited by a network of abusers, are just two examples of EU law enforcement cases dealt with on a daily basis.

The EU Commissioner for Home Affairs has warned of the devastating consequences for children in the EU if messaging applications are encrypted and law enforcement agencies no longer receive the reports they currently do.[42]

In line with the increase in internet adoption in the Global South, there has been a corresponding increase in the usage of these techniques. The Tor Project website states that users from the USA, Russia, Germany, France, UK, Ukraine and the Netherlands make up over half (~55%) of Tor users. However, for the past two years the proportion of users from Iran, Indonesia and India has increased by 14%.[43] It is worth noting that these figures represent total Tor growth, which can be used for both unlawful and legitimate purposes, including human rights activism and freedom of expression.

Hiding in plain sight

Offenders continuously seek new ways to share CSAM without being detected by law enforcement, such as 'disguised websites' using advanced hosting techniques to allow CSAM-hosting sites to hide in plain sight. The same website that reveals legal images to the casual user (or investigator) opening the website URL will reveal CSAM to a user who has visited a particular sequence of sites on their way to the target site. The correct string of cookies acts as the key to unlock the disguised content once the offender completes the sequence.[44]

The term 'sovereign-less' relates to data sovereignty: the idea that data is subject to the laws and governance structures within the nation in which it is collected. Sovereign-less services span national boundaries and have been intentionally designed to operate outside of one clearly defined jurisdiction. This enables offenders to produce material in one jurisdiction and host it in another for consumers in a third location, which makes it almost impossible for national governments and law enforcement organisations to enact national warrants or notices without sophisticated international co-operation.

Sovereign-less apps

The US Department of Justice (DoJ) has attempted to identify and safeguard a minor who is being coerced into self-producing indecent imagery for a group of offenders, using a popular social media and messaging app.

This app is 'sovereign-less by design' and the company promotes the fact that it has never provided information to any government. The US DoJ attempted to contact the company via several channels, seeking only user information in the hopes of identifying the victim.

All attempts to date have failed, with the subpoena being returned to sender.[45]

A further challenge for law enforcement is the use of Content Delivery Networks (CDNs) or 'passthrough services' that copy the pages of a website to a network of servers that are dispersed at geographically different locations. When a user requests a webpage that is part of a CDN, it redirects the request from the originating site's server to a server in the CDN closest to the user and delivers the content. The process of bouncing through CDNs is nearly invisible to the user. The only way a user would know if a CDN has been accessed is if the delivered URL is different than the URL that has been requested.

New types of tech-enabled offending

Online CSAM is being shared in a multitude of ways that were either unavailable or not widely available a few years ago. The live-streaming of abuse, 'abuse-to-order' and SGII are some such examples, as is the presence of material on distributed ledger systems. The advent of encryption, alternate, mixed, virtual and augmented reality, and the decentralisation of the web are already impacting on the production of CSAM and how material is spread and consumed.

Two percent of complaints received to the Republic of Ireland's INHOPE hotline, in 2018 concerned 'virtual child sex abuse imagery',[46] whilst researchers in Germany found 274 links to child abuse content contained within Bitcoin's blockchain.[47]

Technology has also increasingly enabled abusers to live stream 'in the room' contact abuse internationally, with most taking place in the Philippines.[48] In nations of the Global South, with higher levels of poverty and large numbers of vulnerable children, the risks associated with the combination of rapid adoption of high-speed internet connectivity and availability of relatively cheap connected devices are heightened.

One of the biggest concerns with live streaming is the difficulty of detecting and policing the 'live act'. This is due to the challenge of intercepting the encrypted content of private communications channels that cross international borders, and the undesirability – from a public privacy and civil liberties perspective – of authorising untargeted intrusion. This has resulted in growing calls from both service providers and governments for better regulation of services facilitating the live streaming of unlawful content.

The strongest opportunity to identify offenders and safeguard victims occurs in the phase when the offender is negotiating their access to a vulnerable child (approaching and setting up the transaction with families and individuals facilitating this kind of abuse); and when the images or recordings are captured and subsequently shared via online portals and web forums.

Abuse live streamed around the world

A joint investigation involving law enforcement agencies in Australia, Germany, the Philippines and the US resulted in the arrest of a number of offenders for involvement in the production and distribution of CSAM. One offender from Australia was found to be directing live streams of children being abused by a woman. The children's mother was found to have been conducting sexual abuse of her three daughters in cyber shows for several years. The woman had received and collected money transfers from viewers at local money remittance agencies using two different identities.

After being rescued by law enforcement, one of the minors identified a photo of another Australian online offender, leading to an outgoing referral to the Australian authorities and the arrests of offenders in Australia and Germany. With each new investigation developing further leads, a referral loop developed between Australia to the Philippines, Philippines back to Australia, and Philippines to Germany, and this continues to generate further leads. This demonstrates the value of the 'investigation-referral-investigation' cycles, and the benefits of intelligence sharing with international partner law enforcement agencies[49]

Mobile payment systems bypass the need for registration and identity verification

Technology-enabled techniques to pay to access CSAM continue to evolve. While successful interventions by financial coalitions have seen the amount of imagery paid for by bank or credit cards decrease, online payment services, money transfer services and local payment centres are now frequently used.

A popular payment method is the Informal Value Transfer System (IVTS) which uses mobile phones without the need for a credit card or even a bank account. Money can be collected with only a mobile phone number and a reference number, so formal registration and identification is not required.[50] Offenders are also early-adopters of developing technologies, such as cryptocurrencies, to covertly access and share CSAM. In July 2018, Bulgarian police forces arrested eight suspects involved in the dissemination of CSAM. The criminals used Bitcoin to pay for the hosting of a website specifically created to upload pictures and videos of child sexual abuse.[51]

More recently, law enforcement agencies have seen the growth of online marketplaces hosting and trading CSAM on the Dark Web. To gain access, users need to pay a sum of money or provide new 'first-generation' CSAM.[52]

Technology is both an enabler for harm and integral to the solution

Technology does not just enable the growing prevalence of CSAM, but also enables law enforcement, the technology industry and third sector organisations to identify, report and prevent it, and to identify and locate victims and offenders.

Innovative investigative techniques such as artificial intelligence (AI), tracking, website prevention and image-blocking can all be deployed to protect children online. For example, EUROPOL's 'Trace an Object' campaign, launched in May 2017, used the crowd-sourcing of social knowledge to identify objects taken from the background of an image with sexually explicit material involving minors.[53] Tracing a victim by their image alone is challenging. However, CSAM often contains identifiable objects in the background, from consumer products to furniture and distinct building characteristics, which can prove invaluable in narrowing down the location of the abuse and safeguarding the victim.

The view of the USA, Canada, UK, Australia and New Zealand

In a meeting this year, senior Ministers from Australia, Canada, New Zealand, the United Kingdom and the United States were united in their belief that technology firms should not develop systems and services in ways that empower criminals or put vulnerable people at risk. Instead, technology companies should prioritise the protection of their users and the wider public when designing services.

The participants agreed that tackling the epidemic of online child sexual exploitation requires an immediate upscaling of the global response to ensure that all children across the globe are protected, and that there is no safe space online for offenders to operate.[54]

05 Changing offender behaviours

Heightened technical sophistication is driving offending rates, escalating abuse and making investigations more difficult

Globally, there are still gaps in the understanding of the causes and origins of sexually abusive behaviour, with much research emanating from the Global North. We understand the pathway of offending for those with a sexual interest in children far less than the online harm caused by the distribution of terrorism-related and extremist content online.

Years of study have allowed psychologists to determine how vulnerable people are radicalised into extremist ideologies, and to implement steps which help to prevent their escalation and encourage the radicalised to desist and disengage. But it remains unclear whether equivalent techniques can be adapted to dissuade people from first time child sexual offending, from viewing CSAM, and from inciting or conducting 'in-person' contact abuse.

A study into adult sexual offending more generally, prepared by the US Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering and Tracking (SMART), found that the problem of sexual offending behaviour is too complex to attribute solely to a single theory.[55] Multifactor theories provide greater insight into the causes of sexual offending.

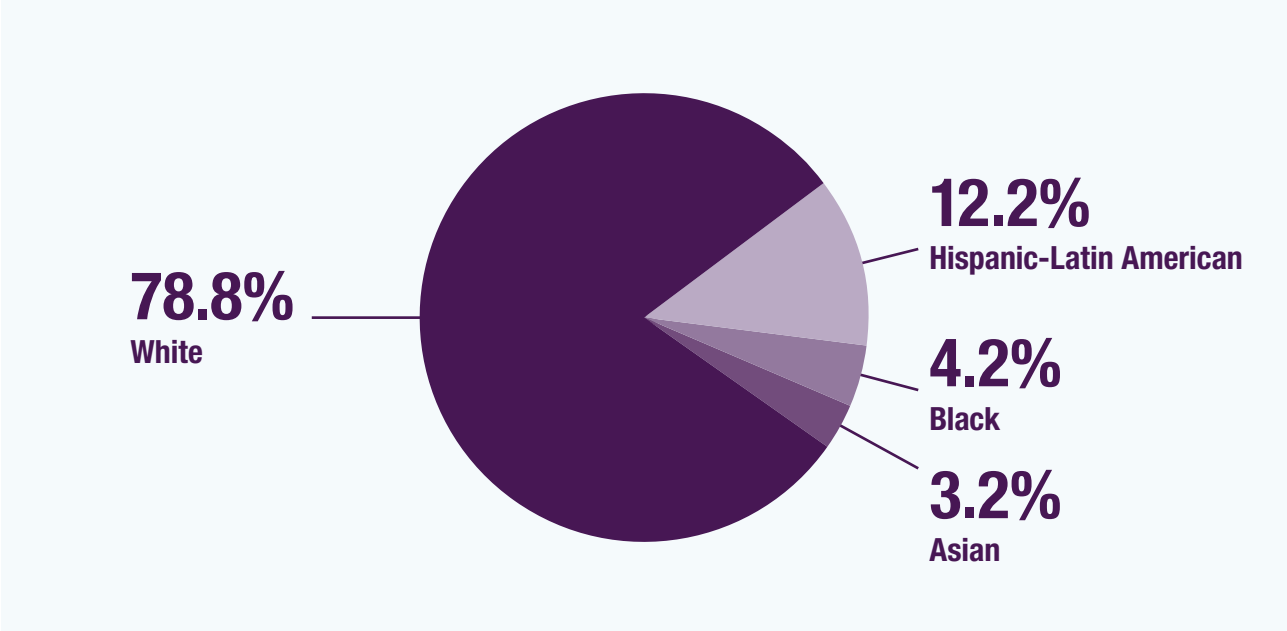
What is known:

- not all persons with a sexual interest in children offend (noting that conducting in-person contact abuse; coercing the production of online sexual activity; and viewing online images are all offences)
- not all offenders are paedophiles (a sexual orientation in adults and late adolescents who direct sexual or erotic feelings or desires towards prepubescent children). Hebephiles display adult sexual attraction primarily toward pubescents. Both categories should be distinguished from those with paedophile or hebephile disorders, who are sexually violent towards children
- negative or adverse conditions in early development – particularly poor relationships with caregivers – can contribute to the behaviour

While the number of OCSE cases is growing, this is in part due to the increasingly sophisticated methods that nations and internet service providers (ISPs) now have at their disposal to identify and remove CSAM and target the offenders. And this is helping to build a better understanding of the offender profile.

