

Child Online Safety:

Minimizing the Risk of Violence,
Abuse and Exploitation Online.

October 2019



BROADBAND COMMISSION
FOR SUSTAINABLE DEVELOPMENT



Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online. October 2019



This report has been created through an iterative and collaborative process, drawing upon the expertise of the participants of the Broadband Commission for Sustainable Development's Working Group on Child Online Safety. This Working Group was established as an initiative of the Broadband Commission and consisted of commissioners and external experts.

The coordination of the external experts and the development of the content was provided under the guidance of Dr. Joanna Rubinstein (President & CEO of World Childhood Foundation USA) and Scott Gegenheimer (CEO of Zain). The process of completing the report was facilitated by Doreen Bogdan-Martin (Director of Telecommunication Development Bureau), Carla Licciardello (Child Online Protection Focal Point) and Anna Polomska (Project Officer and Policy Analyst) of the Broadband Commission Secretariat at the International Telecommunications Union (ITU).

The Broadband Commissioners, the Commissioners' focal points, and, in particular, the members of the Working Group, provided invaluable contributions.

Members of the Working Group

Broadband Commissioners:

Mr. Scott GEGENHEIMER (Co-chair)
Zain

Dr. Joanna RUBINSTEIN (Co-chair)
World Childhood Foundation USA

Ms. Audrey AZOULAY (Co-Vice Chair)
UNESCO

Mr. Bocar BA
Samena Telecommunications Council

Dr. Yee-Cheong LEE
ISTIC

Mr. Marcin CICHY
UKE, Poland

Mr. Börje EKHOLM
Ericsson Group

Ms. Kristalina GEORGIEVA
World Bank

Mr. Mats GRANRYD
GSMA

Dr. Carlos M. JARQUE
America Movil

Baroness Beeban KIDRON
Chair of 5Rights Foundation

Mr. Adrian LOVETT
Web Foundation

H. E. Mr. Hamad Obaid Al MANSOORI
United Arab Emirates

Mr. Kevin MARTIN
Facebook

Mr. Paul MITCHELL
Microsoft Corporation

Mr. Sunil Bharti MITTAL
Bharti Enterprises

Dr. Speranza NDEGE

Kenyatta University

Mr. Denis O'BRIEN

Digicel Group

Dr. Abdulaziz Bin Salem AL RUWAIS

Communications and Information Technology Commission, Kingdom of Saudi Arabia

Ms. Sun YAFANG

Huawei Technologies

External Experts:

Mr. Uri Sadeh

INTERPOL

Dr. Howard TAYLOR

Global Partnership to End Violence Against Children

Mr. John CARR

Independent consultant

Mr. Paul SHAPIRO

ICMEC

Ms. Susie HARTGREAVE

WePROTECT Global Alliance and Internet Watch Foundation

Mr. Robbert VAN DER BERG

ECPAT

Ms. Anna BORGSTROM

NetClean

Dr. Yuhyun PARK

World Economic Forum and DQ Institute

Mr. Johan DENNELIND and Ms. Heddy RING

Telia Company

Mr. Amandeep SINGH

UNSG High Level Panel on Digital Cooperation

Ms. Julie CORDUA

Thorn

Ms. Charlotte Petri GORNITZKA and Ms. Jasmine BYRNE

UNICEF

Ms. Elizabeth LETOURNEAU

John Hopkins University

Mr. Ernesto CAFFO

Telefono Azzurro

Ms. Helen MASON

Child Helpline International

Ms. Dushica NAUMOVSKA

INHOPE

A special thanks to the individuals who helped to put together this report:

Ms. Jennifer SULEIMAN

Zain

Ms. Lina FERNANDEZ DEL PORTILLO

World Childhood Foundation USA

TABLE OF CONTENTS

Foreward	5
Executive Summary	8
Introduction.....	13
What does safer look like?.....	19
A safer child is protected by a robust legal framework.....	21
A company culture that actively promotes child safety.....	21
To be safer, children must be aware of their rights.....	22
The crucial role of education.....	22
Ensuring children are safe by design.....	23
The role of technology in making children ‘safer’ online	24
A summary of ‘safer’	25
The state of children online today.....	26
Why we must act now to protect children	29
The extent of child sexual abuse material (CSAM) online.....	30
Contact risks: grooming, cyberbullying, stalking and harassment	31
Content risks: pornography, CSAM, violence, extremism, gaming and gambling	32
Conduct risks: data misuse, financial abuse and inappropriate behavior	33
Contract risks: how informed is children’s consent online?	34
A summary of the state of children online.....	34
Opportunities	36
Artificial intelligence and the fight against child exploitation online.....	37
Other emerging technologies	37
Growing International cooperation.....	38
Threats and the threat environment	39
Gaps in national policies and laws.....	41
Cybersecurity laws need modernizing.....	41
Lack of accountability systems and mandatory standards.....	42
The need to understand and track offenders.....	43
A range of threats derived from the misuse of technology	44
How gaps in technology enable abuse and exploitation.....	45
The growth of the darknet.....	45
The role of children’s social and cultural contexts	46
The responsibilities of key stakeholders	46
The role of the private sector	48
Recommendations	51
Model provisions on child protection for national broadband plans.....	55
Conclusion	59
Case studies	62
Glossary.....	70
References.....	72
Resources	80

Foreword

1



Foreword by Dr Joanna Rubinstein, President & CEO of the World Childhood Foundation USA, and Scott Gegenheimer, CEO of Zain Group

The Sustainable Development Goals adopted by all the world's nations in 2015 – and the legally binding UN Convention on the Rights of the Child, which this year celebrates its 30th anniversary – represent the global commitment to a better future for all, especially to children; to our next generation, to keeping them healthy, to providing them with access to education, entertainment and skills to ensure their future employability; and to protecting them from any form of violence, neglect, or torture. To give them a future.

Protecting children is not only our moral obligation but it's also good business to support their healthy and happy development. It is upon us to ensure that we provide a path towards a sustainable future for all. For that to happen, adults – parents, caregivers, teachers, legislators, the private sector and other stakeholders – must ensure that children can fulfil their potential.

To make this commitment a reality, the Broadband Commission for Sustainable Development created a cross-sector working group (WG) dedicated to addressing child online safety as a global issue. It consisted of senior representatives from UN agencies and a range of public and private organizations.

The WG was tasked with creating a report that would bring together the available evidence on the scale and nature of the risks and harms children face online and provide actionable recommendations for the prioritization of children's online safety.

Broadband connectivity is a key enabler for children's future. It helps to fuel the achievement of all the Sustainable Development Goals and to ensure that all children have an equal opportunity to thrive, so that no child is left behind.

The Internet has already transformed our lives at an unprecedented pace and scale. For children in developed countries, the digital world is the one they are born into and live within every single day. They are becoming the 5G and ultimately the 4th industrial revolution-ready generation, with Internet of Things (IoT), robotics, virtual reality (VR) and artificial intelligence (AI) changing the way we live and work.

Many adults think about the Internet in a very instrumental way, as something they go to or use from time to time to accomplish specific things. Children don't. For vast numbers, the Internet and its associated technologies are completely integrated into the way they live their lives across a very broad spectrum of activities. It is at once both part of and an extension of their lives: the most important way in which they communicate or engage with homework, friends, school, their favorite bands and sports clubs, even family members.

Recognizing this, the Broadband Commission's goal is to make connectivity a universal right and ensure that all children will have access to the Internet and the benefits it can bring them. How does that translate into numbers? Already today children represent one third of all Internet users. While benefiting tremendously from connectivity for their education and entertainment, they are also exposed to major risks and threats online, including different forms of violence and exploitation, such as child sexual exploitation and abuse (CSEA), bullying, radicalization, and more.

The challenges in tackling the dark side of connectivity are mounting. Unless we act now, the online exploitation of children could scale to even more appalling levels as we expand broadband into developing countries where most children live today. Often, in these newly

digitized territories, educational and law enforcement infrastructures will have difficulty keeping up with sophisticated and determined criminals misusing digital platforms and services. Making a unified global approach is more important and more urgent than ever.

This report aims to increase the prioritization of child online safety among all the key stakeholders and decision-makers from governments, the private sector, civil society, NGOs, and academia. Its recommendations are actionable and represent a call to collective action. They are based on the knowledge and expertise of major expert groups that have a long-standing commitment and experience in fighting various forms of violence against children online.

The fact that 22 commissioners joined the Working Group is testament to the commitment of the Broadband Commission for Sustainable Development to prioritize children in our common agendas.

We are grateful to all the members of the Working Group, the commissioners and the more than 20 experts for their participation in the development of this report and its recommendations. We hope they will help catalyze further actions in urgently addressing child online safety.

We know that it takes a village to keep children safe both online and offline. Therefore, we count on all the stakeholders to prioritize children and to collaborate and generate collective actions to prevent and address all forms of violence, abuse and exploitation of children online.

Children's journey through the digital world and their safety in the real world, we are all building, is everyone's business.

Thank you

Scott Gegenheimer, CEO of Zain Group

Dr. Joanna Rubinstein, President & CEO of the World Childhood Foundation USA

Executive summary

2



Executive summary

Affordable, reliable connectivity is now coming to more countries than ever. It has the potential to transform children's lives, giving them access to previously unimagined educational, cultural, and economic opportunities. But too often, children cannot realize these opportunities, because the Internet is also a place, in which the vulnerable are exposed to the risk of serious harm.

Globally, there are more than 2.2 billion people under the age of 18, making children the biggest vulnerable group in our societies [1].

Children around the world are regularly exposed to risks and harms online, including:

- Sexual abuse, exploitation, and trafficking – ranging from grooming to rape, recorded or streamed by abusers.
- Online harassment, victimization, and cyberbullying.

- Radicalization and recruitment by extremist organizations.
- Exposure to misinformation and age-inappropriate content, such as pornography or violence.
- Apps and games that are designed to encourage unhealthy habits and behaviors.
- Falling victim to illegal or unethical data harvesting and theft.
- The normalization of gender-based violence through exposure to online abuse materials.

To combat these harms and risks requires a coordinated and global approach. Unfortunately, the fight against child online abuse and exploitation is neither unified nor pursued in a way that is consistent across all countries. Capabilities, legal frameworks, awareness, lack of allocated and dedicated resources and the will to act all vary widely between agencies and jurisdictions.

Risks & Harms Online

According to recent research:

- In 2018, the US National Center for Missing & Exploited Children (NCMEC) received 18.4 million reports of child sexual abuse material (CSAM) online [2].
- A recent study found that 17% of parents said their children had been a victim of cyberbullying. In some countries, that figure was as high as 37% [3].
- According to the 2017 DQ Impact Report, 56% of 8-12-year-olds across 29 countries have been exposed to excessive screen time and at least one cyber-risk on average: including cyberbullying, video-game addiction, sexual behaviors, and offline meetings [4].
- One in five children aged between 9 and 17 see unwanted sexual material online and 25% of them reported experiencing extreme fear or distress [5].
- A 2019 study found that 99% of online terms and conditions were written in language too complex for children to understand [6].
- The number of illegal images and videos confirmed by INHOPE's Internet Hotlines increased by 83% from 2016 to 2018*.
- INHOPE also reported that the prevalence of pre-pubescent children (3-13 years old) depicted in CSEA images and videos increased from 56% of all illegal material (122,276) in 2016, to 79% (148,041) in 2017 and 89% (223,999) in 2018*.

*INHOPE Annual Report 2018: http://88.208.218.79/Libraries/IC-CAM_IHRMS/INHOPE_Statistics_Report_2018.sflb.ashx

The World Health Organization (WHO) estimates that every year 200 million children are sexually abused [7]. And increasingly, much of this abuse either takes place online or is captured and digitally distributed. In this case, the Internet is an enabler of abuse and exploitation.

Among the problems currently hampering the fight against the exploitation and all other forms of harm of children online, some of the more serious are:

- The inconsistency of legislation across jurisdictions, with some jurisdictions lacking laws that specifically cover child abuse crimes committed online.
- The lack of regulations and laws that hold service providers accountable for child abuse material (CAM) hosted on their platforms.
- The lack of common standards, definitions, and collaborative modalities across borders, making it difficult to measure the extent of the problem or cooperate fully in tackling it.
- Many countries lack capacity, capability or infrastructure to engage with all the sectors where cooperation is required if we are to eliminate harm to children online.

- The lack of data and research that looks at the problem globally (even in this report, many of the statistics we use are — of necessity — from the global north).
- The often-unmoderated nature of spaces where children spend time online (social media, messaging platforms, live-streaming apps, virtual spaces, interactive games etc.).
- The difficulty of monitoring Internet traffic, along with the rise of new technologies such as affordable smartphones, equipped with high-resolution cameras and video, picture messaging, live streaming, and encryption — all make preventing online child abuse even harder.
- Digital technologies are often designed with limited or no consideration about the ways these could be used to exploit or abuse a child.
- The nascent uptake and use of the technologies designed to detect and tackle online harm and exploitation — as well as the duplication of efforts in developing and applying such technologies. There is a clear and pressing need for the sharing of good evidence-based practice that is proven to prevent and reduce offending.
- Social attitudes and other environmental factors that in some countries and cultures make it easier for abusers to victimize children and to go undetected.
- The digital generation gap — with parents, caregivers, educators, and policy makers often ill-equipped to understand the digital lives of children, or to help them understand and avoid online risks.

- General under-resourcing, limited awareness, and a failure to build and share best practice in online child protection.

The link between child online safety and sustainable development

Not only are these practices an affront to the most basic rights of children, they also threaten to undermine the potential benefits digital transformation can deliver for all countries, but particularly for rapidly developing societies in the global south.

The ITU estimates that for each 10% increase in the penetration of digital services, a country can expect 1.3 per cent growth in GDP per capita [8]. But such benefits can only materialize if all citizens, including children, are able to derive the maximum possible benefit from the opportunities connectivity offers. And they can only do this if they are safe when they go online.

For these reasons, the UN Sustainable Development Goals (SDGs) also set a target under SDG 16.2 to end abuse, exploitation, trafficking, torture, and all forms of violence against children by 2030. To galvanize the action required if we are to meet this ambitious target, the Working Group has drawn up the Child Online Safety Universal Declaration.

The declaration outlines the steps that public and private entities must take in order to safeguard children online. We ask that all states as well as relevant private entities sign the declaration and commit themselves to putting its principles into action. To read and sign the full declaration visit: https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Declaration.pdf

About the report

The report was produced by the Broadband Commission working group on Child Online Safety. This cross-sector working group (WG) is dedicated to addressing child online safety as a global issue. It consists of senior representatives from global bodies including UN agencies, non-governmental organizations (NGOs), law-enforcement agencies, regulators, and private companies. For the full list of members, see page 2.

Introduction

3



Why we must take steps now to protect children online

The Broadband Commission for Sustainable Development works with UN member states and other relevant bodies to promote the expansion of broadband Internet availability, particularly in areas where people are currently underserved.

Recognizing the transformational role of connectivity, the Commission decided to prioritize the push for mass connectivity, because all the available evidence demonstrated that being connected fosters economic growth and opportunity.

The Commission has set itself the targets of ensuring that, by 2025:

- 75% of the world's population will be online.
- 60% of all children will have at least basic digital proficiency.
- 40% of the world's population will be using digital financial services.
- Women and girls will have equal access to the benefits of connectivity.

To achieve these goals, and realize the benefits they will unlock, it is vital that digital tools and services are accessible to everyone on equal terms. This cannot be the case if vulnerable groups are left inadequately protected. And children are, by far, the largest vulnerable demographic.

Recent research from ITU and UNESCO found that more than 50% of the world's population is now online [9]. Children are more than 30% of Internet users. By 2022, another 1.2 billion new users will have been added to this figure, with children being the fastest-growing online demographic [10]. Even the world's least-

developed countries are on course to have universal mobile Internet coverage within the next few years [11].

This explosion in connectivity will benefit the whole of humanity, particularly middle- and low-income countries among whose populations there is a huge and still-unmet demand for the economic, cultural, and educational opportunities Internet access can provide.

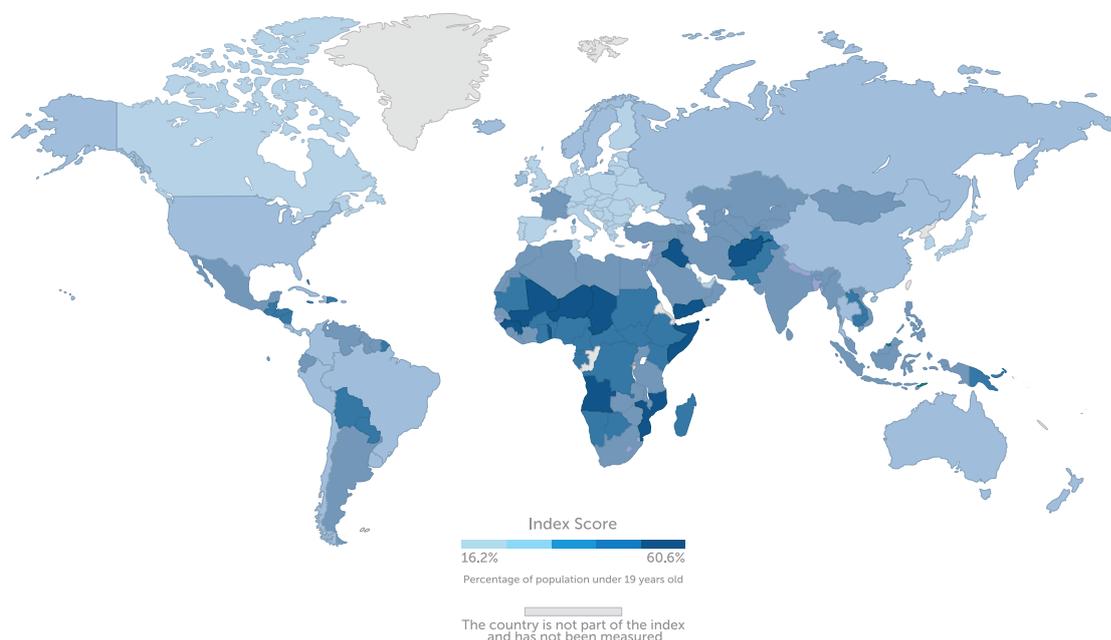
Since 2011, 1.2 billion people have signed up for their first bank account. This has allowed them to participate more fully in local and international marketplaces. And it was achieved in large measure thanks to the growth of digital inclusion and online, particularly through mobile, banking [12].

Research by the ITU shows that increase in the penetration rate of digital services spurs countries' economic growth [8]. Reliable Internet access also increases the chances that someone will be employed by up to 13% [8]. And the adoption correlates with a 2.3% increase in wages [8].

We cannot take these positive outcomes for granted. Globally, there are more than 2.2 billion children under the age of 18 [1]. In some developing countries, children are close to 50% of the population [13]. To realize the full potential of the global digital transformation, these children must be able to access the full range of opportunities the Internet can offer, safely.

Sadly, we know from the experience of developed markets that, without proper safeguards in place, the Internet can be a difficult and – for some – a dangerous environment in which to grow up.

Where do children live?



Source: United Nations, Department of Economic and Social Affairs, Population Division (2019). World Population Prospects 2019, Online Edition.

Most children in the world live in the Global South, particularly in Africa, in nations which are still in the process of digitalization.

In the words of a child, asked by researchers to explain why young people need to be heard on the subject of Internet safety: “It’s important for young people to have a say in these things because a lot of older people try to think about what it would be like as a young person on the Internet, but they don’t realize how vulnerable young people are. So, it’s important that young people get this chance to speak for ourselves” [14].

Children face a range of harms and risks online, from poorly designed services that entrap them (intentionally or not) in age-inappropriate contracts, through cyberbullying and exposure to unsuitable content, right through to severe harassment, online grooming, radicalization, and sexual exploitation and abuse. It is the job of the adult world to find a way to mitigate and prevent these harms and risks.

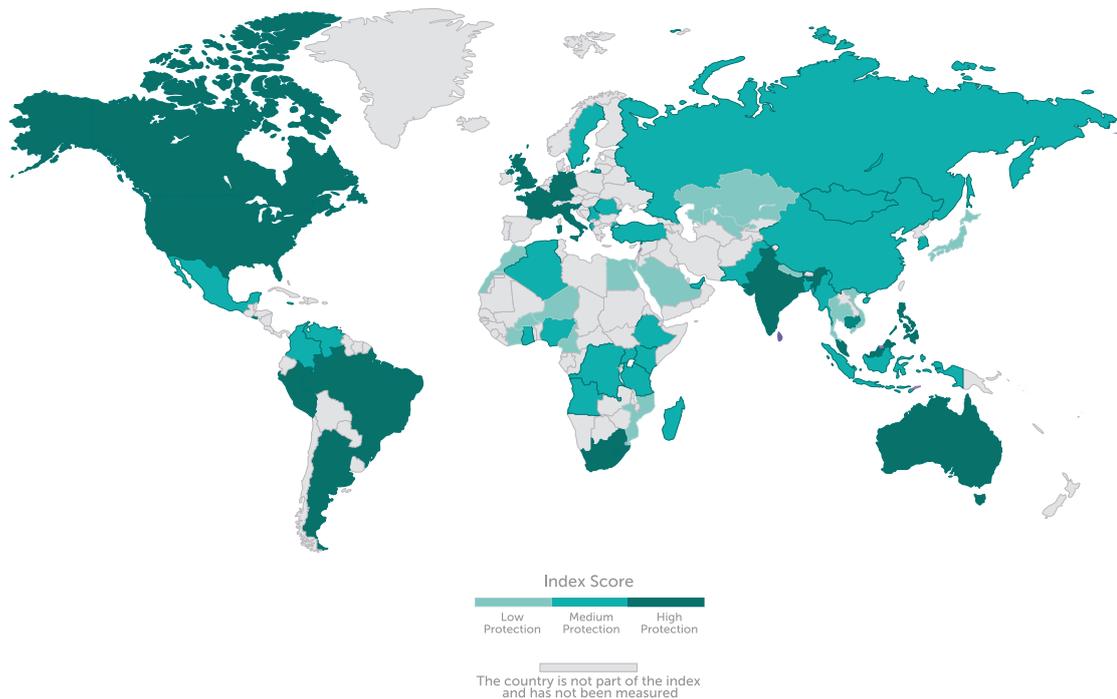
Drawing on the findings of the latest research, this report outlines the broad range of risks that children face online.

It provides a sense of the scale and nature of those risks and recommends concrete and actionable steps that various actors can take to minimize the risks, threats, and harms, and to make children safer online.

Examples of the scale and scope of the problem

- In just one year, the Internet Watch Foundation (IWF) found more than 105,000 websites hosting child sexual abuse material [15].
- In 2018, INHOPE confirmed 223,999 images and videos online as depicting CSEA activity.
- A 2018 study found that most mobile apps aimed at children were harvesting data in ways that breached data-protection regulations — and 19% were collecting personally identifiable information [16].
- It was estimated that > 30% of secondary school pupils will experience cyberbullying [17].

Existence of legislation that seeks to protect children from online grooming



Source: Out of the shadows: shining light on the response to child sexual abuse and exploitation, The Economist Intelligence Unit, 2019.

Of the 60 countries covered by The Economist Intelligence Unit Out of the Shadows Index, only 21 have specific legislation to outlaw online grooming.

Wherever we can collect data we see the same picture — many online platforms and services do not take adequate steps to protect children from a range of harms. As a result, numerous children inevitably fall victim to these harms.

We have learned from countries that have already digitized their economies and social infrastructure that there are concrete steps that can be taken to make children safer online.

These include steps such as:

1. Creating a single authority with ultimate responsibility for child online safety in the country.
2. Ensuring that robust legislation is in place.
3. Ensuring that products and services are safe by design and by default.
4. Building a connected ecosystem in which prevention, detection, and intervention work seamlessly together.
5. Ensuring coordination with different agencies at the national and regional level, such as government entities, private sector, civil society and research institutions.
6. Educating children, parents and caregivers on their rights and ensuring they know who turn to if they need help.

But they also include having reliable statistics and information — consistent across borders — about the experiences of children online.

At present, many agencies collect statistics for the age groups 0-14 and 15-24. This renders children invisible. All data should treat children under 18 years as a distinct group, so that agencies responsible for their welfare have accurate, detailed, and specific information on which to base their

strategies and actions. There is also a lack of agreed common definitions — for instance, identifying who is a child, or what constitutes CSEA — which makes it difficult to build a detailed picture of the state of children's online safety worldwide.

It is to rectify such gaps that the WG developed this report with the goal to prioritize child online safety. The WG's goal is to provide readers — in particular members of government, regulators, private sector companies, including Internet service providers (ISPs), members of civil society, NGOs, and academics — with a single reference point, containing information on best practices, policy responses, and technological tools to use in the struggle against the online abuse and exploitation of children.

Although there are already excellent studies and reports into the safety of children online — many undertaken by the expert members of the WG — often these reports focus on a single issue or form of violence, typically online sexual exploitation and abuse. But this is only one aspect of the online threat environment. There are several other issues, such as bullying, gaming and radicalization to mention a few, that we must collectively address if children are to take full advantage of the opportunities offered to them by the advent of fast, affordable broadband.

The WG recognizes that the majority of the expertise and tools that countries and companies need to tackle these issues are already out there (see the 'resources' section at the end of this report for more details). However, there are technical challenges of detection and enforcement many of which are caused by the rise of online encryption. But an even greater challenge is the lack of awareness among influential stakeholders and decision-makers regarding both the scope and magnitude of child online safety risks, and the tools already available to combat those risks.

The Child Online Safety Initiative since 2010 has addressed these issues by providing a platform for information sharing and awareness raising. The ITU COP Guidelines tackle the issue of child online safety broadly by encouraging stakeholders to take appropriate measures to ensure child protection in the digital world.

A further barrier to the prioritization of the safety and wellbeing of children, is the stigma associated with discussing these risks, especially child sexual abuse. We need to make expertise and tools easy to access, and give those who are eager to be agents of positive change the data and the insights they need to mobilize the commitment to make investments in child online safety.

In this report, we look at the state of children online today. What opportunities are opening up to them? What risks and harms do they face? How could the latter prevent them from grasping the former? And what can we do to ensure that this does not happen? Our key objective and focus is how to prioritize the online safety of all children, but particularly children in low-income countries, where safeguarding structures are often underdeveloped, increasing the risk of harm.

Throughout the report, the WG has done its best to provide resources and suggestions that will be appropriate

to a whole range of markets, each with their own mix of technologies, social pressures and other influencing factors, recognizing that one-size-fits-all is not the solution. This report should be just as useful to readers in low- and middle-income countries, with high levels of mobile-broadband penetration but little fixed-line provision, as it is to those in mature markets.

By working together, across borders, we believe that we can build an Internet ecosystem that fosters the creativity and harnesses the energy of the next generation. With the freedom to explore an increasingly connected digital world, without fear of harm, children will expand their horizons and rise to the challenge of fulfilling their potential. In doing so, they will power the next wave of economic growth and positive social change.

This report, which focuses on children, complements the report by the UN Secretary General's High-Level Panel on Digital Cooperation, which places the safety of children online within the broader context of digital rights and digital cooperation.

The Child Online Safety Universal Declaration linked to this report is a tool to help mobilize and scale up the commitments of governments, the private sector, and civil society to prioritize child online safety through a common framework and concrete actions.

What is a child?

Throughout this report, a child is defined as anyone under the age of 18. This is consistent with Article 1 of the UN Convention on the Rights of the Child (UNCRC), which states that "a child means every human being below the age of 18 years". In practice, some markets treat as an adult anyone who is old enough to consent to data processing, which can be as young as 13 years. This conflation is not justified by any evidence on childhood development milestones. It undermines the rights and threatens the safety of children. See page 63 for a case study outlining the impact of the UNCRC on children's rights worldwide.

What does safer look like?

4



What does safer look like?