GTA18 concluded that offenders may come from any age, race, sex, occupation, socio-economic status or geographical area. Subsequent analysis of data from INTERPOL's International Child Sexual Exploitation (ICSE) image and video database indicates that 92.7% of offenders were male, female offenders were most frequently depicted together with a male offender, most victims were the same ethnicity as their abuser, and the majority (78.8%) of offenders were white (noting that it impossible to determine offender ethnicity in more than 75% of cases, and low proportions of some ethnic groups may reflect the current geographical scope of countries connected to the ICSE database).[56]

Figure 5: Ethnicity of visible offenders[57]



INTERPOL and ECPAT's joint research on unidentified victims in CSAM recommended developing comprehensive frameworks for more reliable categorisations of victim and offender characteristics, such as ethnicity, across regions and countries.

We are also witnessing a younger generation of offenders emerging. They have grown up with technology and are therefore more familiar and comfortable using IT. This results in a set of perpetrators who are more likely to be able to identify and exploit advanced security techniques and services to evade detection.

In Queensland, Australia, a study released in 2018 stated that almost half of the 3,035 offenders handled by the criminal justice system for CSAM were themselves children under the age of 17, with the number of young offenders cautioned for possessing SGII increasing more than tenfold between 2006 and 2016.[58]

Additionally, this generation is less likely to report sexual images of children, with the IWF's recent '#SoSockingSimple' campaign highlighting the lack of awareness and understanding amongst young adult males that viewing CSAM is illegal and should be reported.[59]

The UK National Crime Agency's (NCA) 2019 National Strategic Assessment identifies the main driver of OCSE as sexual gratification. Others seek to gain financially by selling CSAM (particularly live streamed abuse) online or by monetising CSEA-related internet traffic through 'pay-per-click' advertising.[60] Live streamed abuse for commercial purposes is a growing threat; for as little as €10-20 offenders can orchestrate the abuse, in real time, against a child of their choice.[61] And for some, CSAM is used as a form of currency within child abuse networks. Abusers use material to gain notoriety or to 'trade' for new, unseen photos and videos.

Most offenders can still be classified as highly secretive and private lone actors. However, the creation of perceived digital 'safe havens' is leading to an increasing tendency for offenders to congregate in Dark Web forums and online service provider platforms that offer encrypted messaging and streaming. Here, offenders are not just viewing images. They are actively targeting children globally via commercial platforms to manipulate and extort explicit imagery or to gain face-to-face access.

Moreover, the widespread availability of CSAM on the Surface Web lowers the bar to being able to offend. Such communities normalise offenders' behaviour, provide encouragement and validation, and enable offenders to share and learn tradecraft, thus decreasing the likelihood that individuals will seek help and increasing the chances of their offending escalating. The lack of deterrence and support services may also play a role, as some of those with a sexual interest in children may not know how to seek help even if they want to.

Potential escalation paths

In law, distinctions are typically drawn between those who collect CSAM for personal collections and those who actively acquire and share it, and also between those who conduct 'in-person' contact abuse and those whose acts of child abuse are perpetrated exclusively online.

These distinctions are important, as they indicate a possible escalation path from, for example, those who source and view pre-existing images to those who manipulate or coerce children to engage in sexually explicit conduct on their own webcams (including contact abuse by 'self-touch' or between two victims); and from those who pay to direct and observe abuse perpetrated by an 'in-the-room' offender to those who conduct in-person contact abuse themselves.

However, escalation is not inevitable, so there are many opportunities for interventions to prevent or dissuade those who Europol describes as 'simple viewers', allowing law enforcement organisations to focus on the most serious and serial offenders. According to UNICEF, most online offenders without a history of contact offenses are unlikely to cross over into contact offences within one to five years after their first offence.[62] But there is also a growing understanding that online abuse enables a higher risk of deviancy, as offender behaviour is less constrained by fears of detection or identification.[63]

Changing offender pathways

A number of NCA cases demonstrate how technology is changing the ways in which some offenders commit abuse, the depravity of the abuse, and the offender pathway itself.

In one case, an offender joined an online, private discussion group for people with a sexual interest in children. New members had to post brand new abuse images, resulting in the offender raping a six-month-old girl, sexually assaulting a two-year-old boy, uploading the footage onto an encrypted app and sharing it through a popular file sharing site.[64]

In another case, an offender was sending money to known facilitators of live-streamed child sex abuse in the Philippines and was arrested upon his return to the UK. Forensic analysis showed the offender had sent at least 15 money transfers to facilitators between August 2017 and June 2018, and found images of child abuse on his phone.[65]

Another offender was imprisoned in February 2018 for 25 years after pleading guilty to 137 offences relating to 300 victims of sadistic 'hurt core material' on the Dark Web. The offender gained access to children online by coercing and blackmailing them through open forums and e-commerce sites, before moving conversations onto secure and encrypted platforms to conduct sextortion and blackmail. The offender forced victims to conduct more and more depraved activity by threatening to distribute abuse images and personal details across the Dark Web.[66,67]

Such cases demonstrate the escalation and incitement to offend through peer-networking on both the Surface Web and Dark Web, where discussions with like minded individuals lead offenders to sharing methods to commit offences and evade detection.

Together, these case studies are indicative of a changing offender pathway and a clear relationship between indirect and direct contact abuse.

Some offenders arrested for the viewing or possession of indecent imagery of children claim they have not committed any crime as there was no contact abuse, and that they weren't involved in any coercion, especially where children have posted images and videos themselves. In 150 of 195 countries covered by the Rule of Law Project by the International Center for Missing and Exploited Children (ICMEC), domestic legislation now meets Criteria 4, which criminalises the knowing possession of CSAM regardless of the intent to distribute.[68]

From a safeguarding perspective, distinguishing between 'contact' and 'non-contact' abuse is misleading. Where the offender is not physically present in the room but directing the conduct remotely, these victims of 'contact abuse by self-touch' may report a heightened sense of guilt and shame, making recovery difficult.[69]

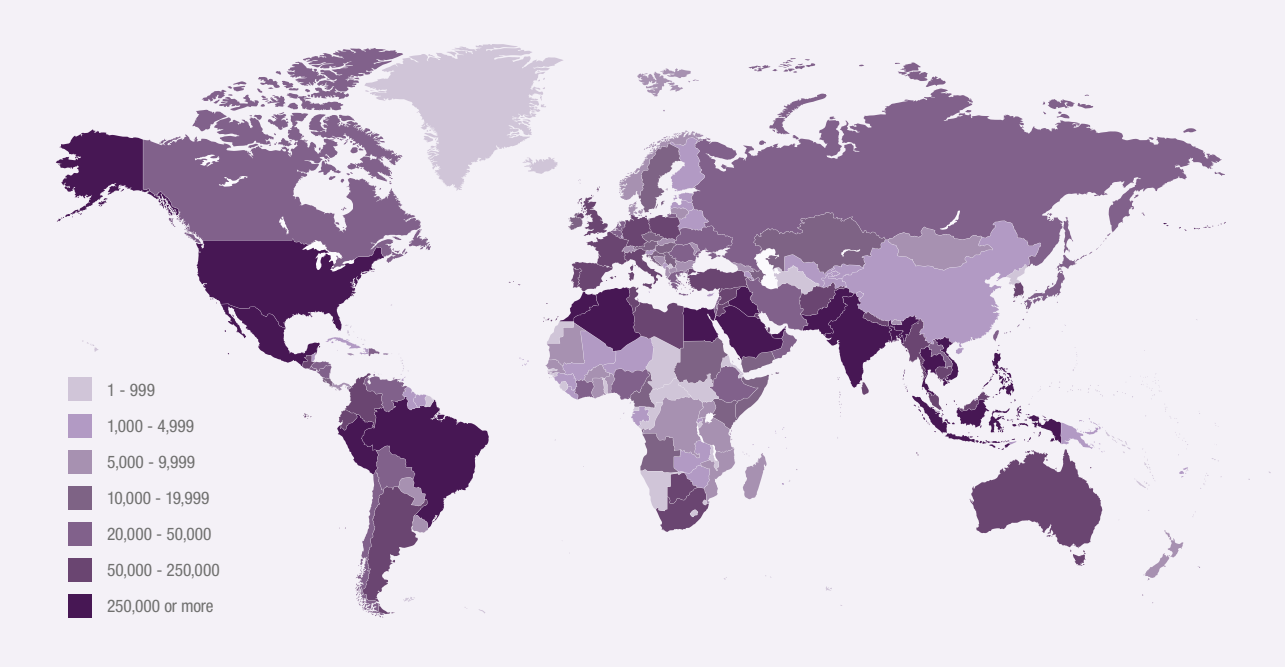
Offender demographics mirror their societies

A study by the UK's Centre of Expertise on Child Sexual Abuse (CSA Centre) found that, in the Global North, the employment and economic contribution of perpetrators was consistent with the ratios within their societies.[70] For example, research by the British Association of Social Workers (BASW) found that the prototypical online offender in the UK was a white, single male in his 20s or 30s, well educated, employed, with no history of severe mental illness or significant childhood adversity.[71] This aligns with data from law enforcement and non-governmental organisations, which shows that males are disproportionately found to be perpetrators of online CSEA.

These findings may not be truly representative. A large proportion of offending goes unreported and female perpetration is widely under-detected and under-reported.[72] It is likely the current overall offender profile reflects the demographics of those affluent nations that have enjoyed the fastest growth in technology penetration, device ownership and internet access.

As established in Chapter 4, it is not possible to correlate precisely between the demographics of those who produce, host and consume CSAM, as all three activities may occur in different jurisdictions.

Figure 6: NCMEC reports 2018



The heat map of the 2018 NCMEC reports, outlined on the previous page, shows where the highest concentrations of reports of suspected CSAM came from, highlighting the global scale of this problem.[73]

IWF URL stats

87% of all child sexual abuse URLs identified globally by the IWF are hosted in just five countries: the Netherlands, the United States, Canada, France and the Russian Federation[74]

Low-tech and tech-literate offenders

While there is no direct correlation between technical literacy and offending behaviour, increased technical sophistication does appear to decrease the probability of detection and apprehension, and increase the complexity of the investigators' task.

While GTA18 highlighted the emergence of offender communities using highly secured, encrypted and anonymised messaging platforms requiring a high degree of technical expertise, a new wave of offenders is being enabled by secure, mainstream consumer services at a low cost of entry.

The different ways in which offenders seek access to children

Recent statistics released by Chinese courts show that victims and abusers in child sexual abuse cases first connect via the internet in approximately 30% of all reported cases. However, court officials note that "child sexual abuse is a significantly under-reported crime since it often happens in private" and that many do not enter legal processes due to "objective and subjective reasons", including victim fear and challenges in obtaining evidence.