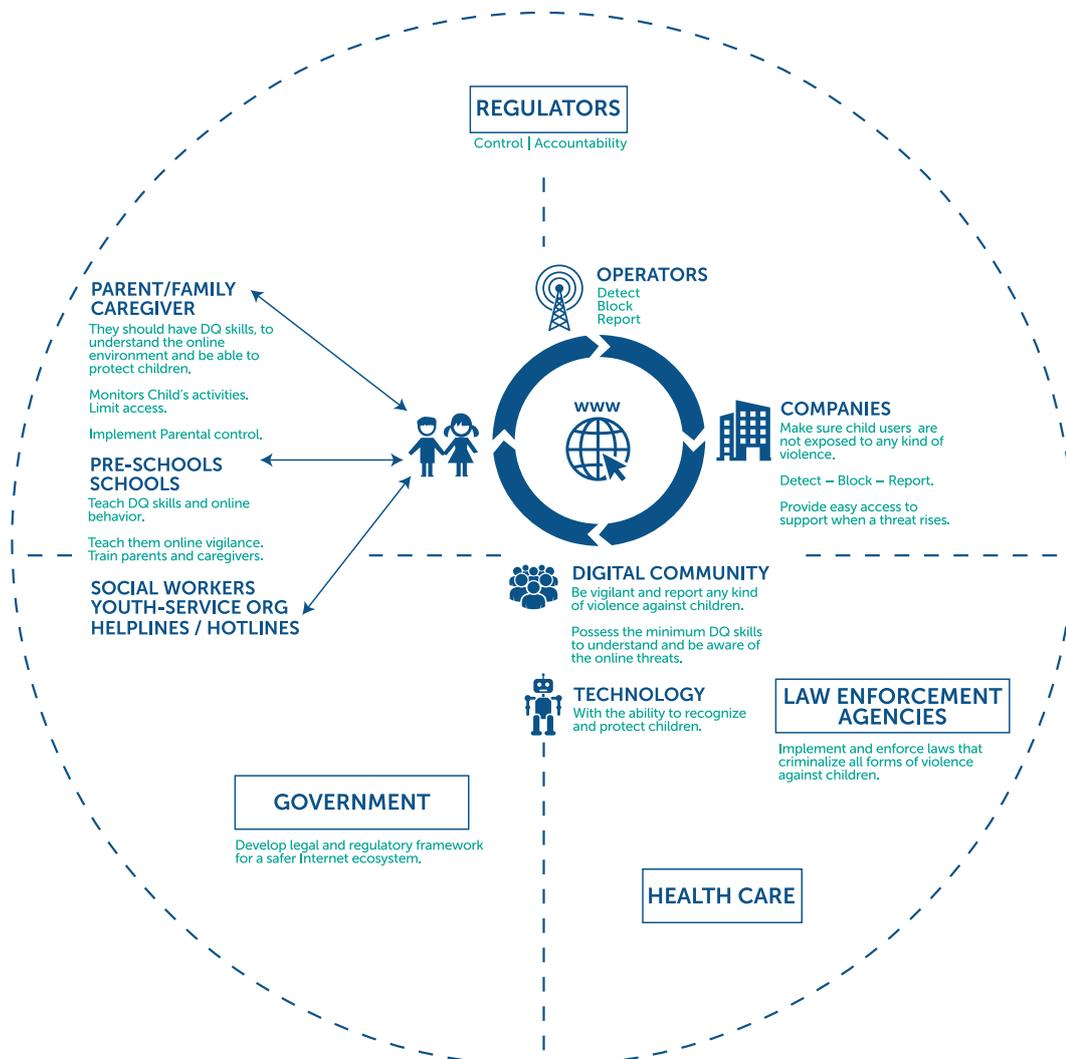
Millions of children in low- and middle-income countries, still in the process of digitalization, are not often adequately protected online. We must rectify this as a matter of urgency, to keep children safe and to ensure they derive the biggest possible benefit from being online.

This is particularly important in developing countries, where a higher percentage of children live today.

These countries stand to benefit most from connectivity, gaining access to quality education, entertainment, health, and other services.

To understand what we need to do to keep children safer when they are online, we must first understand what 'safer' looks like. What would a system in which children were as safe as we could make them look like? And how would a child within that system experience the Internet?

Safer Internet Ecosystem



Source: Lina Fernandez del Portillo.

To fully protect children from online harm or exposure to unacceptable online risk, all relevant stakeholders must be informed, empowered and engaged.

A safer child is protected by a robust legal framework

To protect children against online abuse, a country must have a robust legal framework that defines the rights of children, offences perpetrated against children, and the sanctions those offences incur. A good starting point is to incorporate relevant international conventions into national law.

These international conventions and protocols are:

- **The UN Convention on the Rights of the Child (UNCRC 1989):** this enshrines a wide range of rights for children, including civil, cultural, economic, political, and social rights.
- **UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (2002):** a framework for analyzing approaches to child sexual abuse material (CSAM) offences.
- **Budapest Convention on Cybercrime (2001):** the first binding inter-governmental instrument that deals with computer-facilitated child pornography offences.
- **The Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (2007):** addresses CSAM offences and online grooming offences.

The adoption of the UN post-2015 Development Agenda with 17 Sustainable Development Goals (SDGs) by the UN General Assembly presents new opportunities to prioritize safeguarding children online. A child using the Internet in a jurisdiction that incorporates these provisions and has signed up to the SDGs should enjoy a range of positive rights. These rights should shape the legal and regulatory environment of the Internet service providers and technology

companies that give access to the Internet. They also place obligations on and guide the actions of agencies responsible for children's wellbeing.

For further information, see page 56 for a model of provisions for child online protection, intended as a template for countries to use when updating their national broadband plan.

To read about successful initiatives taken by law-enforcement agencies and their partners in Albania and the Philippines, see the case studies on pages 64 and 65.

A company culture that actively promotes child safety

For children to be as safe as they can possibly be online, they must be able to depend on the companies that provide the services they use to practice active child protection. In its Guidelines for Industry on Child Online Protection (COP) (2015), UNICEF identifies five things technology companies must do to protect children and young people who use their products and services:

1. The rights of children must be integrated into all appropriate company policies and processes.
2. The company must have established processes to deal with breaches of children's rights.
3. The environments that companies offer must be age appropriate.
4. The company must educate children, their parents and caregivers on how to use products responsibly.
5. Digital technology must be promoted as a means of increasing civic engagement.

For more details, read UNICEF's Guidelines for Industry on Child Online Protection: https://www.unicef.org/csr/files/COP_Guidelines_English.pdf

To be safer, children must be aware of their rights

From the youngest age possible, children should know and understand their rights. This empowers the child to recognize when something is wrong to alert a responsible adult, and to be able to report a violation of their rights. For this to happen, teachers and parents must also understand the rights of children online and be able to pass them on, in a language that is appropriate to each child's age [18].

The crucial role of education

To safeguard children; teachers, parents and caregivers should have at least basic digital skills: enough to help their children derive the maximum benefit from being connected, while also recognizing and appropriately responding to potential harms. But in markets experiencing rapid digital transformation, adults often do not have the knowledge to support their children.

The DQ Institute, an international think-tank dedicated to setting global standards for digital intelligence education, has defined eight key areas of digital competencies that a child should master in order to be safe and have a positive experience online.

These eight areas are:

- **Digital identity:** the ability to create and sustain a positive online identity.
- **Digital use:** the ability to use technology in a healthy, balanced way.
- **Digital safety:** the ability to mitigate a range of online risks.
- **Digital security:** the ability to manage and avoid risks to devices and data.
- **Digital EQ:** the ability to recognize, navigate, and express emotions online.

- **Digital communication:** the ability to communicate and collaborate using technology.
- **Digital literacy:** the ability to find, read, evaluate, create, and share digital information.
- **Digital rights:** the ability to understand and uphold human and legal rights online.

All eight competencies are important if a child is to enjoy full access to his or her rights online. In trials, this approach has been shown to be successful. Children trained in the eight competencies were found to have a 15% lower risk of harm online than children who had not been trained [19].

As things are today, UNICEF research has found that 43% of South African children say they never or rarely ask parents for advice about things that happen online [20]. This figure was broadly similar across the markets studied: in Italy, for instance, it's 53% [21], in Serbia 46% [22].

Only education — providing digital skills, including the right of children to be safe online and what all stakeholders can do to secure that right — can fill this gap. And the easiest way to provide this education is through teachers, parents and caregivers. This is why providing digital skills to every child should be a universal right.

Teachers, parents and caregivers play a key role in ensuring children understand how to use digital technology responsibly and safely. Joint meetings and seminars for educators, pupils, parents and caregivers can help sensitize children to the dangers posed by risky online behavior.

Ensuring children are safe by design

To be as safe as possible, a child should be provided with software, apps, and systems that are age appropriate and have been created with children in mind. Built to be safe by design, age-appropriate software or services should:

- Have the best interests of the child as the over-riding design principle.
- Be age appropriate with a robust age-verification function.
- Be transparent and responsible in how it uses and collects personal data.
- Collect and retain only the data it needs to fulfil its function.
- Have policies and standards of behavior that protect children from harm.
- Install with default settings that prioritize privacy over other considerations.
- Only share data in cases of compelling need and in the child's well-defined best interests.
- Should include feedback and reporting from children, parents or caregivers of inappropriate content or behavior.

Ensuring that software, web applications, apps, and websites meet these standards is one of the most important ways in which the private sector, particularly

technology companies, can contribute to safeguarding children online.

To be safe by design, technology must have built-in protections against the following types of risk:

1. Contact risks: the child participates in communication that may lead to harm (this includes risks such as online stalking: predators who pose as children and observe the use patterns of specific children to identify lonely, or otherwise, potential victims).
2. Content risks: the child views unwelcome or harmful content.
3. Conduct risks: dangerous behavior among kids, for instance bullying, sexting, etc.
4. Contract risks: online services should ensure that an adult has consented for the child.

Harms that fall under these categories include CSEA; trafficking; radicalization; illegal or age-inappropriate content and activities; content that promotes harm or self-harm; personal contacts that are illegal or harmful, such as grooming, stalking, or bullying; These age-inappropriate activities are often technically allowed because an online provider's terms and conditions have not been designed with children in mind.

Further reading

Both UK and Australian regulators have produced clear and comprehensive guides to creating systems for children that are safe by design.

In the UK, the Information Commissioner will shortly introduce the Age Appropriate Design Code, a statutory code of practice setting out the specific protections that children merit for their data [24]. It will offer all under-18s a high bar of data protection by design and by default, and apply to all services 'likely to be accessed' by children.

In Australia, the eSafety Commissioner has developed a set of core Safety by Design Principles and has begun work to create a framework of guidance for industry use [25]. The Commissioner is consulting on the tools and resources needed to ensure that user and child safety are embedded into the design of service.

Further information can be found at ico.org.uk and www.esafety.gov.au

The role of technology in making children 'safer' online

Technology on its own won't make children safer. A company or service could have the most sophisticated child-protection software available; yet, if child safety and the right of the child are not foundational to public awareness and education, policy, product design, and operations, children won't be safe. Recent evidence also indicates that parental controls may not be as effective at preventing harm as previously assumed [27].

In the context of the right culture and crime prevention, technology does have a vital role to play as most services have far too many users to rely solely on human monitoring. The right system plays a crucial role in preventing harms and flagging serious behavior for the attention of human moderators.

Relevant child-protection technologies include:

- **Blocking technologies:** usually operating at the ISPs' level, blocking technology recognizes and blocks sites or content that promote harm to children.
- **Heuristic filtering:** technologies that look at variables such as the IP address, content, and keywords, and block sites that aren't blacklisted but may contain harmful content.
- **Automated CSAM detection:** using solutions, such as classifiers, that reference hashed blacklists of CSAM, providers can instantly spot, block, and/or report child-abuse content.
- **Web crawlers:** looking for the same variables as filters (keywords, CSAM images etc.), web crawlers actively search for harmful sites, then alert authorities.
- **Facial recognition:** using facial-recognition technology, authorities and other actors in the sector can quickly identify known victims and perpetrators.

Many of these technologies are powered by artificial intelligence (AI). Without it, neither real-time protection at scale nor pattern-spotting based on long-term trends would be possible, given the volume of data generated every day online.

However, it is worth injecting a note of caution. Leading academics working in AI have warned that many algorithms have biases built in. For instance, because they do not sufficiently control for correlation versus causation, they may mislead human users of the insights they produce into seeing a relationship between two phenomena where in fact no such relationship exists [26].

Another challenge with fully automated solutions is that some of the risks affecting children – grooming and bullying, for example – are context dependent, and those systems do not have the ability to interpret (human) context.

This can lead – among other things – to AI-driven outcomes that discriminate against minorities, women and girls, and other traditionally disadvantaged groups. Given these limits of technology, human review and intervention remains a critically important element in the online child protection space. At this point in time, no child protection AI tools should be utilized in a silo without additional safeguards and protocols to ensure accuracy of data.

Another challenge is that many digital systems are adult-orientated and require nuanced decisions or actions that are not age appropriate. To tackle this problem, we must ensure that systems provide children with special protections and do not expect children to be able to make adult decisions.

A summary of 'safer'

To conclude, a child who is as safe as he or she can possibly be online will:

- Be protected by a robust, effective, and enforced legal framework that protects children's rights.
- Use child-appropriate online solutions and services that were designed to protect children and mitigate risks.
- Be empowered by a set of comprehensive digital competencies that can enable children to minimize risks and maximize potentials on the Internet; recognize when their rights are being violated; and be supported by adults who understand children's rights and how to safeguard them online, who have access to safe and trusted mechanisms to report any violations of those rights.

The state of children online today

5



The state of children online today

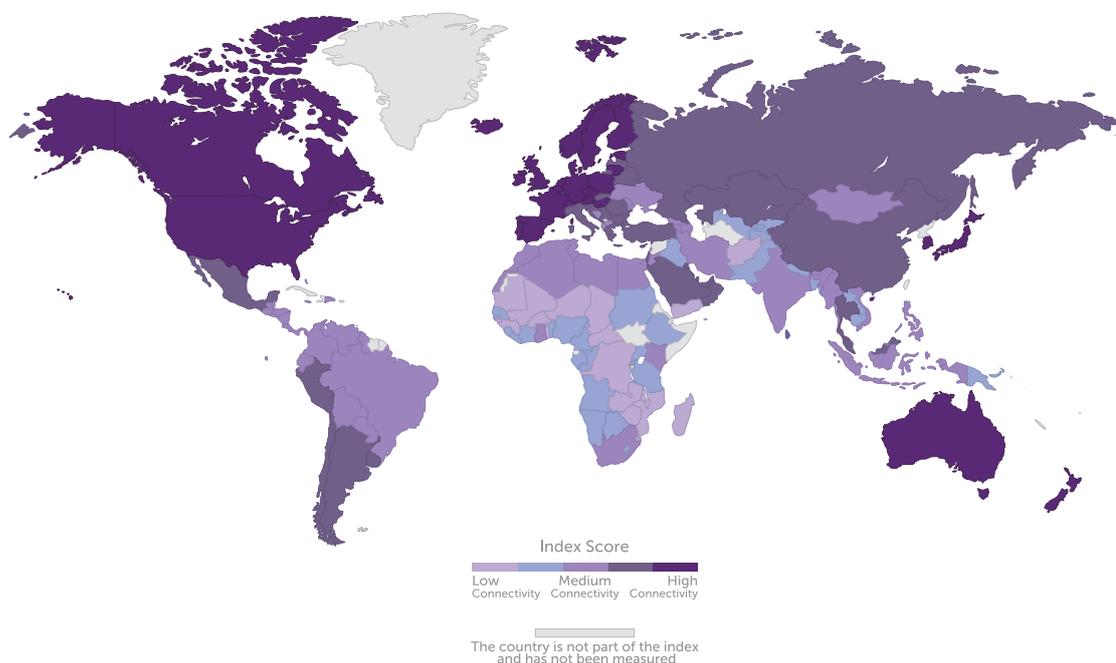
According to UNICEF research, worldwide, 71% of young people are already online [28]. And the availability of affordable smartphones and mobile broadband is making it easier for young people to get online. According to the ITU, in the least-developed countries (LDCs), 35% of Internet users are young people, compared with 13% in mature digital markets [29].