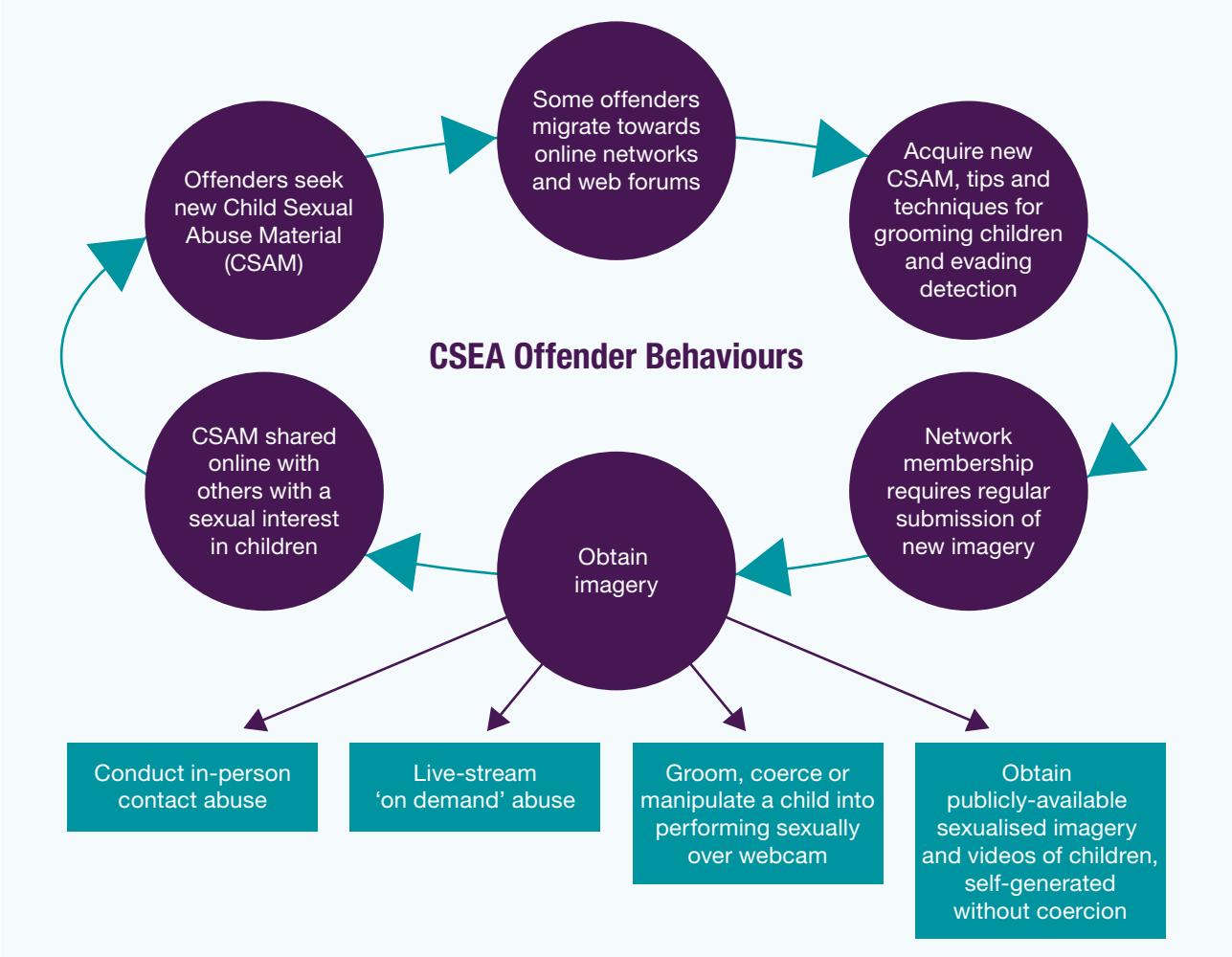
In one case, an offender was sentenced to 11 years for coercing his victims into providing sexually explicit images by informing victims he was a television executive looking for talent. The offender proceeded to use these images to blackmail victims for further photos and videos. In another case, a 32 year-old used a dating app to engage with children, before abusing one victim met through the app in a local hotel room.[75,76]

In another instance, an offender based in rural China was able to access Tor-based bulletin boards. When the offender noted that slow internet connections were limiting his ability to use Tor, he switched to peer-to-peer file sharing sites, often using a VPN to hide his IP address.[77]

These case studies demonstrate that offenders can and do use a full range of technology in order to access and exploit children, and this phenomenon is universal and not exclusive to the Global North.

In parallel, the growth in social media use has allowed direct access to children at scale. This has led to significant increases in online grooming, blackmail and extortion. Individual offenders can simultaneously target multiple children, blackmailing and extorting them at speed. As a result, CSEA has become associated with the grooming of children through social media. However, children remain vulnerable to in-person contact abuse by family members and those in positions of trust, and in some countries is often linked to cyber-sex trafficking.[78,79] In fact, 67% of online CSAM imagery appears to have been taken in a home setting.

Figure 7: CSEA Offender Behaviours



Many of the above factors are driving a vicious cycle of offender behaviours. The emerging picture is that those with a sexual interest in children seek new indecent images and videos of children online, and may even seek in person contact with children. Improved security and anonymity mean these individuals are increasingly drawn towards online networks and web forums, where they acquire not just images but tips and techniques for grooming children and evading detection. Designing preventative measures will require further research to understand the causes and origins of sexually abusive behaviour.

06 Victims' online exposure

Greater levels of online access and shifting cultural norms are lowering the age range of victims and increasing their vulnerability

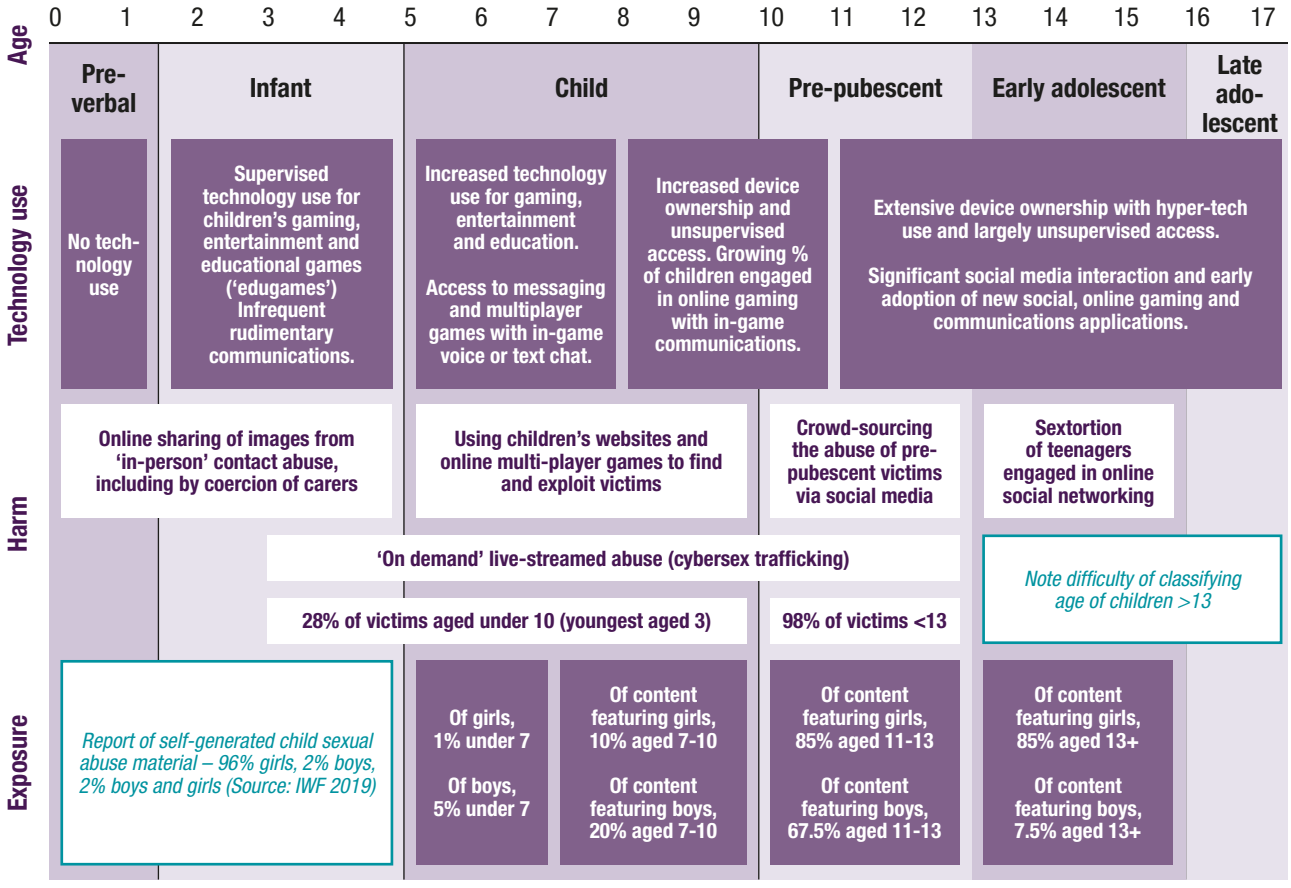
We have applied the following categorisation of victims according to their age and related technology adoption. Using fresh evidence from parental surveys and web forums concerning children's use of popular social media and online multiplayer gaming services, this suggests that the average age for each type of technology use is approximately two years lower than we first reported in GTA18.

When we categorise the same age groups in relation to the types of harm they are exposed to, and the percentages of children in each age range who are exposed to different harms, there is a clear correlation with the types of technology each age group is using.

According to UNICEF, one in three internet users worldwide is a child.[80] This equates to 122 million children coming online in 2018 alone. This represents significant challenges for adult supervision and safeguarding.

Children are acquiring ownership of, and/or unsupervised access to, internet-enabled smart devices at younger ages, and using them for unsupervised interactions with strangers using social media and multiplayer online gaming.[81] This exposes children and vulnerable people to a wide range of risks (the UK Government has categorised 29 online harms) of which OCSE,

Figure 8: OCSE victim categorisation



online terrorist and extremist content represent the greatest scale and severity.[82]

The problem is particularly acute in affluent societies. Many carers and teachers, who have a vital role in defining the terms of children's online access, have not experienced these risks and harms in their own childhoods. Therefore, the awareness of dangers that govern norms of physical engagement with the outside world have not yet evolved online.

While the recommended minimum age to create a social media account is 13, and higher in some jurisdictions (and for Facebook, Twitter, Instagram, Snapchat, and other US social media firms this is a legal minimum) there are indications of extensive access to online services and device ownership among 5-13 year olds, and clear indications that children are being exposed to the online world earlier.

The impact of unsupervised access to social media, and gaming services is seen by the age profile of the subjects of SGII, and by the results of online surveys of parents and users. The popular multi-player online children's game Fortnite® has a Pan European Game Information (PEGI) rating of 12, but in a 2018 online poll from Survey Monkey and Common Sense Media, 26% of parents chose 8-11 as the age children should be allowed to play.

42% of infants in Australia are using internet-enabled devices by the age of two, and 81% by the age of four

51% of six to 13-year-olds in Germany have a smartphone or mobile phone[83]

80% of under 14-year-olds in Singapore have accessed the internet[84]

90% of 11 to 16-year-olds in the UK say they have a social media account, and 44% of 5 to 15 year olds own a smartphone[85]

Emerging use of gaming platforms

One technique offenders use is to offer a child a piece of equipment or some in-game currency that the child needs or wants for a particular game. One offender mentioned seeing a young girl livestreaming on YouTube. He asked her if she liked a certain game, and if she wanted in-game currency. When she said she did, the offender asked for her gaming ID and started talking to her on the platform, eventually receiving SGII in exchange for the in-game currency.[86]

Socio-economic factors

The vulnerability of children online is amplified by a range of socio-economic and cultural factors. Children are acquiring ownership of, and/or unsupervised access to, internet-enabled smart devices at younger ages, and using them for unsupervised interactions with strangers using social media and multiplayer online gaming. This exposes children and vulnerable people to a wide range of risks of which OCSE, online terrorist and extremist content represent the greatest scale and severity. This problem is particularly acute in affluent societies. Many carers and teachers, who have a vital role in defining the terms of children's online access, have not experienced these risks and harms in their own childhoods. Therefore, the awareness of dangers that govern norms of physical engagement with the outside world have not yet evolved online.