Nevertheless, there are still parts of the world in which millions of young people are still waiting for their first connection. In Africa, for instance, 60% of young people are not yet online [30]. But with the number of African Internet users

growing by 20% a year [31], many of these young people will soon be online. The same is true for the least-developed countries globally, in which 70% of young people are not yet online [29]. There is also a stark gender gap in the least-developed countries: with girls 71% less likely than boys to use the Internet [32].

In Sub-Saharan Africa, Asia and Latin America, connectivity has not yet reached all children. With the expansion of affordable broadband to these parts of the developing world, there is an urgent need to put in place measures to minimize the risks and threats to these children, while also allowing them to capitalize on all the benefits the digital world can bring to our societies.

GSMA Mobile Connectivity Index: State of mobile connectivity around the world by 2018

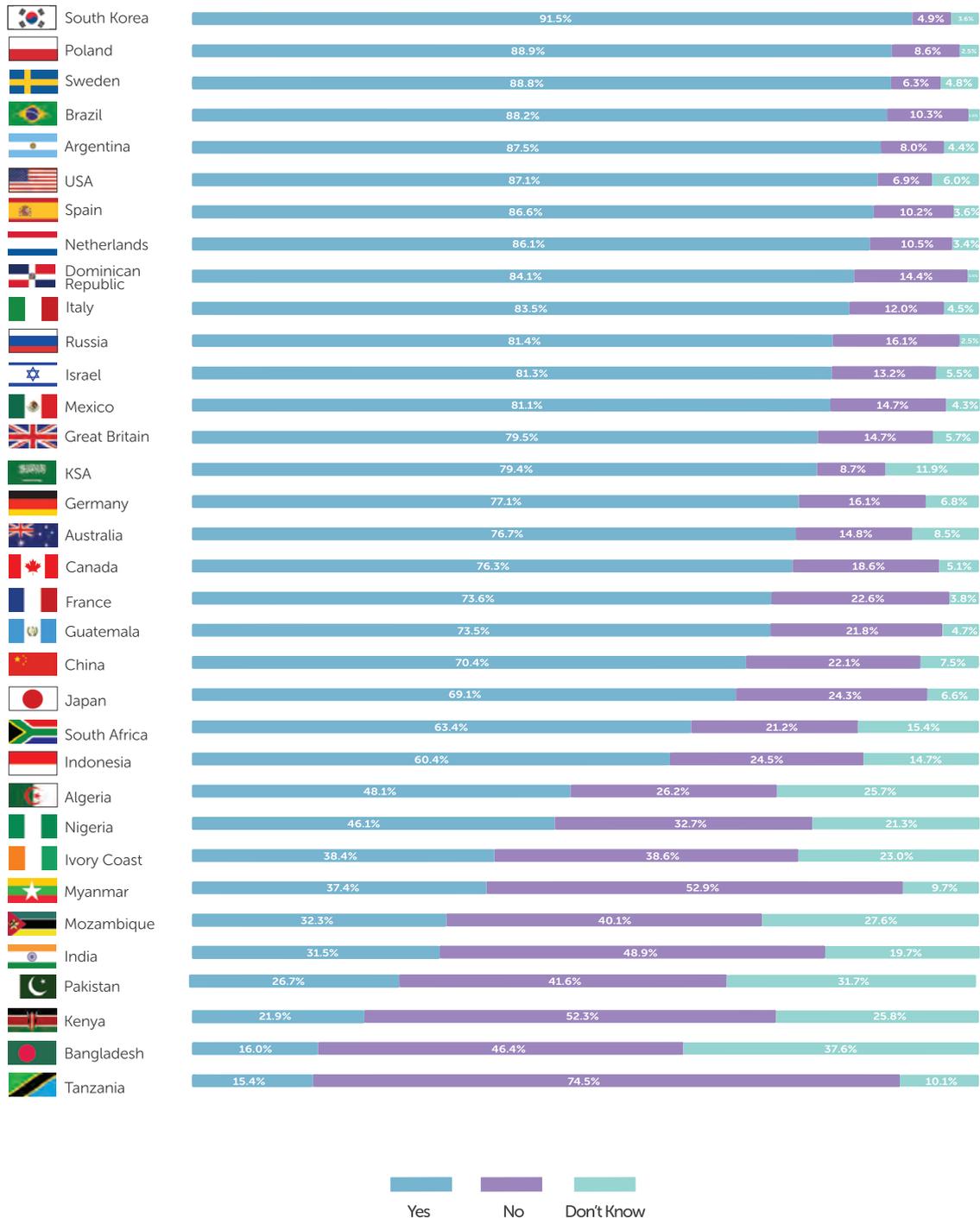


Source: GSMA Global connectivity Index 2019, GSMA Intelligence Unit
<https://www.mobileconnectivityindex.com/#year=2018>

In developed nations, mobile connectivity is becoming ubiquitous. In the near future, this will also be the case for many developing countries.

Children's use of mobile phone to access the Internet in 34 countries.

Has your child/any of your children (aged 5-17) used the internet on a mobile phone in the last 3 months?



Source: GSMA Intelligence Unit

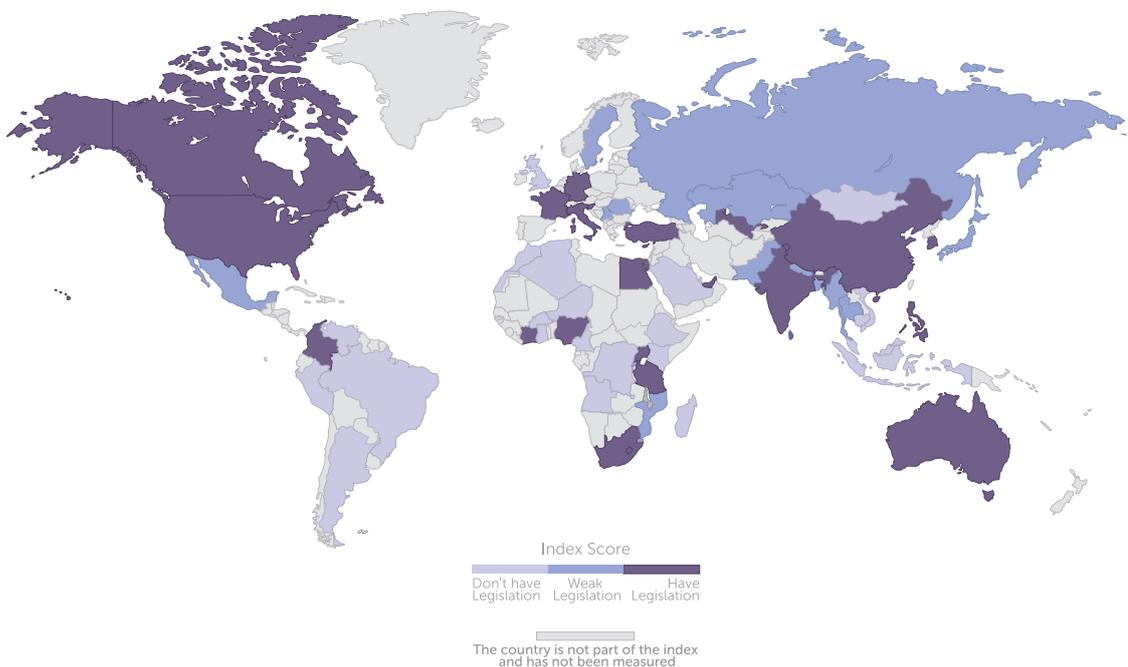
Surveys and studies show that most children in developed, and in many developing countries already regularly use mobile phones to access the Internet.

Why we must act now to protect children

No country has perfect child online protection systems in place. Even in high-income countries with two decades of Internet growth behind them, there are often gaps in the online child-protection eco-system.

Internet protection from a legislative perspective

Mandatory reporting, content blocking, detecting and record keeping of CSAM



Source: Out of the shadows: shining light on the response to child sexual abuse and exploitation, The Economist Intelligence Unit, 2019.

In this case the Index found out that only 9 out of the 60 countries established in their legislation mandatory reporting, content blocking, deleting and record keeping of CSAM. To highlight in this short list, we have China; India; Philippines; South Africa; Tanzania and Turkey. From the three expected actions 11 countries do only two and 15 does only one. And 25/60 don't do anything in this particular matter.

If a renewed global emphasis on digital child safety prompted regulators and legislators to close these gaps, the positive ramifications for children would be profound. In numerous countries, searching questions are being asked about whether relying on self-regulatory mechanisms to achieve progressive change for children is still the best model. Current concerns about the impact of end-to-end encryption on global efforts

to detect and disrupt the distribution of CSAM demonstrates well the urgency of these questions [33] [34].

In some countries undergoing digitalization, there are neither the laws, the policies, the systems, nor the technologies necessary to keep children safe. Aside from a few examples, such as Rwanda (see the Case Study 2 page 63), the push to expand connectivity has not been accompanied by

the same level of effort to ensure children's safety. Not only does this leave millions of children and young people at risk of harm, it risks undermining the ability of digital transformation to deliver the economic and social progress.

The extent of child sexual abuse material (CSAM) online

According to work by the World Health Organization (WHO), every year 200 million children are sexually abused [7]. And increasingly, much of this abuse either takes place online or is captured and digitally distributed. In this case, the Internet is an enabler of abuse and exploitation.

INTERPOL's Child Sexual Exploitation database holds more than 1.5 million images and videos, collectively recording the abuse of more than 19,400 victims worldwide [35]. In the US, the National Center for Missing & Exploited Children (NCMEC) has a database of more than 25 million files containing images of child victims [36]. It is recognized that those numbers are only a small fraction of all of the CSAM available (unique pictures and copies of copies) and that much remains undetected. It is alarming that the number of Cyber Tipline reports received by NCMEC grew nearly tenfold in three years, from 1.1 million in 2014 to 10.2 million by 2017, and almost doubled in 2018 with 18.4 million reports received.

In 2018, the Internet Watch Foundation (IWF) announced a 32% increase in the number of sites reported to it that contained confirmed CSAM [37]. They found the following regarding CSAM content::

- 39% of victims were younger than 10 years, 55% were between 11-13 years, and 5% were 14-15 year old.
- 78% of CSAM material depicted girls, 17% depicted boys, and 4% depicted both sexes.
- 23% of all online CSAM in 2018 was of the severest kind, including images of rape and torture.
- 82% of CSAM was found on image-hosting sites, with no or limited user verification.

INHOPE, the International Association of Internet Hotlines, works with 46 member hotlines in 41 countries. When a member of the public reports CSAM that is hosted in a country other than the one in which the hotline is located, INHOPE informs the hotline in the host country using its secure software solution, ICCAM [107].

The International Survivor's Survey conducted by the Canadian Center for Child Protection also shows that younger children are at higher risk with 56% of the survivors indicating that the abuse they suffered began before the age of four, and 87% were 11 years of age or younger [38].

Research by ECPAT found that 56% of victims in CSAM were prepubescent and 4.3% were infants or toddlers. And the younger the victim, the more severe the abuse was likely to be [39].

According to a report by NetClean, which specializes in solutions that detect CSAM online, 85% of police officers who investigate online child abuse say they have encountered organized groups of offenders running forums and online communities. And almost half of the officers surveyed reported that the number of organized groups was rising [40].

The challenge of self-generated content

In just the first six months of 2019, the Internet Watch Foundation (IWF) received 22,482 reports of self-generated CSAM: a third of all the reports to which the IWF responded. 96% of the victims featured in this content were girls and 85% were aged 11 to 13. These images and videos show children, mainly in a domestic setting, who've been groomed or coerced into performing sexual acts for viewers watching via a webcam. Abusers record the footage and share it online.

Contact risks: grooming, cyberbullying, stalking, and harassment

Cyberbullying is another violation of the rights of children. UNICEF defines cyberbullying as using electronic messages to harass, threaten, or target another person. Often adults are unaware that it is happening, and so they cannot help. Because of connectivity, environments that might once have been a sanctuary for the child, in particular his or her home, are turned into an arena of secret torment. Interestingly, a 2018 study found that teens often regard cyberbullying as normal and do not wish to involve their parents — increasing their isolation [41].

At the same time research conducted in 28 countries, including the USA, China, India, Russia, and Brazil found that, on average, 17% of parents said their children had been a victim of cyberbullying. In some countries, that figure was as high as 37% [3].

Another aspect of bullying is online sexual harassment. A 2017 study of children in Denmark, Hungary, and the UK found that 6% of children had had their explicit pictures shared without their permission. 25% had been the subject of online rumors about their sex lives. And 31% had seen people their own age create fake profiles in order to share sexual pictures of a third party. More worrying still, 9% had received sexual threats from people their own age [42].

Finally, another well-known form of contact-harm is grooming. The International Centre for Missing and Exploited Children (ICMEC) defines grooming as the process by which an adult builds a relationship with a child, to facilitate online or offline sexual contact [43]. Because it's usually a precursor to a more serious crime, statistics on the extent of online grooming in isolation are hard to come by. But the impact on child victims is profound.

Victims report feeling shame, losing confidence, committing self-harm, suffering panic attacks, and feeling a loss of confidence. In a recent report by the Swedish telecoms company Telia, 17% of the children surveyed said their pictures had been circulated on social media without their consent and 7% said they had been blackmailed. Every fourth child said they had received disturbing contacts and messages online, girls more often than boys [44].

Radicalization as grooming

In 2014, three American high-school girls from Denver were intercepted in Germany, on their way to join the Islamic State jihadist group (ISIS) [45]. All three had been radicalized and recruited online. Most Western and Middle Eastern countries have seen similar cases. Nor is the problem confined to ISIS. Worldwide, there are countless extremist groups — including the Taliban, Al Shabab, white-supremacist groups and others — that seek to radicalize and recruit children. Children and young people in these scenarios are extremely vulnerable and, once in the hands of their radicalizers, may find it impossible to escape. That is why it's so important to develop systems for spotting at-risk children before they go from online to offline participation.

Content risks: pornography, CSAM, violence, extremism, gaming and gambling

In the pre-Internet era, it was relatively easy to prevent children accessing harmful or age-inappropriate content. To obtain a license to operate, adult venues had to enforce an age bar. Unfortunately, this is not the case online. It is all too easy for children to find and view adult-themed content related to topics such as gambling, pornography, CSAM and violence.

Many children are now regularly exposed to adult pornography online. A 2018 study in *The Journal of Adolescent Health* found that one in five children aged between nine and 17 see unwanted sexual material online [5].