In parallel, many in the Global South are receiving the full spectrum of services instantaneously as mobile data infrastructure and low-cost devices provide unregulated access without the corresponding investment in upgrading education, legislation, social services and law enforcement services. This is compounded by different social norms around child sexuality, and there are particular challenges around investigations and support for male victims, especially in societies that perceive boys as resilient and more able to protect themselves.[87]

The Communications Authority of Kenya reports that mobile usage in Kenya's 44 million population stands at around 88%, even though 42% of the Kenyan population lives below the poverty line, and inequality levels are among the highest in Africa.[88] In such circumstances, children in the lower income groups are at greater risk of being sold, abused or trafficked online to provide family income.[89]

Similarly, in Cambodia, special economic and free-trade zones have been identified as particularly problematic for child sexual exploitation and trafficking, as the economic opportunities have made these destinations attractive to children and families from poorer regions.[90]

Canada
The Canadian Project Arachnid has scanned 2 billion web pages globally for CSAM since 2016, issuing over 4.6 million takedown notices to internet service providers. 85% of these relate to victims who are not known to have been identified by law enforcement[91]

Cameroon, The Gambia, Kenya, Togo and Uganda
54% of children have seen someone of their age in CSAM online, and about 10% of children have been approached by online contacts to share sexualised images[92]

Mexico
12,300 internet accounts were distributing CSAM in Mexico in 2017[93]

United Kingdom
21% of surveyed girls aged 11–18 had received requests for a sexual image or message.[94]

Displaced communities face increased risk

There is a growing body of evidence that suggests children in displaced communities, including refugees and economic migrants, are at increased risk of OCSE due to the low rule of law alongside growing technology adoption within communities where child protection capabilities are limited.

In the Middle East, the United Nations High Commissioner for Refugees has reported instances of young male Syrian refugees in Lebanon and Jordan being blackmailed into sexual activity by older boys or men who covertly use mobile phones to record indecent imagery that they threaten to upload to the internet.[95]

In China, the political instability of neighbouring states has resulted in high numbers of displaced people, with particularly vulnerable child communities. Popular messaging services and social media platforms are being used to facilitate the sex trafficking of women and children from rural regions.[96]

The threat of deportation, e.g. for North Korean migrants, may result in victims being reluctant to report abuse. Research from the Korea Future Initiative highlights that children as young as nine years old are featuring in cyber-sex live streams.[97] This vulnerability is particularly being exploited by more affluent East Asian societies, including South Korea, where an NGO report found that 95% of commercial exploitation of children is arranged over the internet.[98]

Cultural factors

Social factors can also influence vulnerability to online CSEA; children from the Lesbian, Gay, Bisexual and Transgender (LGBT+) communities are more likely to explore their sexual orientation online, which can increase their vulnerability to blackmail and exploitation and decrease the likelihood of them reporting abuse.

One study of online CSAM found that 80% of victims were female, 87% were Caucasian, and 83% of visible adult offenders were male.[99] With the tech divide closing and the Global South moving online, we anticipate these statistics will become more reflective of a globalised society and cultural factors, the rural/urban divide, access to support services and wider societal differences.

The normalisation of sexual behaviour online

Shifting cultural norms around image sharing and adult sexual interactions online are changing the landscape. Large numbers of children are participating in the production of erotic or sexualised images of themselves, which can be shared more widely or harvested and redistributed by those with a sexual interest in children. In the first six months of 2019, the IWF dealt with 22,484 reports of self-generated child sexual abuse material.[100]

Arizona State University research of over 1,000 students from seven US Universities indicates that ‘sexting’ is now considered a normal part of modern dating and is not associated with sexually risky behaviour.[101] The IWF has reported that this behaviour is being emulated by children and is beginning to play a significant role in victim vulnerability.[102] INTERPOL investigators have confirmed this cultural phenomenon is not localised to the Global North and has complex safeguarding implications in societies with strong cultural and religious taboos concerning extra-marital sexual interaction.[103]

The biggest challenge with SGII is that it is a catch-all term for a range of behaviours where the child's level of control varies; from consensual, peer-to-peer sharing within age appropriate relationships, through to the coercive process where adults (and some adolescents) groom, manipulate or blackmail a child into performing sexually over webcam for the purpose of obtaining more explicit imagery, and sharing this online with other offenders.

Designing platforms for adult/child interaction

In April 2016, two American nationals pleaded guilty to the production of CSAM and to designing and operating two websites for the purpose of coercing and enticing minors as young as eight years old to engage in sexually explicit conduct on web camera. Ten further members of this group across the US and South Africa were charged and sentenced.

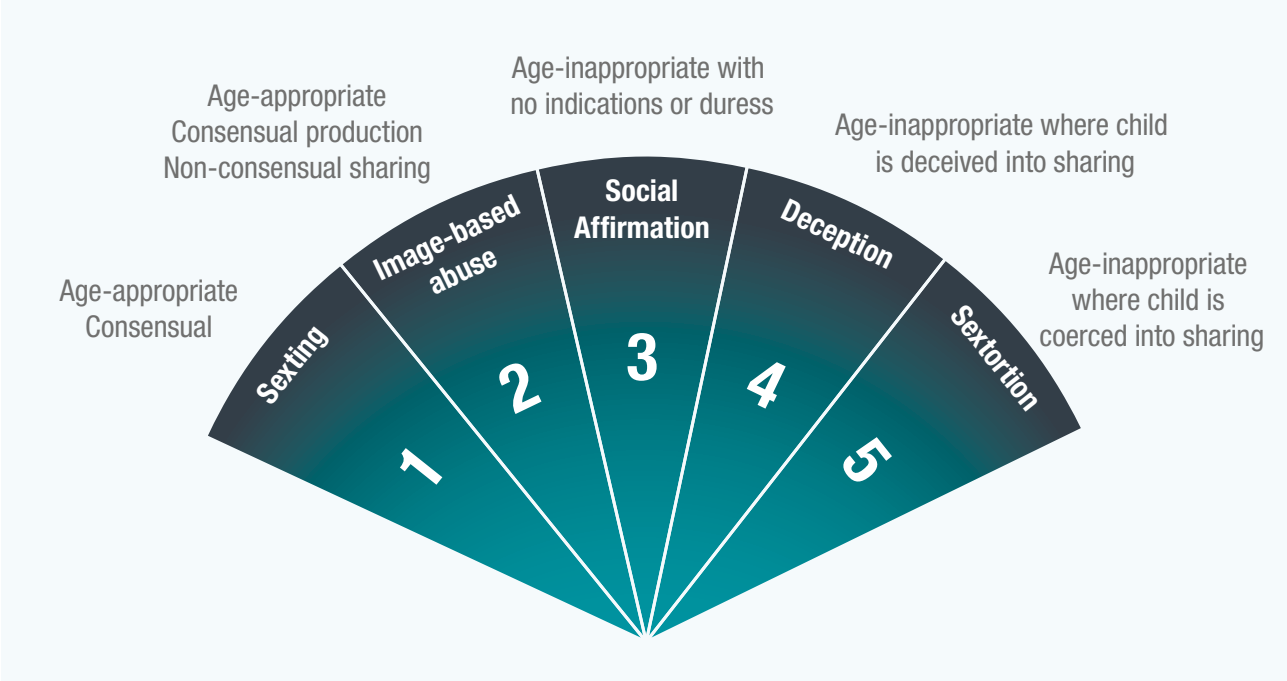
To lure children in, they created false profiles on social networking and video sites popular with children, and used pre-recorded videos of prior minor victims, often engaging in sexually explicit conduct, to convince children that they were chatting live with another minor.

These videos coerced and enticed the children to engage in sexually explicit activity via their own webcam, which could then be viewed live by multiple adult members without the victim's knowledge. Members of the websites ranked the efforts of one another to lure children to the website and coerce sexually explicit conduct. An estimated 1,500 minors were lured to the websites.[104]

The risks associated with peer-on-peer abuse and exploitation perpetrated by under-18s, and the risks associated with this group as they become adults, has also been identified as an emerging threat.

There are distinct differences in relation to the relative age of the participants, the degree of consent/coercion, and the criminal intent of the people sharing and receiving the images. But in all cases, there is a high risk that SGII and videos of children will be obtained and shared online.

Figure 9: Categorisation of self-generated indecent imagery (SGII)



1. **Sexting** refers to **age-appropriate, consensual** production and sharing of sexualised imagery between two adolescents or young people, where there is an assumed level of trust that the images will remain private between the parties. There is a risk these images are shared by others without consent.
2. **'Image-based abuse'** (also referred to as 'non-consensual indecent imagery' (NCII) refers to **age-appropriate** production and sharing of sexualised imagery between two adolescents or young people, where the images are **shared publicly without consent**.
3. **'Social affirmation'** refers to the **live-streaming of sexual and sexualised performances by children** over webcam with the aim of collecting 'likes' and validation. The subjects are typically highly engaged with no apparent perception that their conduct represents a harmful sexual encounter.
4. **'Deception'** refers to when a child is **tricked by an adult or adolescent** into believing they are engaged in consensual production and sharing of sexualised imagery with age-appropriate peers. The conspirator grooms children to engage in sexually explicit conduct on their own webcams, which can be viewed live, without the victim's knowledge, by individuals with a sexual interest in children. This conduct frequently escalates to (5).
5. **'Sextortion'** refers to the process whereby adults or adolescents **groom, coerce or manipulate** a child into performing sexually over webcam for the purpose of obtaining more explicit material to share with other offenders. There is a higher risk of deviancy as the offender often has less fear of what they can get away with. The depth of victim trauma is heightened by the sense of self-blame and guilt arising from blackmail and extortion.

There has been a significant increase in SGII in the last two years, whether produced consensually or as the result of manipulation or coercion. In the first six months of 2019, the IWF responded to 22,484 reports of self-generated CSAM online (exactly one third of all the reports they actioned in this period).[105] Just over a sixth of these images were categorised as the highest severity (below).

16% Images involving penetrative sexual activity and/or images involving sexual activity with an animal or sadism

25% Images involving non-penetrative sexual activity

58% Other indecent images

Of all the reports, 96% featured girls, 2% featured boys and 2% featured girls and boys together. Of this imagery, over 10% of this imagery of girls, and nearly 20% of the imagery of boys, featured children aged between 7 and 10 years old.

Age	Girls (96%)	Boys (2%)
Under 7	0.7%	4.8%
7-10	10.4%	19.8%
11-13	84.5%	67.7%
Over 13	4.4%	7.7%

The actual number of 13-18-year-old subjects may be higher, as the IWF does not block images where they cannot determine whether the subject is aged under 18.

There are unintended consequences associated with criminalising young people sharing sexual imagery, with the risk that societies inadvertently label children inappropriately sharing 'sexting' images as 'dangerous sex offenders' when in most cases their 'crime' is naivety. However, harmful sexual behaviour by young people is an area that needs a lot more attention, and research is beginning to focus on this cohort, who need support and therapeutic intervention.

Children's changing relationship with technology increases risk

Two cases from Peru demonstrate how technology has influenced OCSE.

In one case, an offender was sharing CSAM with another individual through social networks. On his arrest, he confessed that a woman had sent him the CSAM from Peru. During the investigation, prosecutors found the victim's mother's mobile phone, which contained photographs and videos in which she sexually abused one of her daughters and then sent those materials through email and other social networks to a contact outside Peru.