Another study found that almost 40% of teens wanted to copy the sexual practices they had seen in online pornography [46]. A UK study from 2017 found that four out of five children thought that social media and Internet companies should do more to protect them from sexual material [47].

Many children are also, unfortunately, being exposed to hate-speech and extremism online. A report in the US, found that 37% of Americans were subjected to severe hate and harassment online in 2018. And 38% had either stopped using the service in

question or changed the way they used it [48].

Children may also be exposed to risks through online games. Despite being age restricted, many games do not operate effective age verification. Because of this, children can often access forums and chat functions that are not moderated. They may also be exposed to age-inappropriate sexual and violent game content, cyberbullying, and grooming in the forums and chat rooms [49].

A recent review of the academic literature on gambling found that up to 12% of teens internationally may be problem gamblers [52]. Studies in a range of markets including the UK, Canada, the US, and the Nordic countries found that between 8% and 34% of children under the age of 18 had gambled online at some point [53].

The potential harms associated with problem gambling are significant, as well as the potential of incurring significant debt. A recent study found that problem gamblers were 15 times more likely than average to commit suicide [54].

Finally, children unsupervised online run the risk of viewing violent content more generally, which may be age-inappropriate, upsetting, or even show criminal activity. A study conducted in 2018 found that exposure to violent media correlated strongly with increased susceptibility to anti-social behavior [50].

A study by the EU Kids Online network found that 18% of children said they were worried about exposure to violent online content [51].

Conduct risks: data misuse, financial abuse, and inappropriate behavior

Many services are designed to be age limited, often prohibiting children under 13, in line with the US Child Online Privacy Protection Act (COPPA). But in too many cases, it is trivially easy for children to bypass these age restrictions. Studies by the Pew Center in the US and the NSPCC in the UK have found that by the time they are 12, around half of children already have social media accounts [55] [56].

Potential harms associated with under-age social media use include:

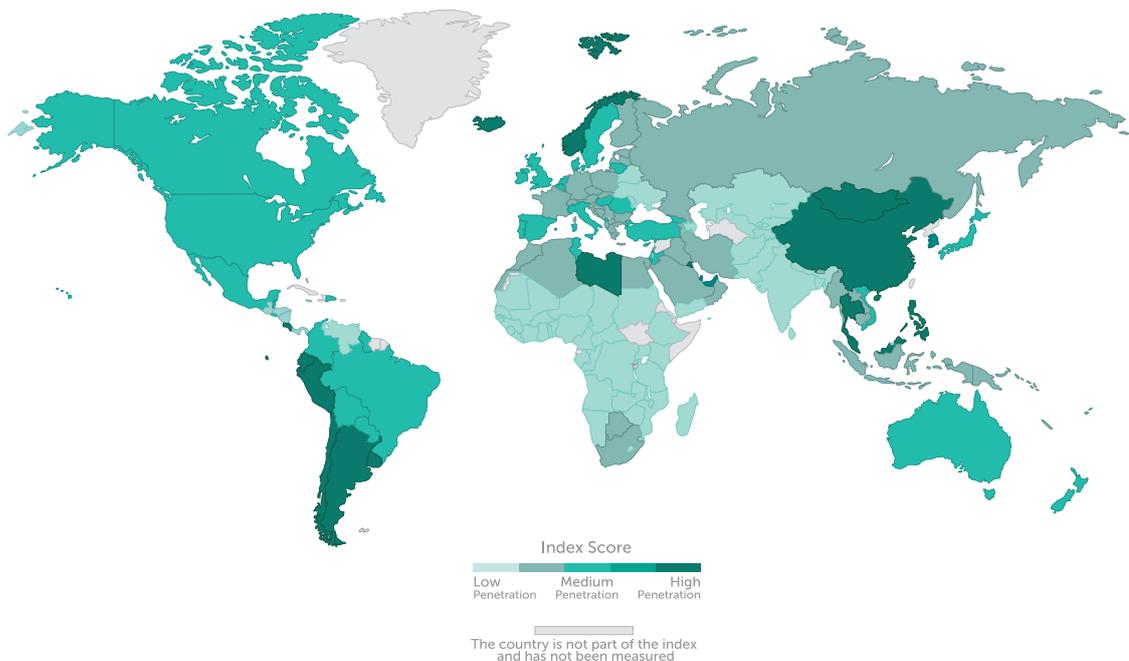
- Low rates of physical activity contributing to childhood poor health [57].

- Sleep disruption, impacting on wellbeing at school [58].
- Anxiety and depression, which studies show to be heightened by social media use [59].

Another risk, which it's all too easy for children to fall foul of, is unintended and unauthorized spending. Many programs offer in-app purchases, often heavily promoted by adverts within the game or application.

A recent study published in the Society for Developmental and Behavioral Pediatrics found that nearly all apps aimed at children contain advertisements, many of which researchers describe as "manipulative". Among other practices, the research noted the frequent use of pop-up ads to interrupt play and game characters urging children to make purchases willingly or unwillingly [60].

GSMA Mobile Connectivity Index: Mobile social media penetration in 2018



Source: GSMA Mobile Connectivity Index 2019, GSMA Intelligence Unit

Young people in many countries worldwide already have access to social media on mobile devices. With broadband expansion social media penetration will rapidly increase, exposing more children to risks and harms online.

Contract risks: how informed is children's consent online?

All of the risks outlined on the previous pages of this section fit within a framework of digital interactions not fit for children. A 2019 study by two law professors found that 99% of online terms and conditions were written in language too complex for the average university undergraduate to understand [6].

Children would have no way of understanding what they were signing up for when they installed the app or logged on to the site. Services and obligations that are designed for adults must be age-limited — so that children cannot sign up to them without a guardian's permission. Without understanding what they are doing, children may sign up for wide-ranging data surveillance. In most contexts, companies are not allowed to treat children in this way. But if their systems do not put the welfare of children first, they may end up doing so anyway.

While online, children also risk spending money without permission of parents or caregivers and having their data harvested. Recent research shows that 90% of third-party apps in the Android Play store harvest user data such as age, gender, location, and usage patterns [61].

Children's digital footprints, and the ability of various platforms to combine and integrate that data to produce insights, has the potential to determine and impact children's futures. We run the risk of allowing an entire generation's childhood to be captured as data, quantified, sold, and re-sold. This data — which could include anything from sensitive personal details, such as date of birth, right through to details of a child's online activity — collected without the informed consent of its under-age subjects, could influence children's later life chances, including their access to education, services, and employment.

A summary of the state of children online

Worldwide, children are too often exposed to harm, abuse, and violence due to the lack of monitoring on the Internet. Even children who do not fall victim to predatory behavior of adults often find themselves disadvantaged by the actions and omissions of services and products that do not take their needs into account or take sufficient steps to protect them [23].

UK Children's Commissioner Creates Child-friendly Terms and Conditions

In 2017, the Children's Commissioner of the United Kingdom created plain-English versions of the terms and conditions for the platforms Facebook, Instagram, Snapchat, YouTube, and WhatsApp. Written with lawyers, these were designed to be easy to understand, so that parents and caregivers could understand what children were signing up to when they joined one of these services. You can find these simplified terms and conditions here:

<https://www.childrenscommissioner.gov.uk/publication/simplified-social-media-terms-and-conditions-for-facebook-instagram-snapchat-youtube-and-whatsapp/>

Opportunities

6



Opportunities

We are undergoing a global digital transformation. Not only does this promise to deliver a range of benefits for children — for instance, increased access to educational, cultural, and economic opportunities — there are also encouraging signs that the technological and social changes it brings about will revolutionize the struggle against online child sexual exploitation and abuse.

Artificial intelligence and the fight against child exploitation online

The development of artificial intelligence (AI) has the potential to help companies and law enforcement process more suspected CSAM or other child-abuse content, and accurately identify illegal material, abusers, and victims more often and faster.

In 2018, Google announced the introduction of a new deep neural network to improve the detection of CSAM. In tests, the company reported that using the AI has helped improve detection and reporting rates by 700% [62].

Microsoft Germany is working with the country's police to develop an AI that can identify CSAM faster [63], as are authorities in the Netherlands [64], Australia [65], and the United Kingdom [66]. The Griffeye Brain tool is an AI classifier that scans previously unseen material to suggest files it believes depict child sexual abuse. It helps speed up investigations and highlight previously unknown child sexual abuse material [67].

Police in the UK are also using AI to find and identify online extremist content of the kind used to radicalize children [68]. Facebook is building an AI-driven system that is designed not simply to identify child sexual abuse material but also conversations that include the tell-tale signs of grooming [69].

Early in 2019, Microsoft organized a hackathon to work with the WePROTECT Global Alliance (WPGA), which brought together engineers and legal and operational experts from Microsoft, Google, Facebook, Snapchat, and Twitter to develop an AI tool to tackle online grooming [70]. In the US, Marinus Analytics has developed AI-powered software that searches online adverts for sexual services to identify victims of trafficking and collect evidence to help police bring traffickers to justice [71]. Thorn has deployed AI technology within its child sex trafficking investigations tool, Spotlight, to give law enforcement in all 50 US states and Canada the ability to accelerate victim identification and reduce investigative time by more than 60% [72].

At the 2019 Code 8.7 conference entitled Using Computational Science and AI to End Modern Slavery, participants raised the possibility of a common international database of victims (such as the INTERPOL Child Sexual Exploitation database) or of traffickers, accessible to law enforcement around the globe [73]. Although less eye-catching than AI or emerging technologies, this would be a huge technological step forward in the fight against the trafficking of children.

There are even plans to use AI to combat cyberbullying and online harassment. Recently, Instagram launched an AI-driven tool to spot and forestall incipient online harassment [74]. In Europe, an EU project called Creep uses AI to spot cyberbullying and to tell the difference between bullying and simple disagreement [75].

Other emerging technologies

Other emerging technologies also have the potential to help in the struggle against child harm online. In chapter 4, we looked at technologies such as list-based blocking, heuristic filtering, and the use of web crawlers to find, detect, report, and block CSAM and other forms of child-abuse content. These technologies are not new, but they have not been widely used.

Other genuinely new technologies being applied to fighting child abuse online include:

- Improved facial-recognition technology that helps to identify child victims of sexual exploitation faster [76].
- Greater processing power and improved image recognition that allows a suspect's 1TB hard drive to be scanned for known illegal content in as little as 30 minutes [77].
- Predictive analytics being used by authorities to identify children at risk of abuse and intervene before abuse happens [78].

As these and other new technologies approach maturity, there will be many opportunities for organizations to use them in the fight against child harm online. What's more, simply the fact of a country being connected to the Internet can simplify and accelerate cooperation between its law-enforcement agencies and companies with those in other countries.

Growing international cooperation

Since 2008, ITU launched the Child Online Protection (COP) Initiative as a multi-stakeholder effort within the Global Cybersecurity Agenda (GCA) framework. This initiative brings together partners from all sectors of the global community

to create a safer and empowering online experience for children around the world. And over the years, the initiative has continuously been raising the issue to the international community.

Another encouraging development has been the increase in cooperation between countries and across sectors to find common solutions in the fight against online child exploitation. Recent global initiatives include the WePROTECT Global Alliance and the Child Dignity Alliance.

Increasingly, law-enforcement agencies are also working cross-border. In 2017's Operation Tantalio, INTERPOL, Europol, and law-enforcement agencies from 15 countries cooperated to arrest 39 subjects and take down an online ring distributing CSAM [79]. In 2019, Thailand, the US, Australia, New Zealand, and Bulgaria worked together to arrest and prosecute offenders in Thailand, Australia, and the United States, and to rescue 50 children [80].

There is also increasing collaboration between hotlines, ISPs, and law enforcement. Through its secure platform ICCAM, INHOPE takes tips from hotlines all over the world and acts on them to remove CSAM in any participating country. Testimony to the value of this approach is the fact that 60% of the videos discovered by ICCAM in 2017 were not previously known to international law enforcement agencies [81].

Threats and the threat environment

7



Threats and the threat environment

Abuses, exploitation, and poorly designed systems that expose children to unnecessary risks are all far too common online. And these harms do not happen in a vacuum. They are enabled by a range of technical, social, and legal factors. To protect children online, it is important to understand the risks they face and the factors behind those risks.

Companies and other bodies could easily minimize some risks at the design stage. They could, for instance, stop the real-time locations of children being available to other users; embed security-by-default in smart devices for the home (preventing accidental streaming); build age-verification and child-centered design into their products and services; and cut back on the use of competitive hooks, which encourage risky behavior.

Another key contributor to the level of risk children face online is the lack of effective and robust mechanisms (including appropriate legislation) by which the state and civil society can respond to those who actively seek to exploit or abuse children online [83].

Middle- and low-income countries may have a less well-developed technological capacity and resources to prevent or investigate online crime. Even high-income countries may lack cybercrime strategies.

And in some cases, laws may not have been updated to include specific offences and instruments relevant to investigating and prosecuting cybercrime [82]. Technology changes faster than legislators and law enforcement can keep up, leaving loopholes for careless innovation or abusers to slip through.

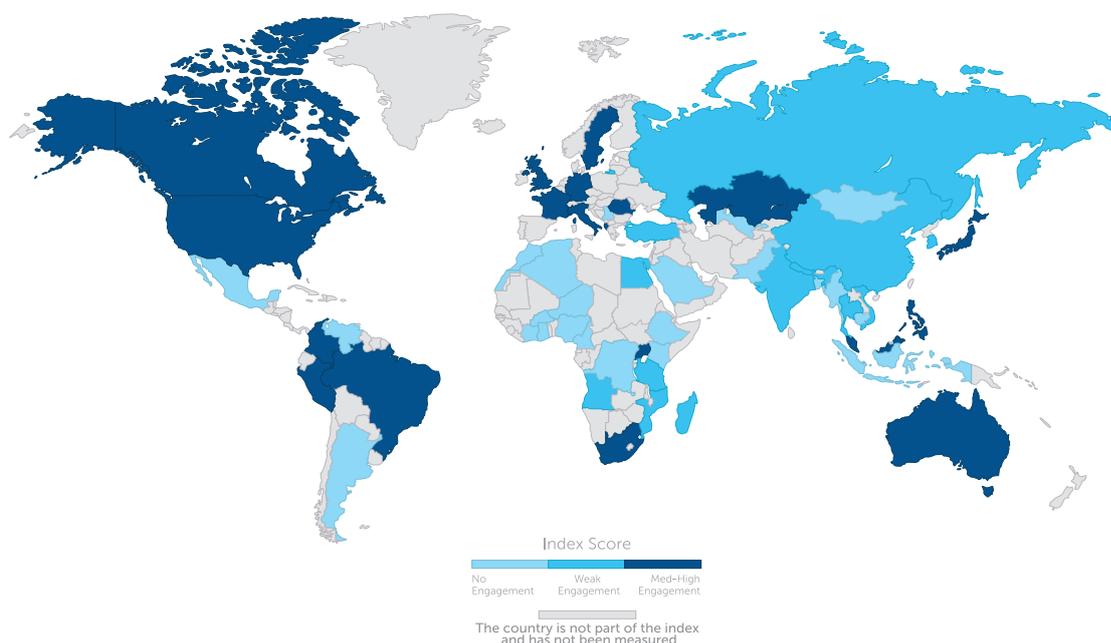
The EIU Out of the Shadows Index

The Out of The Shadows Index [83], developed by the Economist Intelligence Unit (EIU), conducted a study of 60 countries (covering 85% of children worldwide) to assess their ability to respond to sexual violence against children, including online.

The data from this study was used to create an index, with a scope of 100 indicating the highest level of protection and zero the lowest. Among other things, the EIU found that:

- No country is doing enough and only four countries scored above the 75th percentile.
- 11 countries scored less than 50 for the environment they offered children.
- 16 countries scored less than 50 for the quality of their child-protection legal framework.
- 36 countries scored less than 50 for the engagement of civil society and industry.
- 37 countries scored less than 50 on their legal capacity to protect children.

Industry engagement: response to sexual violence against children online



Source: Out of the shadows: shining light on the response to child sexual abuse and exploitation, The Economist Intelligence Unit, 2019.

Of the 60 countries studied by the EIU, in only 10 were there technology industry reporting mechanisms that were actively used to report violence against children online.

Gaps in national policies and laws

As global society undergoes an often-rapid digital transformation, there is a risk that new technologies and approaches are put in place without properly considering the impact on vulnerable members of society – particularly in the case of children.

Many countries do not have sections on children’s needs and rights in their national broadband plans. This increases the chance that public and private entities will create policies, platforms, and services that are not, by design, suitable and safe for children.

To address this problem, UNICEF, the UN Global Compact, and Save the Children have laid out the Children’s Rights and Business Principles [84]. These provide a set of clear and actionable principles that organizations can follow in order to build respect for children and children’s rights into every aspect of their operations.

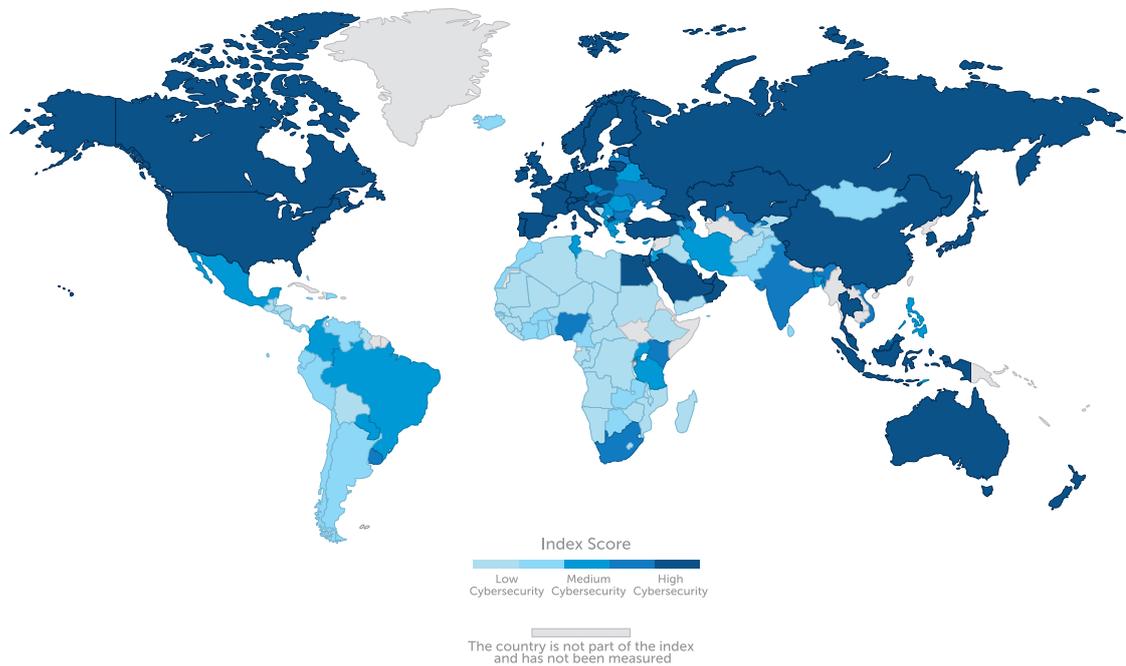
You can find the principles here: <https://www.unicef.org/csr/theprinciples.html>

For a case study on how national legislation and policy can be successfully reframed to protect and enhance children’s rights online, see the case study on page 63, which outlines the work done by the Rwandan government and its partners.

Cybersecurity laws need modernizing

Today, only 72% of countries have functional cybercrime legislation [85]. Even within nations, there is often a lack of consistent legal and operational definitions of what constitutes harm to children online and lack of coordinated action between different agencies. That leads allows criminals operating in jurisdictions with lax legal frameworks to distribute CSAM with impunity, worldwide.

GSMA Mobile Connectivity Index: Cybersecurity Index



Source: GSMA Mobile Connectivity Index 2019, GSMA Intelligence Unit

On the GSMA Global Connectivity Index, many of the countries with the lowest cybersecurity ratings are also the countries with the higher concentration of population under the age of 19.

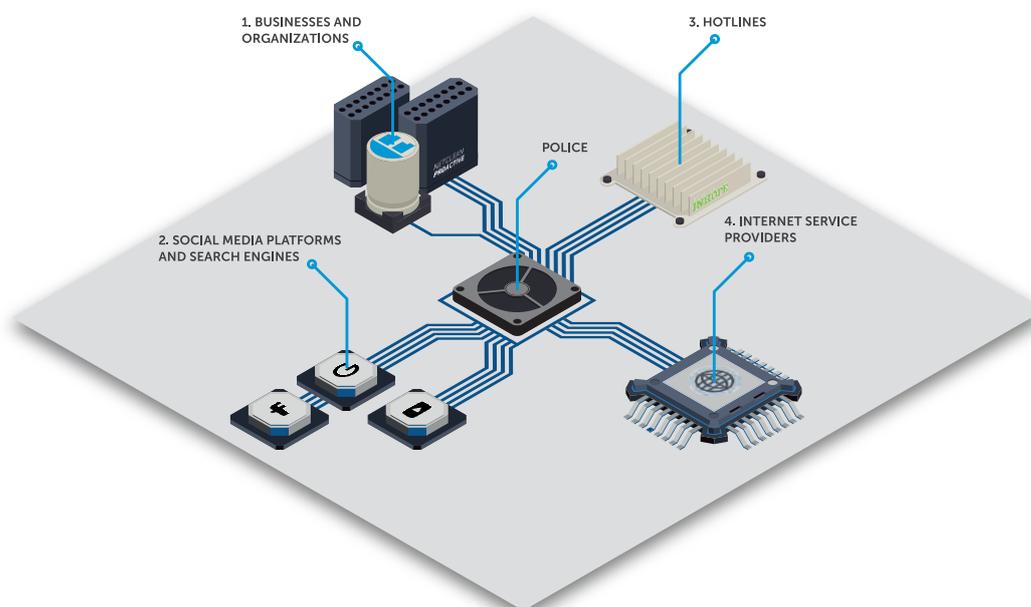
To deal with this, countries must adopt rigorous cyber-security laws that are consistently enforced by properly equipped, resourced, and motivated police forces. Given the cross-border nature of online child abuse and exploitation, it's also important to recognize that child protection is a global issue, requiring international cooperation and harmonized classifications and legal frameworks in accordance with the ITU COP guidelines and UNICEF COP Guidelines for industry [86].

Only with internationally agreed standards and classifications will states be able to share data and pool resources to combat child abuse committed online.

Lack of accountability systems and mandatory standards

Making the Internet a safer place to explore is easier to do when regulators and law enforcers can work closely with Internet service providers (ISPs), mobile network operators, search engines, public Internet facilities, and similar agencies. These companies have the capability to detect child abuse material at the source and forward relevant details to the authorities. But in order to do so, they need legislation and procedures that make clear their role and responsibilities in this process.

Flow of cooperation



Source: NetClean

To succeed in detecting perpetrators, removing CAM and rescuing victims, all stakeholders must work together and know their respective roles.

However, fewer than one in six countries have established in their legislation mandatory ISP reporting, content blocking and deleting, and record keeping. More than 40% of countries have no legislation at all in this regard. Another significant obstacle is gaps in standard definitions and the lack of adherence to the Luxemburg guidelines, which makes it difficult to coordinate the fight against online child abuse and exploitation internationally [87].

The need to understand and track offenders

As well as finding and shutting down the sites and services abusers use to commit their crimes, there is also a need to identify and understand the offenders themselves. This is vital if we are to prevent known abusers revictimizing children but also if we are to learn how to spot potential abusers and intervene before they offend.

Too often, however, offenders go undetected and unpunished. And even when criminals are detected and prosecuted, it was found that up to 8% of those convicted of online child-contact offences go on to reoffend [88].

To increase the detection rates of abusers and reduce the risk of convicted abusers to reoffend, it's necessary to have a greater understanding of what characterizes and motivates offenders — for CSAM crimes but also for other types of offences, including cyberbullying, harassment, and radicalization.

In 2018, Thorn published a report in partnership with NCMEC, that examined trends in actively traded CSAM. Among other findings, this report found that while male producers far outnumber female producers. Cases that involved female producers were more likely to depict extreme intra-familial abuse of younger children. In addition, this research found

that distributed CSAM is becoming more violent over time, with relatively more cases depicting penetration than 10 years ago [89]. According to research by NetClean, the average CSAM offender is male, with more than 50% of police officers never having encountered a female offender [90].

Developing insights such as these is key to helping law enforcement allocate its scarce resources in ways calculated to make the biggest possible impact. And given the growth of darknet sites, which are far harder and more expensive to investigate, preventing first-time and repeat offenses can have a huge impact on the scale of the task faced by law enforcement.

In recent years, there has been an emergence of 'Stop it Now' Helplines offering free and anonymous phone or chat-based counseling and support for people who experience feelings or thoughts of sexual interest in children – potential offenders [91].

A range of threats derived from the misuse of technology

In the early days of the Internet, newsgroup message boards were one of the most significant vectors for the distribution of child sexual abuse material (CSAM). With the rise of the World Wide Web, much CSAM and other abuse content moved from newsgroups to be hosted on websites.

By the mid-2000s, authorities and providers were increasingly aware of the problem of websites hosting CSAM and became more active in shutting down sites and prosecuting both publishers and users of these sites.

This prompted many abusers to migrate their activity to peer-to-peer (P2P) file sharing services. The sheer volume of traffic being deployed by P2P networks made them difficult to police – a problem only exacerbated by the growing use of

encryption. Social media is also popular with abusers as a channel on which to target children and exchange information with each other. To be effective in detecting abuse and exploitation, rescuing children, and prosecuting abusers, we must always address the full range of threats and the complete threat environment. The WePROTECT Global Alliance Global Threat Assessment 2018 identifies the following factors, among others, as significant complications in the fight against online child abuse and exploitation:

- The availability of high-speed Internet enables abusers and the sharing of CSAM.
- The increasing availability of encrypted messaging helps abusers communicate secretly.
- The use of virtual private networks (VPNs) makes it easier for criminals to hide their actions.
- Production costs for rich media, such as video and hi-res photos, is falling all the time.
- Deepfake photo manipulation technology makes it easier to create and hide CSAM.
- Livestreaming allows one-time sharing of CSAM and is difficult for authorities to detect.
- Cheap cloud storage makes it easier for abusers to store and share CSAM online.
- USB storage is now so cheap that moving CSAM is easy. Often these drives are protected by data-privacy laws that are stricter than the laws protecting children.

Encryption and other anonymization technologies are increasingly common and present a significant challenge to tackling the problem of child abuse and exploitation online, both for law enforcement and other entities. Encryption makes it impossible to detect child sexual abuse material until the file is unencrypted, as it reaches the receiver of the encrypted message. To address that problem, it would be essential for legislation to mandate ISPs to have access to image-forensic solutions that will enable them to screen pictures and videos for CSAM. Solutions that can be adopted include PhotoDNA, currently used by many technology companies. Law enforcement also faces the challenge of encrypted storage spaces, that take a lot of effort and technical know-how to break. Legislators should address this challenge prioritizing children's rights while ensuring the right to privacy is not violated.

How gaps in technology enable abuse and exploitation

Software and solutions already exist to help private companies, regulators, and law enforcement detect, report, and otherwise act against sites and services hosting CSAM. Many of these solutions are highly automated and use hashing algorithms to minimize the exposure of staff to harmful content. Many are also available at little or no cost.

To win in the struggle against online abuse and exploitation, all relevant agencies and organizations — including private companies that provide online services — must use the full range of suitable technologies available to close the technical gaps that make it easier for abusers to operate online.

An example of the kinds of technology suites available include:

- **NetClean ProActive:** software based on signature matching and other detection algorithms, which automatically detects child sexual abuse images and videos in enterprise environments.
- **Thorn's Safer:** a tool that can be deployed directly onto a private company's platform to identify, remove, and report CSAM.
- **Griffeye Brain:** an AI that scans previously unclassified content, compares it with the attributes of known CSAM content, and flags suspect items for review by an agent.
- **PhotoDNA:** a tool that creates hashes of images and compares them to a database of hashes already identified and confirmed to be CSAM. If it finds a match, the image is blocked.

For a more complete list of software, see the resources section at the end of this report.

It should be noted that plans by a range of Internet companies to implement end-to-end encryption across their services, including on popular browsers, social media platforms, and messaging services, threaten to nullify the tools designed to disrupt the distribution of CAM and CSAM. These tools are not perfectly compatible with end-to-end encryption. Therefore stakeholders — public and private — must take concrete steps now to ensure that encryption is implemented in a way that allows the tools to continue operating.

The growth of the darknet

The term "darknet" refers to sites and services that, more than just being outside of plain sight, are purposefully hidden using encryption tools and protocols. The best available estimate is that there are about 8,500 sites on the darknet, accessible using the encrypted and anonymized Tor browser [92]. According to research from 2019, roughly 100 of these sites are marketplaces on which illegal goods, potentially including child sexual abuse material, are for sale [92].

Darknet sites may be simple marketplaces or they may act as online communities in which offenders create a shared sense of normality, enabling and encouraging each

other's activities. This encourages abusers to commit increasingly serious crimes. Coupled with the availability of cheap and high-quality camera phones, the darknet is one of the key platforms of online abuse and exploitation today.