In another case, a 16-year-old met a 44-year-old man through an LGBTQ+ app. The offender asked for naked pictures of the minor and asked him to have sexual intercourse. Because of his high vulnerability, the child sent his photos and, influenced by the offender, they met and engaged in sexual activities. After this, the offender harassed the victim to meet again.[106]

On-demand live streaming

There is some evidence of the internet being used not only to facilitate transactions and sex trafficking, but also to traffic children specifically to meet the demand for cybersex. This is enabled by the perception in some cultures that cybersex causes less harm because the abuse is remote. A recent study of 300 Filipino children who had been sexually abused online found that exploitation behind the webcam was considered a 'step up' from sexual exploitation on the street.[107] Parents who were involved in live OCSE (some of whom are groomed by perpetrators to introduce them to cybersex) felt that it did not pose harm to their children as there was no direct physical contact between the perpetrator and the victim.

Trends towards cybersex trafficking have led to calls to delineate child sex trafficking from general trafficking under law, with harsher penalties enforced due to the dual nature of the crime.

07 The socio-environmental context

Stark differences between the Global North and South are creating a worrying global discord

Local environmental factors can compound vulnerability and make it difficult to establish common ground internationally over what constitutes abuse, as well as increasing the challenge of any international response to child safeguarding, offender identification and apprehension.

The surge in internet accessibility has increased the risk of OCSE in many countries where mobile and broadband technology are still recent innovations, and where the necessary support resources, education guidelines and safeguarding measures to combat it are not yet technically mature. Consequently, there will be increasing numbers of young people in developing nations using the internet while unaware of the risks they face online or of available international support services.

Environmental factors and education

Whilst socio-economic factors and wealth inequality links victims and their vulnerabilities as discussed in Chapter 6, in the Global North there has been significantly greater investment to educate children in online safety and sexual relationships. Moreover, civil society organisations are regularly consulted on government policy and offer confidential helplines for vulnerable children. However, technological development continues to outpace the ability of governments to support, educate and regulate the technology sphere.

This is most profound in, but not exclusive to, the Global South, where large numbers of users are achieving device ownership and internet access in a context where such factors as poverty and inequality heighten children's exposure to sexual exploitation. For example, the promise of financial stability can incentivise low-income families to expose their own children to sexual exploitation and abuse. The breakdown of family support can result in children ending up on the street, where the absence of safeguarding measures and support networks can increase their vulnerability to trafficking and to sexual exploitation in travel and tourism. While the drivers of OCSE in the developing world are under-researched, UNICEF suggests that children's online and offline vulnerability closely mirror each other.[108]

Unmasking abusers

In 2015 a Kenyan offender was sentenced to life in prison for participating in the Dreamboard OCSE website. The offender admitted posting 121 messages on the site – a private, members-only online bulletin board that promoted OCSE and encouraged the sexual abuse and exploitation of very young children in an environment designed to avoid detection by law enforcement. The offender was considered a 'Super VIP' member of Dreamboard, a designation given to members who were prominent on the site and produced their own CSAM.

The prosecution was the result of Operation DELEGO, an investigation launched in December 2009 that targeted individuals around the world for their participation in Dreamboard. A total of 72 individuals across five continents were charged as a result. To date, 49 offenders have either pleaded guilty or been convicted after trial. Sentences have ranged from five years to life in prison.[109]

Defining, regulating and legislating OCSE

While education and supporting resources are helpful in raising digital awareness amongst children and families at a national level, international efforts at combatting OCSE are constrained by inadequate baseline terminology and supporting regulation and legislation.

The UN Convention on the Rights of the Child (1989) and the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (OPSC, 2000) are the most comprehensive international legal instruments that promote and safeguard the rights of the child and protect children from sale, sexual exploitation and sexual abuse. However, these treaties were adopted at a time when communications technologies and internet services were much less developed and less widespread, and when sexual offences against children did not have the close linkage with the digital environment that is now prevalent.

On 30 May 2019, the UN Committee on the Rights of the Child adopted its first ever Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography (OPSC) Guidelines, with the aim of making it easier for nation states to understand what is expected of them in terms of implementation and compliance.[110]

The only regional treaty to address in detail how nation states should prevent sexual offences against children, prosecute perpetrators and protect child victims is the Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, known as the Lanzarote Convention.[111] Its standards have inspired changes in legislation and policies in countries around the world. They include the EU Directive on combatting sexual abuse and sexual exploitation, which provides a holistic legislative framework covering the definition of offences, investigation and prosecution, prevention and assistance to victims.[112] The Lanzarote Convention has also inspired the Inter-American Court of Human Rights, which has established important case law for child protection, and the African Committee of Experts on the Rights and Welfare of the Child, which has developed experience and expertise to tackle important issues such as sale of children and child marriage.[113]

Nevertheless, inconsistent definitions at the global level make it difficult to agree internationally what constitutes OCSE. Subsequently, regulatory and legislative divergence has created loopholes that enable offenders to evade law enforcement and exploit vulnerable children.

The challenges of proving exploitation to remove imagery

The Australian eSafety Commissioner's Office highlighted that an internet search of one offender's legal name, alongside his daughter's CSAM nickname, reveals images that are all crops of her face from abuse material in which she features. However, it is difficult to get these removed when the cropped images do not show sexual abuse.

The recent trend of children uploading films of themselves dancing to YouTube became popular with offenders who left comments referring to the parts of the videos they found most arousing. The service's algorithm then began producing playlists of this content and promoting them to offenders.

Canada's national tipline for reporting OCSE has found they need to prove that an image is of a child, rather than that it is not. If there is any doubt that an image might depict an adult (common for over 13s) it is especially challenging to have it removed.[114]

Disparity in international legislation

Definitions of offences vary considerably between countries. CSAM-related offences are generally, but not exclusively, clearly defined in countries with high levels of internet usage and include considerations for internet-enabled crimes. However, in countries with a relatively recent history of internet adoption, legal definitions are often lacking. For example, as of 2018 CSAM is not defined in law in Bosnia-Herzegovina, China, Indonesia, Lebanon, Peru, Saudi Arabia, Singapore, or Vietnam, to name but a few examples.[115]

Recent ICMEC research comparing legislative standards across the world with their model national legislation found that while 118 countries have legislation sufficient to combat CSAM, the strength of this legislation varies greatly from country to country.[116]

ICMEC analyses progress with CSAM legislation in every country around the world every two years and offers concepts to be considered when drafting anti-CSAM legislation.

The report's core criteria are to assess whether national legislation:

1. exists with specific regard to CSAM;
2. provides a definition of CSAM;
3. criminalises technology-facilitated CSAM related offenses;
4. criminalises the knowing possession of CSAM, regardless of the intent to distribute;
5. requires Internet Service Providers (ISPs) to report suspected CSAM to law enforcement or to some other mandated agency.

The 2018 report[117] shows that:

No of countries	Criteria
118	countries have legislation sufficient to combat CSAM offences (meet at least four of the five criteria)
21	countries meet all five criteria
16	countries have no legislation at all specifically addressing CSAM
51	countries do not define CSAM
25	countries do not provide for technically-facilitated CSAM offences
38	countries do not criminalise the knowing possession of CSAM, regardless of intent to distribute

This disparity is compounded by an observed trend of lower sentences for online offenders in demand-side countries (who direct and cause live sexual abuse or exploitation by instructing and paying in-person offenders to violate children) relative to the offenders committing the 'in-person' contact abuse.

A report by the International Justice Mission's Philippines programme emphasises that this trend appears to:

- undermine the gravity of their serious, repeated and sometimes violent CSEA offences
- fail to provide justice for vulnerable victims, including from poor developing world nations
- fail to sufficiently restrain these offenders
- are less likely to deter the offender population.[118]

Online offenders are the minds and money behind in-person contact abuse and should be punished, restrained and deterred accordingly; they are effectively inciting contact abuse and committing it by proxy, and so are responsible for it having occurred. 'Demand-side' offenders direct and cause live sexual abuse or exploitation by instructing and paying in-person offenders to violate children of specific ages, at specific times, in specific ways. They produce CSAM every time they direct and watch the live abuse remotely, and they entice, solicit, and coerce minors to produce sexually explicit videos and images for consumption and distribution.

It is not only countries with low levels of internet usage, however, that struggle to accurately define CSAM. Even in countries with robust laws, prosecutors find it challenging to determine appropriate and consistent tariffs for combination offences (such as grooming, live streaming, CSAM sharing and blackmail); and the internet's blurring of the distinction between physical and online harm can enable offenders to evade the law. For example, before a prosecution can be launched, existing online grooming laws in most countries require that communication be followed by a meeting or clear plan to meet a child, despite a growing number of cases of online grooming where offenders appear to have no intention of meeting in person.[119] Instead, the objective is to receive or send SGII. While the production, possession and distribution of such material are all illegal, loopholes enable screen captures of such content to be shared even after the original has been identified and removed from the internet.[120]

Targeting offenders through multi-national law enforcement

In 2018, in a multi-national investigation by INTERPOL, US Homeland Security and authorities in Thailand and Australia, nine offenders were arrested for using and facilitating the running of a Dark Web site hosting CSAM.

The site had 63,000 users worldwide and featured abuse of more than 100 children, the youngest being identified as 15 months old. Despite stringent efforts to remain anonymous, investigators were still able to trace and identify the offenders.

The site's primary administrator abused his nephew in order to make contributions to the site and consequently was sentenced to 146 years in prison. Another offender, also a site administrator and pre-school teacher, received a sentence of 40 years, a record in Australia for CSEA offending. At least 50 children have been identified and saved from abuse since the operation's launch, and efforts to identify and rescue more of the children are ongoing.[121,122]

A proposed baseline definition

INTERPOL is leading international efforts to establish a universal 'baseline' definition of OCSE, based on criteria which would be deemed irrefutable by all nations. [123]The proposed criteria:

- the victim is a real child;
- the victim is pre-pubescent, or in the very first signs of puberty (typically under 13 years old);
- the imagery conveys either:
  - sexual activity of the child, with the child, in the presence of a child, between children; or
  - a focus on the vagina, penis or anal region of the child; and
- the image is verified by several specialists from different countries.

Regulation of online harms

Among the nations of the Global North, governments, law enforcement organisations, the technology industry and third sector are increasingly co-operating to find innovative solutions to mitigate the spread of online harms.

There has been progress in some countries, including Australia, Germany and the UK, to improve online safety by introducing stricter internet regulation. Australia's eSafety Commissioner, created in 2015, is the established regulator, educator and coordinator for online safety, covering a range of harms. In April 2018, the USA passed a law known as 'FOSTA', which modified the Communications Decency Act to exempt services providers from Section 230 immunity from liability for publishing information provided by third parties for services that knowingly facilitate or support sex trafficking.[124] And the EU has announced it will review the change to equivalent immunity provided by the e-Commerce Directive.[125] However, the internet is not constrained by national borders or legal systems. The challenge lies in designing a new regulatory framework to address a global problem that has no internationally-agreed standards or definitions.

In April 2019, the UK Government published an Online Harms White Paper, which proposed establishing a national body to regulate harmful content and make the UK the safest place in the world to go online.[126] In July, following a two-day summit on current and emerging threats to national and global security, senior ministers from the UK, Australia, Canada, New Zealand and the United States reaffirmed their commitment to work together with industry to tackle a range of security threats including OCSE. And during a roundtable with technology firms, ministers stressed that law enforcement agencies' efforts to investigate and prosecute the most serious crimes would be hampered if the industry carries out plans to implement end-to-end encryption without the necessary safeguards.[127]

The rule-of-law dichotomy

While countries with weak rule of law create more opportunities for offenders to exploit vulnerable children, countries with strong rule of law and advanced infrastructure are responsible for hosting a substantial proportion of CSAM online, including the Netherlands and USA as the top two countries where CSAM is hosted for global audiences. The rigorous adoption of data privacy measures in nations with strong rule of law has enabled the secure web-hosting of CSAM.

It is already apparent that the demand to remove barriers to law enforcement access to private communications will collide with global e-privacy concerns. The IWF has highlighted that asking ISPs to actively monitor their networks for illicit content would directly conflict with Article 15 of the European Union's e-Commerce Directive.[128] At present, private companies have no legal obligation to share data about the abuse on or reported to their platforms, or about the actions they have taken to protect the children involved.

Growing public frustration with the role of ISPs as an enabler of a wide range of online harms is likely to bring data privacy regulations under increasing scrutiny over the next decade. Policy decisions that increase encryption and anonymity will have a crucial impact on OCSE and our ability to combat it.

International co-operation is imperative to tackle the increasing severity, scale, and complexity of offences

In 2019, 337 people were arrested across 38 countries including the UK, US, Ireland, America, South Korea, Germany, Spain, Saudi Arabia, the United Arab Emirates, the Czech Republic and Canada in relation to a dark web child abuse site called 'Welcome To Video'.

This site, was run by a 23-year-old offender from South Korea, contained more than 250,000 videos of abuse, with users having made more than one million downloads of CSAM. The website monetised the sexual abuse of children and was one of the first to offer videos of serious abuse for sale using the cryptocurrency Bitcoin. The site was taken down by an international taskforce set up by the NCA and included Homeland Security Investigations and Internal Revenue Service Criminal Investigation in the US, the South Korean National Police and Germany's Federal Criminal Police.

Nikki Holland, NCA Director of Investigations, said: "Dark web child sex offenders – some of whom are the very worst offenders – cannot hide from law enforcement. They're not as cloaked as they think they are, they're not as safe as they think they are."

The case illustrates what law enforcement is seeing in child sexual abuse offending: increases in severity, scale and complexity, including a direct link between viewing abuse images and contact abuse, as well as offenders using the dark web and encryption to hide their activity and identifies.[129]

08 The sphere of harm

The trauma associated with online abuse takes an enormous and increasingly life-long toll on victims, their families and society

The four lenses of global technology trends, offender threat, victim vulnerability and the socio-environmental context all converge to give rise to the fifth lens: harm.

The trauma associated with online abuse takes an enormous and increasingly life-long toll on victims and their families, together with the societal costs of providing medical treatment, social care and mental health support. OCSE has been linked to mental health challenges in later life, depression, increased risk of substance addiction and severe behavioural problems. This impacts not only the victim but also the surrounding family network and the social/national health and support systems.

A 2017 study from the US National Institute of Justice (NIJ) found that children with a history of physical and emotional abuse were more likely to exhibit behavioural problems during middle childhood, which could subsequently lead to adult criminal behaviour. The effects appear to present differently in girls than in boys, with the former tending to internalise problems that manifest as anxiety, depression, and social withdrawal, while boys and young men tend to externalise problems, with heightened hostility, aggression, and delinquency. Both types of behaviour have been shown to lead to adult criminal behaviour and are linked to troubles with education, employment, productivity and financial prospects.[130]

There are specific challenges in countries where, for legal and socio-cultural reasons, male victims of child sexual abuse are marginalised in the eyes of society and/or the law, or are not believed or helped even when they do disclose abuse.

Costing of online child sexual exploitation

According to the Finnish Preventing Sexual Crimes Network, the cost of a sexual crime is €150,00 for medical care and therapy per victim.[131] Europol have indicated that this is a very conservative estimate, as it does not include life long cost of harm. However, over those same three years, preventative therapy for the offender costs €9,600.

Costs of a sexual crime against a child within three years	
Costs of preliminary investigation	€3,000
Costs of judicial system	€5,000
Prison sentence of 2-5 years	€121,600
Costs of the 'STOP' programme in prison	€4,300
Medical costs of a victim	€5,500
Therapy costs of a victim in three years	€9,600
TOTAL	**€149,000**
Costs of preventative therapy in three years	€9,600

One academic study placed the lifetime economic cost of sexual abuse of children in the US at approximately US$9.3 billion, including the costs associated with government spending and productivity losses.[132]

INTERPOL Secretary General Jürgen Stock has said: *"The scale of this crime is shocking, made worse by the fact that these images can be shared online globally at the touch of a button and can exist forever. Each time an image or video clip is shared or viewed, the child is being re-victimised."*[133]

The story of Olivia, as told in the 2018 Internet Watch Foundation Annual Report, fully details the impact and trauma of re-victimisation as the images of her abuse have sadly remained in circulation.

Olivia's story: the ongoing impact of abuse

At three years old, Olivia should have been playing with toys, enjoying an innocent childhood. Instead, she was subjected to appalling sexual abuse over a number of years and repeatedly raped and sexually tortured.

After five years, the police rescued Olivia. While the physical abuse ended and the man who stole her childhood was imprisoned, the images were still in circulation and offenders continue to share and probably profit from Olivia's misery. Since being rescued, Olivia's image appeared online five times each and every working day.

We know, from talking to those who have suffered re-victimisation, that it's a mental torture that can blight lives and make it difficult to leave abuse in the past.

Knowing an image of your suffering is being shared or sold online is hard enough. But for survivors, fearing they could be identified or recognised as an adult is terrifying.[134]

Another growing challenge is the victim's fear over disclosing what is happening to them or, in some cases due to their young age, a lack of understanding that it is wrong, possibly because abuse was committed by a perpetrator within the family unit or a position of trust. There can be a number of contributing factors, including the fear they will not be believed, the fear of permanency – that the images and related messages will forever remain online, and feelings of shame, embarrassment and guilt. Marie Collins, the founder of the Marie Collins Foundation and a victim of sexual abuse as a child, has spoken about these feelings at length: *"As a child I wouldn't have told anybody about my abuse because if I had told someone about the pictures, they might have found them. I definitely didn't want anyone to find them because they would then have seen how awful a person I was… but I always worried about those pictures… where they were and who had seen them."*[135]

This fear of permanency is real and re-victimisation is a relatively new consideration that is amplified by online abuse. Imagery continues to be circulated for years following the original period of abuse, even after the victim has been rescued and the offender caught and prosecuted.

Recognising that we are now starting to see the first generation of victims of child sexual abuse imagery whose abuse has been distributed online reach adulthood, the Canadian Centre for Child Protection's International Survivors' Survey is seeking to better understand the impacts of this crime, and to determine what policy, legislative and therapeutic changes are required to respond to the needs of these victims.[136]

The Phoenix 11

The Phoenix 11 is a group of eleven survivors whose child sexual abuse was recorded, and in the majority of cases, distributed online. The Phoenix 11 has banded together as a powerful force to challenge the inadequate responses to the prevalence of child sexual abuse images on the internet.

In February 2018 the Canadian Centre for Child Protection, along with the US National Center for Missing and Exploited Children (NCMEC), organised the first retreat for this unique group of survivors in North America. Its purpose was to provide a place for survivors to share some of the challenges they face or have faced in a safe and supportive environment, to network and build relationships with other survivors. One outcome was the establishment of an advocacy group group, the Phoenix 11, to focus on bringing the collective voice of victims and survivors to the international stage to effect change.

The Canadian Centre assists and supports the efforts of the Phoenix 11 to advocate for change by writing letters on their behalf, facilitating the use of their Community Impact Statement in court proceedings, and soliciting feedback from them on educational and other materials intended for external audiences.[137]

Technology is also an opportunity to stop abuse

In a world where growing numbers of children have social media accounts and spend an increasing portion of their time online, the question of how best to protect them becomes of paramount importance. Although governments have the responsibility of setting laws and implementing policies across their jurisdictions, they cannot fight the battle alone. Private sector businesses, local communities, organisations developing technology to find and remove content and the media all have a crucial part to play.

The Child Dignity Alliance's Technical Working Group report includes the recommendation that industry should be strongly encouraged, or even required through domestic legislation, to:

- be required to scan their networks, platforms and services, or take similar active measures, as a default operating procedure to detect known CSAM, including so-called 'passthrough' services
- enforce standards and codes of conduct against illegal behaviour on their platforms
- implement 'safety by design' frameworks, codes of practice or minimum standards.[138]

Revictimisation

In August 2019, a male and a female reporter contacted the Aarambh Foundation, who host the IWF's reporting portal in India, with URLs of video content featuring themselves as children. The victims' distress at the emergence of online content of their childhood, and the social stigma surrounding this, had a direct effect on their lives, including jobs, marriage and social engagements. By reviewing reports from local law enforcement in India, the organisations were able to verify the report and their ages, and ensure the offending URLs were removed.[139]

With new challenges arising as private businesses and social media platforms move towards more secure communications and end-to-end encryption, there will need for global action to ensure that new technologies can be used in the identification and management of illegal and harmful content.

Artificial intelligence and machine learning (ML) are playing a crucial role in doing the 'heavy lifting' of detecting harmful images and videos at scale. This reduces the harm of revictimisation and enables trained specialists to focus their efforts more efficiently and prioritise their reviewing in the right places. But they do not provide the whole answer; for example, current generation ML models encounter some difficulties recognising the faces, ages and gender of children with different racial backgrounds, and these are some of the deficiencies the global technology community should be focusing on.

Project Arachnid

Operated by the Canadian Centre for Child Protection, Project Arachnid is an innovative tool to combat the growing proliferation of CSAM on the internet.

The Project Arachnid platform was initially designed to crawl links on sites previously reported to Cybertip.ca that contained CSAM and detect where these images/videos were being made publicly available. Once CSAM was detected, a notice was sent to the provider hosting the content requesting its removal.

Project Arachnid still carries out the crawling activities described above, but it is continually evolving and adapting to enhance its capabilities to accelerate the detection of CSAM, thus facilitating its speedy removal.

In its first three years of operation, Project Arachnid has handled the following volumes:

- 2 billion web pages scanned containing 91 billion+ images. Of those, 13.3 million suspicious (meaning possible CSAM based on PhotoDNA)
- 4.6 million takedown notices sent to providers
- 85% of the notices relate to victims who are not known to have been identified by police.[140]

09 Forward look

Based on our assessment of the threat, these are some of the recommended steps that nations can take individually or collectively, to mitigate the impact. Further details are available in the Global Strategic Response to Online CSEA, available on the WePROTECT Global Alliance website: https://www.weprotect.org/

This year's report demonstrates that rapidly expanding global access to the internet and low-cost smart devices means more potential victims and perpetrators coming online. Easy consumer access to new secure communications services, with end-to-end encryption, means that offenders are increasingly well protected in their 'digital safe havens', with unprecedented levels of co-operation and information sharing. Offenders have multiple channels to access a single instance of abuse, and peer encouragement validates and normalises offender behaviours.

While these technological and social aspects proliferate offending and move offenders closer to their victims, there are additional social, cultural and economic factors at play that amplify the risk and harm. There has been a steady decline in the age of children allowed unsupervised access to social media and multi-player online games; and an emerging behavioural shift that normalises image sharing and sexual behaviour online.

Important contributing factors to tackling the issues at their current scale are the ability of each nation's legal framework to provide adequate protection for children; the availability of suitably-trained law enforcement personnel that can be rapidly and effectively deployed to pursue offenders, and to locate and safeguard the victims; and their capacity to engage and regulate the technology industry to apply appropriate protective measures in line with up-to-date policies. But we must not forget that the responsibility for OCSE sits first and foremost with the offenders.

Today, through the WePROTECT Global Alliance, nation states, law enforcement organisations, the technology industry, academic institutions and the third sector can all become part of the global solution to this heinous crime against the most vulnerable in our societies.