According to a study cited by ECPAT International, only 2% of the sites on the darknet host child sexual abuse material, but those sites are responsible for 80% of the traffic on the darknet [93].

The role of children's social and cultural contexts

Children are by nature vulnerable to those who are responsible for their safety. But while child abuse is never the responsibility of the child, there are many factors present in a child's environment and upbringing that can increase their vulnerability to such offences.

A child raised in a culture where secrecy is encouraged, who is exposed to sexual material, or who witnesses situations where sex is exchanged for money, drugs, or protection, can become less able to see sexual violation as unacceptable. A child exposed to violence or oppressive control – or one that has a fear of authority figures – can find it hard to seek protection [94].

Neglect, emotional isolation, or disability can lead to low self-esteem and a poor self-image. This in turn can cause a child to see themselves as undeserving of protection [95]. A major factor in this is often a weak or absent connection to a trusted, safe adult. Children with no framework of protection, runaways for instance, are at particular risk, as are those living in residential care, or children with disabilities [96].

Socio-cultural norms including shame and fear are also significant factors in permitting abuse and exploitation to go unreported. Threats against the child or against others they care about, can lead to an atmosphere of secrecy. Shame and

the fear of being judged can also prevent children from disclosing these crimes [97].

Other factors that may exacerbate the risk of abuse include:

- Social isolation as a result of excessive screen time.
- A lack of age verification, allowing children to access unsafe adult content and forums.
- The sexualization of children in the wider culture.

The problem is far wider in scope than just the influence of a few "bad actors". It includes all of the factors that influence a child's online behavior and that child's ability to access unsafe material and forums. It also takes in the attitudes of adults in that child's life and the nature of the structures within which those adults operate. Do those structures obstruct abuse or facilitate it?

Nor is the role of the social environment only a factor in a child's vulnerability to CSEA: it also determines how safe a child is from the full range of online risks and harms, including grooming, radicalization, and economic exploitation.

The responsibilities of key stakeholders

A great many people have a responsibility for nurturing and supporting children as they grow to adulthood – parents, caregivers, families, educators, health professionals, community leaders, law enforcement, and the private sector for example. But many of these people have little or no training in how to protect children against online risks and harms.

The state must ensure that all these stakeholders can fulfil their role as protectors and know how to play their part in keeping children safe from online harm and helping young people to fully take advantage of the educational, economic, and cultural opportunities the Internet has to offer.

Key actions in supporting stakeholders include:

- Prioritize stakeholder training and invest time and budget accordingly.
- Make educators, parents, and caregivers aware of online risks and how to mitigate them.
- Train providers of children's services to spot when abuse may be happening and intervene.
- Give law enforcement the powers, the technology, and the expertise it needs.

The role of the private sector

8



The role of the private sector

The great majority of the key infrastructure and the services we use every day online were built and are run by private companies. Any effort to safeguard children online must have the backing and full commitment of the private sector, if it is to succeed. Private companies must also commit to properly funding both their own and collective efforts to combat child abuse online.

Companies want to do the right thing by the children who use their services. Nevertheless, the outcomes often leave much to be desired. In just six months in 2018, UK police alone recorded 1,944 cases of grooming on Instagram [98]. Early in 2019, it became apparent that offenders were using YouTube comments to contact children [99]. According to research by an anti-bullying charity, 37% of teenagers who responded said they had been bullied on Facebook [100].

How can the private sector improve its approach to child online safety? To find out, the working group surveyed some of the leaders in the field. This is what the survey told us:

- Companies and NGOs that do child online protection well, base their approach on an established framework – for instance, the WePROTECT Model National Response framework, or “Children’s Rights and Business Principles” (CRBP), developed by Save the Children, UNICEF and UN Global Compact.
- The leaders use a range of technologies, from detecting, filtering, and blocking through to emerging technologies, such as artificial intelligence.
- Child protection policies and strategies are developed in coordination and consultation with a range of internal and external stakeholders, including government, civil society, and children.

- Policies and strategies must tackle the culture and everyday use of digital services that normalize sexual or risky behaviors, or routinely put children in environments designed for adults. Greater commitment must be shown to protecting children’s data, reputations and providing age-appropriate experiences and spaces [23].
- The strategies have clear and measurable goals. Not only does this make it possible to determine success, it also makes it easier for new stakeholders to adopt the campaigns.

Outreach and education also play a key role in successful prevention. Examples include DQ’s #DQEveryChild platform and the EndViolence #SafetoLearn campaign.

- When bottlenecks and obstacles occur, leaders in child online protection actively engage with regulators and other stakeholders to overcome these obstacles.
- The success of online child safeguarding policies and campaigns is tracked and measured. And the metrics are shared with all relevant stakeholders.

Although all of the organizations involved recognized that child online safety is an ongoing learning process, their pursuit of best practice puts them among the leaders in the field. Participants included Airtel, America Movil, DQ, Facebook, Global Partnership to End Violence Against Children, Ericsson, ITU, IWF, Kenyatta University, Microsoft, Moore Center, NetClean, Samena, Telia, UKE, UNESCO, UNICEF, WPGA, and Zain.

The market for tech talent is extremely tight, almost everywhere in the world.

In the US, the economy needs 150,000 more skilled technology professionals than are available [101]. In Europe, that figure is 420,000 [102]. In the Asia-Pacific region, it's one million [103].

In such a competitive environment, the public sector and other organizations dedicated to combating child abuse online often have difficulty in attracting the tech talent it needs to stay ahead of increasingly innovative, motivated, and well-funded online abusers and cybercriminals.

Some private companies — including Facebook, Snapchat, Twitter, and Google [70] — work closely with law enforcement, government, and NGOs

to develop tools and approaches for combatting child abuse and exploitation online. NetClean and Thorn have compiled best practices for private industry in tackling CSAM on their platforms, in addition to offering their tools for companies to detect CSAM [104] [105].

As well as helping specialist agencies, dedicated to promoting child online safety, private companies can also make a significant contribution to promoting children's digital wellbeing by ensuring that all their own services and platforms are safe by design (see page 21 for more details).

Six ways the private sector can help fight online child abuse

There are many ways in which the private sector can contribute to the struggle against child abuse online – here are just six that could make a real difference:

1. By ensuring that their systems and services for children are safe by design.
2. By having prominent, well-resourced reporting and moderating functions.
3. By providing programming and engineering talent to develop anti-abuse technology.
4. By working closely with law enforcement to tackle abuse as quickly as possible.
5. By working with financial regulators and investigators to track the flow of money from abuse.
6. By working to educate teachers, parents, and caregivers to help them keep children safe from harm online.

Recommendations

9



Recommendations

The core objective of the Broadband Commission Working Group on Child Online Safety is to raise awareness of the online risks and threats to children. It also brings forth a set of recommendations to minimize those risks and threats, while simultaneously being able to capitalize on the benefits the expansion of broadband will bring to children, particularly those in developing countries.

The recommendations aim to mobilize political will and collective action by all the key stakeholders. These include governments, regulators, operators, the private sector, social media and gaming platforms, Internet service providers, UN and other child-focused agencies, and the Broadband Commissioners and their peers. Collectively, we must now prioritize child online safety.

The digital world is the world in which most children in developed countries live, play, and learn today. Increasingly, the digital world is also becoming the world of children in developing countries. It should respect children's rights to be free from all forms of violence, abuse, and exploitation. It must become a safer world, preparing future generations to thrive in the digital space.

The goal of these recommendations is to provide a framework that supports collaboration and action among the stakeholders who play an integral role in prioritizing child online safety.

Child Online Safety Universal Declaration

The Broadband Commission for Sustainable Development recommends that all individuals and groups who count themselves as champions for children's rights in the digital space join our collective action by signing the Child Online Safety Universal Declaration to:

Include child online safety strategies in all national broadband and/or digital plans by 2021

In 2003, the Broadband Commission launched a transformative initiative engaging governments to develop national broadband plans. To date, 163 countries have implemented, and are continuously updating, these plans with ITU-supported partners evaluating and holding them accountable.

We call upon all countries to implement evidence-based strategies for child online safety following examples such as the WePROTECT Model National Response (for CSEA and CSAM) and other strategies addressing different types of threats and risks, within their national broadband and/or digital plans.

Prevent, detect, respond, and take action

Domestic and international industry players, including operators, Internet service providers, and social media and gaming platforms, should put in place a set of minimum competencies — technologies, systems, and protocols — to detect and address any sort of abuse (classified as criminal activity) against children. They should also work with civil society to raise awareness of the issues around child online safety and to help all the adults responsible for a child's welfare — including parents and caregivers, schools, youth serving organizations and communities — develop the knowledge and skills they need to keep children safe.

The working definition of online abuse against children must include:

- Child sexual exploitation and abuse (CSEA).
- Child sexual abuse material (CSAM).
- Any other violations of the UNCRC, including cyberbullying, data harvesting, or providing services potentially harmful to children.

When they detect content on their internal platforms or on platforms they operate, oversee as regulators, or have any other form of responsibility for, stakeholders should report and remove such content in collaboration with other relevant actors.

Industry leaders should assist smaller companies with the implementation of technology-driven solutions, capacity development, and reporting processes.

Children's rights to protection from crimes (online as well as offline) should be prioritized without compromising the right to privacy of all Internet users (including children).

Establish clear and accountable mechanisms to ensure child rights are included in operating model

Children are already more than 30% of Internet users. The expansion of broadband in the developing countries of Sub-Saharan Africa, Asia and Latin America will significantly increase this figure.

In recognition of this and of the particular vulnerability of children to online abuse, stakeholders should commit to establishing a senior position, or a team, dedicated to integrating the principles of the United Nations Convention on the Rights of the Child into the organization's operating model.

Companies should report the actions, including outcomes, taken by this team or executive in their annual corporate and sustainability reports. Regulators and other official bodies should include this information in their annual accounting to legislators or other relevant overseers.

Harmonize definitions and terminology and develop common standards

Stakeholders must work together to develop a universal framework for cooperation in the fight against online child abuse. This must include standards for legal interoperability that allows data and intelligence sharing between law-

enforcement agencies and trusted private and civil-society entities.

Across countries and jurisdictions, legislation should aim to adopt consistent definitions and terminology, as well as the classification of online crimes against children in compliance with the WePROTECT Model National Response and other evidence-based models and frameworks. Any existing legal barriers to companies deploying technical tools in the fight to combat violence against children should be removed, including making the legal analysis for child online safety for each country available to trusted private entities at no cost. Countries should develop universal content classification in order to facilitate data sharing.

Technical data should be available across trusted sectors and jurisdictions to facilitate law-enforcement case management efforts and to assist victim identification. Stakeholders should commit to supporting work to produce a greater consistency of practice in relation to the annotation of hashes and data entry. They should guarantee the secure maintenance of data concerning identified and unidentified victims.

Use age-appropriate design and meaningful data-consent for social media and gaming platforms, and others online services for children

All companies that develop or deploy solutions to protect children, or that can be directly or indirectly used by children in any way, should minimize the risks and threats to child online safety. They should take steps to verify ages and identities of users, and prevent the dissemination of hatred, incitement to violence, and the production and distribution of harmful and illegal content such as CSAM. Companies providing online products, services, and apps for children should use age-appropriate design as well as child-friendly terms and conditions. Children should not be asked to consent to things that are not, in legal terminology, 'in the best interests of the child'.

Invest in data collection and research and in the development and scaling up of technology-driven solutions

The private sector should work with other players, such as NGOs and academia, to reduce the siloed and fragmented approach to the development and availability of technical tools (including AI).

The technology that tackles online violations of children's rights should, whenever appropriate, be open source or shared, standardized, platform-agnostic, and placed at the disposal of all relevant and trustworthy parties involved, regardless of sector. Private and public-sector should invest resources and support each other in developing technology solutions to help in the fight against online child abuse.

This work should not jeopardize the work of law enforcement or child safety. There is also the need to invest in research to understand the impacts of new digital technologies on children in order to preempt potential risks and harms, acting before online abusers can take advantage of new technologies, legal loopholes, or online and social phenomena.

Develop common metrics for child online safety

Working together, the international community should develop a universal set of metrics that stakeholders can use to measure all relevant aspects of child online safety. Organizations and individuals can use these metrics to determine the success of child online safety activities when reading the annual reports of institutions and agencies, including but not limited to:

- UNICEF
- The International Telecommunications Union (ITU)
- The International Monetary Fund (IMF)

- The World Bank and other development banks
- The GSMA (mobile industry association)
- The Organization for Economic Co-operation and Development (OECD)
- The European Union
- The African Union
- The Arab League
- The DQ Institute
- The World Economic Forum

Using the metrics from the Economist Intelligence Unit Index and the annual Broadband Commission State of Broadband report will help all stakeholders, across borders, track progress in countries' responses to child sexual abuse and other forms of online violence.

Implement universal digital skills education

All children should be taught digital skills as part of a strategy to minimize the risks and maximize the opportunities of technology.

The teaching of digital skills should be part of the school's core curriculum and should include a broader education of children to manage relationships, build resilience, develop critical thinking skills, and seek help when they need it.

To make this possible, we recommend that leaders from public, private, and civil sectors implement the digital intelligence framework (DQI), developed by the DQ Institute, or an equivalent, at all levels.

For complementary information, see Technology, Broadband and Education report:

https://www.broadbandcommission.org/Documents/publications/BD_bbcomm-education_2013.pdf

Model provisions on child protection for national broadband plans

10



Model Provisions for Child Online Protection To be Included in National Broadband Plans and Cybercrime Laws

These provisions are intended as a template for countries to use when drawing up their own online-child protection section of their national broadband plan.

1.1 Relevant provisions that must be reflected in National Broadband Plans

The following provisions should be included in National Broadband Plans to establish the appropriate foundation for an informed, effective, and enforceable approach to the protection of children online.

1.1.1 Accession to International Conventions and Protocols

The accession to international conventions and protocols demonstrates awareness as well as willingness and commitment by a country to adopt international best practices, codes of conduct, tools, policies, standard terminologies, share information, and to cooperate with other signatories. It also helps to accelerate know-how and the implementation of relevant processes.

A provision should be included that formally sets out the accession of the country to the UN Convention on the Rights of the Child (UNCRC), which entered into force on 2 September 1990. The UNCRC aims to ensure a wide range of human rights for children – including civil, cultural, economic, political, and social rights.

A provision should also be included that sets out the accession of the country to the UN Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, and Child Pornography, which entered into force on 18 January 2002. This is one of the most important international

legally binding instruments that can be used to analyze the legislative and regulatory approaches to address CSAM offences in alignment with relevant international standards.