To tackle this persistent and growing threat, there are steps that nations can take individually, and actions they need to take together:

- ✓ **The international community** should give greater consideration to programmes designed to prevent first-time offending and recidivism, in view of the high costs of through-life therapeutic support to victims, and of detecting, prosecuting, incarcerating and rehabilitating offenders.
- ✓ **The international community** should engage upstream technology and service providers more consistently at the national and international levels.
- ✓ **The international community** should consider a paradigm shift in the current notice and take-down model for relieving victims from trauma and taking bad content hosts offline, while improving international access and data sharing.
- ✓ **The international community** should continue building a consistent classification schema for OCSE, analysing existing loopholes in legislation to inform new policy.
- ✓ G**lobal technology companies** should be more proactive in their efforts to scan, detect and remove CSAM and thwart grooming attempts, embracing a safety by design approach rather than a reactive stance to OCSE, for example through verification of children online.
- ✓ **Nations** with specialist expertise in aspects of the Model National Response should have a duty to share this with other countries (see https://www.weprotect.org/the-model-national-response for further information).
- ✓ **Nations** should aim to appoint a national leader, educator and regulator to coordinate online safety efforts and to facilitate take-down of harmful content.
- ✓ **Nations** should ensure the support networks for whole-life victim support are appropriately resourced and funded.
- ✓ **National policymakers** should seek a balanced approach to security, privacy and public safety legislation, ensuring that privacy does not invalidate or cancel out the ability for companies to proactively scan for CSAM or grooming behaviour.
- ✓ **National policymakers** should take a victim-centric approach to designing prevention campaigns and intervention measures, working with professional media agencies and involving the perspectives of victims and the voices of young people.
- ✓ **Law enforcement agencies** should work together to increase the sharing of advanced technologies and innovative investigative techniques, to improve victim identification and disrupt OCSE at scale.
- ✓ **Online safety experts** should share best practice educational frameworks, content and teaching methods, and evaluate their effectiveness in behavioural change.
- ✓ **Social care providers** should attain a better understanding of those who are most vulnerable or susceptible to online exploitation, and develop tailored interventions to support them.

10 Endnotes

1 'Definition of Child Sexual Exploitation' (UK Government, 2016: pg. 3) available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/591512/HO_DfE_consultation_response_on_CSE_definition_FINAL_13_Feb_2017__2_.pdf (accessed 01 October 2019)

2 'Global Threat Assessment 2018' (WePROTECT Global Alliance, 2018: pg. 5)

3 http://www.missingkids.com/footer/media/vnr/vnr2 (accessed 01 October 2019)

4 https://transparency.facebook.com/community-standardsenforcement#child-nudity-and-sexual-exploitation (accessed 01 October 2019)

5 'Project Arachnid' (Canadian Centre for Child Protection, data as at 1 November 2019) available at: https://projectarachnid.ca/en/#shield)

6 http://www.missingkids.com/footer/media/vnr/vnr2 (accessed 01 October 2019)

7 Cited in 'Internet Organised Crime Threat Assessment' (EUROPOL, 2019: pg. 30)

8 'The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report' (Terre des Hommes, 2018: pg. 3) available at: https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (accessed 01 October 2019)

9 'Internet Organised Crime Threat Assessment' (EUROPOL, 2019: pg. 30)

10 INTERPOL correspondence with PA Consulting Group (2019)

11 National Strategic Assessment (National Crime Agency, 2019: pg. 13)

12 'Association of Sexting with Sexual Behaviours and Mental Health Among Adolescents' in Jama Paediatrics (Mori et al, 2019) cited in https://www.huffpost.com/entry/talking-to-your-kid-about-sexting_l_5d408dc8e4b007f9accf9939 (accessed 01 October 2019)

13 Global Threat Assessment 2018' (WePROTECT Global Alliance, 2018)

14 Direct case study-based insights submitted to PA Consulting researchers by the EVAC Fund, 15 October 2019

15 Direct case study-based insights submitted to PA Consulting researchers by the Australian eSafety Commissioner, 17 October 2019

16 'Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile devices, social media and e-commerce' (We Are Social, 2019: pg. 8), available at: https://wearesocial.com/global-digital-report-2019 (accessed 01 October 2019)

17 Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online', (Broadband Commission: 2019)

18 Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile devices, social media and e-commerce' (We Are Social, 2019: pg. 8-63)

19 'The State of the World's Children 2017: Children in a Digital World' (UNICEF, 2017: pg. 1)

20 'INHOPE Statistics Report' (INHOPE, 2018: pg. 2)

21 https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html?smtyp=cur&smid=tw-nytimes (accessed 11 October 2019)

22 'Annual Report 2018' (Internet Watch Foundation, 2019)

23 'Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile devices, social media and e-commerce' (We Are Social, 2019: pg. 8-63)

24 'Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile de

25 'Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile devices, social media and e-commerce' (We Are Social, 2019: pg. 8)

26 Estimate attributed to Dr Michael Seto, clinical and forensic psychologist at the Royal Ottawa Healthcare group, 'How many men are paedophiles?' cited in https://www.bbc.co.uk/news/magazine-28526106 (accessed 01 October 2019)

27 'How common is males' self-reported sexual interest in prepubescent children?' (Dombert et al., 2016) and 'The Revised Screening Scale for Pedophilic Interests (SSPI-2): Development and Criterion-Related Validation' (Seto et al. 2015)

28 https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html?smtyp=cur&smid=tw-nytimes (accessed 11 October 2019)

29 'Annual Report 2018' (Internet Watch Foundation, 2019: pg. 18-19)

30 INTERPOL correspondence with PA Consulting Group (2019)

31 Global Threat Assessment 2018' (WePROTECT Global Alliance, 2018: pg. 5)

32 'National Strategic Assessment' (National Crime Agency, 2019: pg. 13)

33 'Internet Organised Crime Threat Assessment' (EUROPOL, 2018: pg. 32)

34 Internet Organised Crime Threat Assessment 2019 Report (EUROPOL), available at: https://www.EUROPOL.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment

35 'The Internet is Overrun with Images of Child Sexual Abuse. What Went Wrong?' (New York Times, 2019) available at https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html (accessed 01 October 2019)

36 'Internet Organised Crime Threat Assessment' (EUROPOL, 2018: pg. 32)

37 'Global Digital Report 2019: Essential insights into how people around the world use the internet, mobile devices, social media and e-commerce' (We Are Social, 2019: pg. 88), available at: https://wearesocial.com/global-digital-report-2019 (accessed 01 October 2019)

38 'Breaking the Dark Net' (VG, 2017) available at https://www.vg.no/spesial/2017/undercover-darkweb/?lang=en (accessed 01 October 2019)

39 'The Top 7 Messenger Apps in the World' (Inc., 2018) available at: https://www.inc.com/larry-kim/the-top-7-messenger-apps-in-world.html

40 'DNS over HTTPS: Why we're saying DoH could be catastrophic' (Internet Watch Foundation, 17 July 2019) available at https://www.iwf.org.uk/news/dns-over-https-why-we%E2%80%99re-saying-doh-could-be-catastrophic

41 Internet Organised Crime Threat Assessment' (EUROPOL, 2018: pg. 33)

42 'Draft Council Conclusions on combating the sexual abuse of children' (Council of the European Union, 2019) available at: https://data.consilium.europa.eu/doc/document/ST-12326-2019-INIT/en/pdf (accessed 10 October 2019)

43 https://metrics.torproject.org/userstats-relay-table.html (accessed 29 October 2019)

44 'How paedophiles use cookies and keywords to hide sexual abuse images in innocent looking sites' (Independent, 2017) available at: https://www.independent.co.uk/life-style/gadgets-and-tech/features/paedophilia-child-sexual-abuse-images-video-codes-keywords-clues-cookies-iwf-masking-breadcrumbing-a7661051.html (accessed 01 October 2019)

45 US Department of Justice correspondence with PA Consulting Group (2019)

46 'Virtual child abuse imagery a headache for Gardaí' (Irish Times, 2019) available at: https://www.irishtimes.com/news/crime-and-law/virtual-child-abuse-imagery-a-headache-for-garda%C3%AD-1.3803910 (accessed 01 October 2019)

47 'Child abuse imagery found within bitcoin's blockchain' (Guardian, 2018) available at: https://www.theguardian.com/technology/2018/mar/20/child-abuse-imagery-bitcoin-blockchain-illegal-content (accessed 01 October 2019)

48 Internet Organised Crime Threat Assessment' (EUROPOL, 2019: pg. 33

49 International Justice Mission correspondence with PA Consulting Group (2019)

50 Internet Organised Crime Threat Assessment' (EUROPOL, 2018: pg. 35)

51 Internet Organised Crime Threat Assessment' (EUROPOL, 2018: pg. 32)

52 Internet Organised Crime Threat Assessment' (EUROPOL, 2018: pg. 37)

53 Further information on the EUROPOL 'Trace an Object' campaign available at: https://www.EUROPOL.europa.eu/stopchildabuse (accessed 01 October 2019)

54 Security summit ends with pledges to tackle emerging threats', (UK Government, 2019) available at: https://www.gov.uk/government/news/security-summit-ends-with-pledges-to-tackle-emerging-threats (accessed 01 October 2019)

55 'Etiology of Adult Sexual Offending', in Sex Offender Management and Planning Initiative at the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (Faupel, S., and Przybylski, R.) available at: https://www.smart.gov/SOMAPI/sec1/ch2_etiology.html (accessed 01 October 2019)

56 'Towards a Global Indicator: On unidentified victims in child sexual abuse material' (INTERPOL, ECPAT, 2018) available at https://www.ecpat.org/wp-content/uploads/2018/03/TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-MATERIAL-Summary-Report.pdf

57 INTERPOL ICSE database

58 'Mapping Online Child Safety in Asia and the Pacific,' in Asia and the Pacific Policy Studies, Vol. 5, Issue 3, (Singh, R. D., 2018: pg. 651-664)

59 '#SoSockingSimple wins ISPA best PR campaign' (Internet Watch Foundation, 12 July 2019) available at: https://www.iwf.org.uk/news/sosockingsimple-wins-ispa-best-pr-campaign

60 'National Strategic Assessment' (National Crime Agency, 2019: pg. 12)

61 US Department of Justice correspondence with PA Consulting Group (2018)

62 'The State of the World's Children 2017: Children in a Digital World' (UNICEF, 2017)

63 Presentation to Policing Institute for the Eastern Region (PIER) Conference on 'Tackling Online Child Sexual Exploitation' (Anglia Ruskin University, 25-26 April 2019) by Marcella Leonard (expert in psychosexual therapy, child and public protection) www.leonardconsultancy.co.uk

64 Operation NYCLATOPE, UK National Crime Agency (NCA) correspondence with PA Consulting Group (2019)

65 Operation WHILOCK, UK National Crime Agency (NCA) correspondence with PA Consulting Group (2019)

66 UK National Crime Agency (NCA) correspondence with PA Consulting Group (2019)

67 Operation CACAM, UK National Crime Agency (NCA) correspondence with PA Consulting Group (2019)

68 'Child Sexual Abuse Material – Model Legislation and Global Review' (International Centre for Missing and Exploited Children, 2018) available at: https://www.icmec.org/child-pornography-model-legislation-report/ (accessed 01 October 2019)

69 Marcella Leonard (of Leonard Consultancy) correspondence with PA Consulting Group (2019)

70 'Characteristics and motivations of perpetrators of child sexual exploitation' (Centre of Expertise on child sexual abuse, 2018) available at: https://www.csacentre.org.uk/csa-centre-prod/assets/File/CSE%20perpetrators%202%20-%20Characteristics%20and%20motivations%20of%20perpetrators%20of%20CSE.pdf (accessed 01 October 2019)

71 'Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation' (British Association of Social Workers: 2017) available at: https://www.basw.co.uk/system/files/resources/basw_64920-4.pdf (accessed 01 October 2019)

72 "A review of the evidence for female sex abusers" (McCloskey & Raphael, 2005), cited in 'Who Abuses Children?' (Australian Government Institute of Family Studies CFCA Resource Sheet, 2014) available at: https://aifs.gov.au/cfca/publications/who-abuses-children (accessed 01 October 2019)

73 NCMEC Data, provided by INTERPOL, 05 September 2019

74 'IWF global figures show online child sexual abuse imagery up by a third' (IWF, 2018) available at: https://www.iwf.org.uk/news/iwf-global-figures-show-online-child-sexual-abuse-imagery-up-by-a-third (accessed 19 October 2019)

75 'China Vows to Take A Hard-line on Child Sexual Abuse' (Supchina, 2019) available at: https://supchina.com/2019/07/24/china-vows-to-take-a-hardline-on-child-sexual-abuse/ (accessed 01 October 2019)

76 'It's sex abuse even with no touch' (China Daily, 2019) available at https://www.chinadailyhk.com/articles/233/225/172/1542599418213.html (accessed 01 October 2019)

77 US Department of Justice correspondence with WPGA Secretariat and PA Consulting Group (2019)

78 End Violence Against Children (EVAC) fund correspondence with WPGA Secretariat and PA Consulting Group (2019)

79 'Child sexual abuse images on the internet: a cybertip.ca analysis' (Canadian Centre for Child Protection, 2016) available at: https://www.protectchildren.ca/pdfs/CTIP_CSAResearchReport_2016_en.pdf (accessed 01 October 2019)

80 End Violence Against Children (EVAC) fund correspondence with WPGA Secretariat and PA Consulting Group (2019)

81 'The State of the World's Children 2017: Children in a Digital World' (UNICEF, 2017: pg. 1)

82 'How safe are our children?' (NSPCC, 2019)

83 Figures cited in 'Studies in Child Protection: Technology-Facilitated Child Sex Trafficking' (International Centre for Missing and Exploited Children, 2018: pg. 10)

84 Figures cited in 'Studies in Child Protection: Technology-Facilitated Child Sex Trafficking' (International Centre for Missing and Exploited Children, 2018: pg. 10)

85 Figures cited in 'Studies in Child Protection: Technology-Facilitated Child Sex Trafficking' (International Centre for Missing and Exploited Children, 2018: pg. 10)

86 'Fortnite Frenzy Key Findings' (Common Sense Media, 2018) available at: https://www.commonsensemedia.org/fortnite-frenzy-key-findings (accessed 01 October 2019)

87 UK Home Office correspondence with PA Consulting Group (2019)

88 'Sexual Exploitation of Children in Cambodia Submission for the Universal Periodical Review of the human rights situation in Cambodia' (APLE Cambodia, ECPAT International 2018)

89 Figure cited in 'The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report' (Terre des Hommes, 2018: pg. 6) available at: https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (accessed 01 October 2019)

90 Figure cited in 'The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report' (Terre des Hommes, 2018: pg. 11) available at: https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (accessed 01 October 2019)

91 'Sexual Exploitation of Children in Cambodia Submission for the Universal Periodical Review of the human rights situation in Cambodia' (APLE Cambodia, ECPAT International, 2018: pg. 4)

92 https://projectarachnid.ca/en/#faq (accessed 03 November 2019)

93 'Understanding African Children's use of ICT; A youth-lead survey to prevent sexual exploitation Online', (ECPAT International, 2013) cited in 'The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report' (Terre des Hommes, 2018)

94 Cited in 'Sexual Exploitation of Children in Mexico Submission for the Universal Periodic Review of the Human Rights Situation in Mexico (ECPAT Mexico, 2018) available at: https://www.ecpat.org/wp-content/uploads/2018/07/Universal-Periodical-Review-Sexual-Exploitation-of-Children-Mexico.pdf (accessed 01 October 2019)

95 'How safe are our children?' (NSPCC, 2019: pg. 13)

96 'We keep it in our hearts: sexual violence against men and boys in the Syria crisis' (UNHCR,

97 'Teenage Brides Trafficked to China Reveal Ordeal' (New York Times, 2019) available at: https://www.nytimes.com/2019/08/17/world/asia/china-bride-trafficking.html (accessed 01 October 2019)

98 'Sex Slaves: The Prostitution, Cybersex & Forced Marriage of North Korean Women & Girls in China' (Korea Future Initiative, 2019) available at https://www.koreafuture.org/report/sex-slaves (accessed 01 October 2019)

99 'Korean Approaches to Online Protection for Children in Digital Era' (Jalil, J., 2013) cited in 'Global study on sexual exploitation of children in travel and tourism' (ECPAT International, 2016: pg. 27) available at: https://www.protectingchildrenintourism.org/wp-content/uploads/2018/10/Global-Report-Offenders-on-the-Move.pdf (accessed 01 October 2019)

100 1'Child sexual abuse images on the internet: a cybertip.ca analysis' (Canadian Centre for Child Protection, 2016) available at: https://www.protectchildren.ca/pdfs/CTIP_CSAResearchReport_2016_en.pdf (accessed 01 October 2019)

101 IWF briefing to PA Consulting researchers, 27 September 2019

102 Research conducted by Johnstonbaugh, M., Arizona State University, cited in 'Sexting is a normal part of modern dating', (Daily Mail, 2019) available at: https://www.dailymail.co.uk/sciencetech/article-7363601/Sexting-normal-modern-dating-NOT-associated-sexually-risky-behavior.html (accessed 01 October 2019)

103 IWF briefing to PA Consulting researchers, 27 September 2019

104 INTERPOL briefing to WePROTECT Secretariat and PA Consulting researchers, 05 September 2019

105 https://www.justice.gov/opa/pr/members-international-child-exploitation-conspiracy-plead-guilty (accessed 15 October 2019)

106 Internet Watch Foundation correspondence with PA Consulting Group (2019)

107 End Violence Against Children correspondence with PA Consulting Group (2019)

108 'The dark side of the internet for children: online child sexual exploitation in Kenya – A Rapid Assessment Report' (Terre des Hommes, 2018: pg. 14) available at: https://www.terredeshommes.nl/sites/tdh/files/uploads/tdh-nl_ocse_in_kenya_research_report_feb_2018.pdf (accessed 01 October 2019)

109 'The State of the World's Children 2017: Children in a Digital World' (UNICEF, 2017)

110 https://www.justice.gov/opa/pr/kenyan-child-pornography-producer-sentenced-life-prison-participation-dreamboard-website (accessed 15 October 2019)

111 'Explanatory Report to the Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography' (ECPAT International, 2019)

112 'Convention on Protection of Children against Sexual Exploitation and Sexual Abuse ('the Lanzarote Convention')' (Council of Europe, 2007)

113 'Directive 2011/93/EU on combatting the sexual abuse and sexual exploitation of children and child pornography' available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093 (accessed 03 November 2019)

114 'Terminology Guidelines: For the protection of children from sexual exploitation and sexual abuse' (Interagency Working Group in Luxembourg, 2016)

115 Australian eSafety Commissioner's Office correspondence with PA Consulting Group (2019)

116 Child Sexual Abuse Material – Model Legislation and Global Review' (International Centre for Missing Exploited Children, 2018) available at: https://www.icmec.org/child-pornography-model-legislation-report/ (accessed 01 October 2019)

117 Child Sexual Abuse Material – Model Legislation and Global Review' (International Centre for Missing and Exploited Children, 2018) available at: https://www.icmec.org/child-pornography-model-legislation-report/ (accessed 01 October 2019)

118 Child Sexual Abuse Material – Model Legislation and Global Review' (International Centre for Missing and Exploited Children, 2018) available at: https://www.icmec.org/child-pornography-model-legislation-report/ (accessed 01 October 2019)

119 International Justice Mission correspondence with PA Consulting Group (2019)

120 Child Sexual Abuse Material – Model Legislation and Global Review' (International Centre for Missing and Exploited Children, 2018) available at: https://www.icmec.org/child-pornography-model-legislation-report/ (accessed 01 October 2019)

121 'Trends in Online Child Sexual Exploitation: Examining the distribution of Captures of Live-streamed Child Sexual Abuse (Internet Watch Foundation, 2018)

122 ‘50 children rescued, 9 sex offenders arrested in international operation’ (INTERPOL, 2019) available at: https://www.INTERPOL.int/en/News-and-Events/News/2019/50-children-rescued-9-sex-offenders-arrested-in-international-operation (accessed 20 October 2019)

123 ‘Fifty children saved as international paedophile ring busted’ (BBC, 2019) available at: https://www.bbc.co.uk/news/world-48379983 (accessed 20 October 2019)

124 1INTERPOL correspondence with PA Consulting Group (2019)

125 The Fight Online Sex Trafficking Act (FOSTA) and Stop Enabling Sex Traffickers Act (SESTA) became US law on April 11, 2018

126 ‘US, Europe threatens tech industry’s cherished legal ‘shield’’ (Politico, 2018) available at: https://www.politico.eu/article/tech-platforms-copyright-e-commerce-us-europe-threaten-tech-industrys-cherished-legal-shield/ (accessed 20 October 2019)

127 ‘Online Harms White Paper’ (UK Government, 2019) available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf (accessed 20 October 2019)

128 ‘Five Country Ministerial communiqué: emerging threats, London 2019’ (UK Government, 2019) available at: https://www.gov.uk/government/publications/five-country-ministerial-communique/five-country-ministerial-ommunique-emerging-threats-london-2019 (accessed 20 October 2019)

129 ‘Online Harms White Paper Response’ (Internet Watch Foundation, 2019: pg. 9)

130 ‘337 arrested after takedown of horrific dark web child abuse site Welcome To Video’ (NCA, 2019) available at: https://nationalcrimeagency.gov.uk/news/337-arrested-after-takedown-of-horrific-dark-web-child-abuse-site-welcome-to-video (accessed 21 October 2019)

131 ‘Effects of Child Maltreatment, Cumulative Victimization Experiences, and Proximal Life Stresses on Adult Crime and Antisocial Behaviour’ (Herrenkohl, T. I. et al., 2017)

132 Preventing Sexual Crimes’ cited in ‘New and Innovative ways to tackle child sexual abuse’ (Save the Children

133 ‘The economic burden of child sexual abuse in the United States’ (Letourneau, E. J., et al., 2018: pg. 413-22)

134 ‘INTERPOL network identifies 10,000 child sexual abuse victims’ (INTERPOL, 2017) available at: https://www.INTERPOL.int/en/News-and-Events/News/2017/INTERPOL-network-identifies-10-000-child-sexual-abuse-victims (accessed 20 October 2019)

135 ‘Annual Report 2018’ (Internet Watch Foundation, 2019)

136 Cited in ‘Digital dangers: The impact of technology on the sexual abuse and exploitation of children and young people’ (Barnardo’s and Marie Collins Foundation, 2016: pg. 37)

137 International Survivors’ Survey (Canadian Centre for Child Protection, September 2017), available at: https://www.protectchildren.ca/en/resources-research/survivors-survey-results/

138 ‘Phoenix 11’ (Canadian Centre for Child Protection) available at: https://protectchildren.ca/en/programs-and-initiatives/phoenix11/)

139 Aarambh Foundation correspondence with PA Consulting Group (2019)

140 Project Arachnid’ (Canadian Centre for Child Protection, data as at 1 November 2019) available at: https://projectarachnid.ca/en/#shield)

Find out more

You can find more information on our website
www.weprotect.org

or follow us on Twitter @weprotect