A provision must be included that sets out accession to the Budapest Convention on Cybercrime of 23 November 2001. This represents the first binding inter-governmental instrument that deals with computer-facilitated CSAM offences.

A provision must be included that sets out accession to the Lanzarote Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse of 25 October 2007. This instrument contains provisions addressing CSAM offences and online grooming offences. It establishes the various forms of sexual abuse of children as criminal offences, including such abuse committed in the home or family, with the use of force, coercion, or threats.

1.1.2 Definitions

Provisions must be set out in the National Broadband Plans and Cybercrime Laws to define what connotes a crime within the context of child online protection. It is anticipated that the following definition may be adopted:

A crime against a child in the online environment shall be defined as:

- Any act or omission including but not limited to the handling of (production, preparation, transmission, storage, publication, or promotion) of content (books, writings, drawings, photos, movies, symbols for the purpose of exploitation, enticement, distribution or display, audio recordings, music, software programs, mobile applications, or electronic games) if the subject matter pertains to a juvenile of less than 18 years of age and if the material depicts or can be used for child sexual abuse.

- Cyber-grooming, sexual exploitation, unauthorized contact, and solicitation of a child to perform unlawful acts.
- Unlawful provision of goods and/or services, meant for adults, to minors and juveniles.
- Provision of goods and/or services that, if used without restriction, may cause minors or juveniles to develop an unhealthy addiction to technology.
- Utilization of online tools to perpetuate the trafficking of children.
- Failing to report an offence against a child or children, within a reasonable period, to the law enforcement authorities or supervisory body when an individual or entity acquires constructive or actual knowledge of such offence.

1.1.3 National Initiatives

Provisions must be outlined in the National Broadband Plans setting out commitments to launch child online protection initiatives based on specific objectives.

For example, the action plan adopted by Sweden:

- The Government's objectives are to ensure that no child in Sweden is subjected to sexual exploitation; no child in another country is sexually exploited by persons from Sweden; child victims of sexual exploitation receive all the support and help they need; and Sweden contributes to effective international cooperation on this issue.

1.1.4 Responsibilities of Intermediaries

A provision must be included that addresses the responsibilities of intermediaries, such as electronic communications network providers

and ISPs. The provision must demonstrate the commitment of the country to ensuring that information, communications, and technology companies undertaking work within its national borders, which act as intermediaries, will take constructive steps to prevent images, videos, and links to child abuse material from appearing on portals managed by the companies. It should include provisions that oblige technology providers to ensure that new encryption techniques do not make it impossible to use tools designed to detect child abuse material, identify victims and gather evidence on offenders.

The law will require ISPs to remove child sexual abuse material from public view as soon as it becomes aware of that material. At the same time, the ISP will report the material and the person or entity which posted it to the relevant law enforcement authorities/ internet reporting hotline. ISPs will not notify the customer in any way that the CSAM material has been removed from customer view, as this runs the risk of alerting offenders to the fact that they are under investigation.

1.1.5 Obligations Imposed on Game Developers

A provision must be included that requires game platform developers to put in place screen-time controls (by default) and other parental controls to monitor and supervise the use of gaming devices and mitigate the adverse effects of long and inordinate use of the devices resulting in addiction. Companies not directly involved in the development, but in the marketing of such online games should endeavor to ensure that game platform developers implement such controls. Gaming platforms that operate chatrooms, forums, and other similar facilities must ensure that children are safe from grooming, bullying, data theft, and other threats when using those features.

1.1.6 Commitment to Working with Third-Party Organizations

A provision must be included that commits the country to ensuring that it works with international third-party organizations, such as the ITU Child Online Protection (COP), the WePROTECT Global Alliance, Global Partnership to End Violence Against Children, Child Dignity Alliance, the Virtual Global Taskforce (VGT), or the Internet Watch Foundation (IWF) to name a few.

The WPGA is an international movement dedicated to national and global action to end the sexual exploitation of children online. The VGT is an international collaboration group of law enforcement agencies, non-government organizations, and industry partners to protect children from online and offline sexual exploitation. The IWF offers a safe avenue for anyone to report suspected online child sexual abuse images and videos anonymously, conducts its searches using the latest technologies and removes illegal content. Additionally, there are other organizations and initiatives addressing cyberbullying or other forms of threats and harms online.

1.1.7 Data Protection

A provision must be included that the country will enforce relevant legal standards of personal data protection and online privacy, particularly for children. The UK government has already done this, with its Data Protection Act 2018, which includes specific data protection provisions for under 18s and is world-leading in taking a privacy-by-design approach. The act builds on efforts that have provided UK legislations with an improved understanding of the role of data in children's online experiences: for instance, the role of data-driven recommendations engines in promoting inappropriate material — such as pro-anorexia sites, self-harm materials, addictive-loop content and so on — to under-age users [106]. Many other countries are now in the process of following suit.

1.2 Relevant Provisions for Cybercrime Laws

1.2.1 Definitions

A provision must be included in the cybercrime law defining what connotes cybercrime against children. The definition set out above in section 1.1.2 will apply.

1.2.2 Establishment of Reporting Mechanisms and Institutional Support Agency for Child Online Protection

A provision must be included that establishes an officially recognized agency that offers institutional support on child online protection. Typically, the Computer Emergency Response Team (CERT) takes responsibility for managing child online protection, reporting to NCMEC, INTERPOL and ICMEC.

Another provision must be included that institutionalizes the establishment of an avenue, such as a portal, telephone hotline, the national child helpline (where operational) or mobile application, through which incidents related to online child protection could be reported. Furthermore, a portal should be made available to inform children, parents, and educators about online threats, best practices, policies, and tools for cyber-safety and through which enquiries or complaints can be made.

Similarly, a portal should be made available that government representatives, law enforcement, non-governmental organizations, and academia can also have access to continue to monitor and restrain online threats. The Global Partnership to End Violence Against Children, with its demonstrated convening capacity, neutrality, and global reach, could play a role in creating a platform for all stakeholders to engage and take action to make children safe online and situate this within the broader agenda focused on ending all forms of violence.

Conclusion

11



Conclusion

Humanity is in the midst of the 4th Industrial Revolution, driven by mass connectivity and emerging technologies such as artificial intelligence (AI), the Internet of Things (IoT), virtual reality (VR) cryptocurrencies, and additive manufacturing (3D printing).

The new industrial revolution, like its predecessor, has the potential to make us richer, safer, and happier. But like its predecessor, it also brings with it many potential harms, to children in particular.

But unlike our 19th-century forebearers, who had relatively little control over their environment and only a partial understanding of the changes they were going through, in the 21st century we have the experience, the technology, and the data to help us understand and predict the benefits but also the risks and harms associated with the ways in which our societies are changing.

We must put this knowledge and expertise to use in the service of safeguarding our children against online harms, as well as harms in the offline world that are enabled or promoted by online activity. We have the opportunity to save millions of children from unnecessary suffering, and to prevent harms that will render our societies incapable of deriving the maximum benefit from the digital transformation that they are undergoing.

The good news is that many of the tools needed to act against the scourge of violence, exploitation, and abuse of children online exist. But too often, the work that goes into creating them in one jurisdiction is not shared in another.

All the stakeholders, spanning from governments, law enforcement, the private sector, and experts, recognize that we also need new and more effective tools that can be shared, are platform agnostic, open source, and/or open access.

The private sector is well positioned to invest in the development and dissemination of technology-driven solutions in cooperation with governments, NGOs (expert community), law enforcement, and other stakeholders. But more support, funding, engagement, and technical expertise from the private sector is still required. However, there is also a need to promote and strengthen support for global initiatives, such as the End Violence Fund, which at present is the leading global initiative investing in the development of technology-driven solutions.

The time and resources spent in the duplication of efforts could have been used in detection and enforcement, or some other area of online child protection. This is why it is urgent that countries cooperate to develop common standards, systems, and protocols. Only by doing so, can our child-protection work be as robust, as efficient, and as fast-acting as it needs to be in order to prevent the scourge of child online violence, particularly, in the developing countries where most children live today and will be getting online in the near future.

Endemic online child exploitation and abuse is preventable, but it requires that we all commit to protect children as they access the Internet. We must work together to empower children across all tiers and lifestyles to gain the benefits of connectivity while avoiding or mitigating the connectivity-related risks they face today.

We recognize that to advance our common vision and goals requires individual and collective actions. Therefore, we need to:

- Incorporate the rights of the child into national broadband strategy and all other relevant areas of national policy.

- Cooperate across borders to create internationally valid standards and terminology for defining and measuring the state of children's rights and protection online.
- Ensure products and services designed for children by public or private sector, or an NGO have children's rights at the heart of their operating principles.
- Work with private-sector, civil society, subject matter experts and partners in developing online children's rights standards for our respective jurisdictions.
- Develop ways to engage relevant local stakeholders in campaigns against harms such as child exploitation and other online children's rights issues.
- Use new and innovative technologies such as AI, data analytics, and data motifs, to prevent networks and services from being used by offenders.
- Make measurable progress toward blocking upload of CSAM and other non-sexual child-abuse or child-harm material in the services and products under our respective jurisdictions.
- Commit our organizations to cooperating cross-border with relevant partners to detect, stop, and, where possible, prevent harm to children online.

To help mobilize all the actors in child online safety space, the WG developed a Child Online Safety Universal Declaration. Building on the recommendations of the report, the declaration is an expression of our commitment to children and their wellbeing.

The purpose of the Declaration is to help mobilize relevant stakeholders, such as technology companies and regulators in a position to directly or indirectly contribute to improving children's safety online.

You can find the declaration at:
https://www.broadbandcommission.org/Documents/working-groups/ChildOnlineSafety_Declaration.pdf

We ask you to please share this report with anyone you know who has influence over matters regarding child online safety.

Case Studies and Best Practices

12



Case study 1: The United Nations Convention on the Rights of the Child

For 30 years, the United Nations Convention on the Rights of the Child (UNCRC) has been the exemplary standard by which to interpret children's rights in multiple environments. Its 40+ substantive articles codify the rights of children and provide a framework by which nation states understand their responsibilities to those under the age of 18. It is the most ratified treaty in history, and more than 190 states are signatories.

Challenge

In nations with deep connectivity, childhood has been transformed by the advent and adoption of technologies that mediate, enhance, and interact with almost all of a child's experiences: from education, play, and entertainment to health, communication, and justice. Conversely, a lack of connectivity or access to the same technology impacts on a child's life chances.

As we set our sights on bringing the global population online, we must consider how to realize children's rights in the digital environment; both their right to be connected in order to participate in society, and — once connected — to maintain and exercise their existing, long-standing rights, to make certain that the adoption of digital technology considers children's flourishing by design and default.

The General Comment on children's rights in relation to the digital environment acts as a supplement to the convention and sets out the relevance of children's rights to the digital world.

Strategy

5Rights Foundation is supporting the Committee on the Rights of the Child

(CRC) to develop the General Comment. Led by Professor Sonia Livingstone, the Committee's Working Group has undertaken an in-depth literature review, a three-month public consultation, and bespoke workshops with more than 400 children from a broad number of contexts across the globe.

An expert consultation hosted by 5Rights Foundation on behalf of the Committee, will take place in London in Autumn 2019. Representing all specializations, different sectors, nations, and contexts, this expert group will conduct a detailed analysis of the first draft. An amended draft will go out for further public consultation, and the submission will be considered by the Committee at its May 2020 meeting.

Once formally agreed, the General Comment will be publicized to a broad group of stakeholders — and will include the publication of academic work, child-facing resources, webinars, and contributions to policy events, platforms, and media.

Outcome

In an interconnected world, if a child is not secure in the enjoyment of his or her rights in one context, he or she cannot exercise them in any context. The General Comment will add to our understanding of how to design the digital world with children in mind, and in doing so solidify and secure children's rights for the digital age.

Case study 2: Online Child Protection in Rwanda (funded by End Violence Fund)

With the rollout of broadband and the increasing affordability of smartphones, Rwanda decided to create a framework that would secure the safety of children online.

Challenge

Rwanda needed a child online safety policy that reflected the concerns of key Rwandan stakeholders, incorporated the best practices of the global community, followed cabinet processes and documentation, and built institutional capacity in a new policy area.

It was in this positive context that the Rwandan government invited 5Rights Foundation to develop a Child Online Protection policy. Working with Professor Julia Davidson of the University of East London, 5Rights Foundation developed a National Child Online Protection Policy and Implementation Plan.

Strategy

A multi-disciplinary project group — consisting of experts in enforcement, childhood abuse and trauma, child development, law, data protection, telecoms, business, education, government service delivery and children’s rights — was formed in the UK to consider key policy areas.

Similar disciplines were identified in Rwanda and, with the support of the Rwandan Ministry of ICT and Innovation, they were able to engage with colleagues from justice, enforcement, education, social work, and family expert backgrounds.

Using a broad gap analysis — including interviews with government members, roundtables, a literature review, and academic workshops — the team developed an understanding of Rwanda’s existing digital capacity.

Issues identified by the gap analysis, together with policy issues raised by existing international treaties and best practice, and observations from the expert working group members, were all incorporated into the final policy and implementation document.

Outcome

The collaboration between 5Rights Foundation and the Rwandan government led to the creation of a high-level policy document, setting out eight policy objectives. This document presented the key areas, responsibilities, enablers and multi-stakeholder work that Child Online Protection demands.

Case study 3: Albania: Safer and Better Internet for Children and Youth in Albania (funded by End Violence Fund)

Albania’s Internet domain “.al” often features as one of the top hosts of CSAM. Despite Albania having ratified all core international legislation relevant to CSAM, between 2016-2018 only 12 alleged child abuse cases were identified by police and only one potential perpetrator was detected.

Challenge

Analysis showed that an unclear and poorly developed legal framework around children’s protection from online harm was contributing to low detection rates. Relevant international conventions are not codified into criminal law and as such, international law cannot be accessed or leveraged.

Strategy

The Albanian 2017 Law on Child Rights and Protection was drafted with UNICEF’s direct technical support. It enshrines the principle of children’s protection from all forms of abuse, harm, and exploitation (offline and online) and hence obliges the government to implement it.

Next, UNICEF set up a solid partnership platform for all key governmental institutions, civil society groups, private sector representatives, and children themselves to consult and discuss concrete procedural provisions for the protection of children from online harm.

Working with a range of public and private stakeholders, the partnership platform created a final draft of secondary legislation, elaborating on the implementation of child protection from online harm, which was drafted within six months and successfully submitted to the Council of Ministers for adoption.

Outcome

In July 2019, the Albanian Council of Ministers endorsed the key decision (a by-law) on “Measures to protect children from harmful and illegal materials online”. This introduces for the first time a clear legal provision and the institutional responsibilities for the protection of children from harmful and illegal content online.

Moreover, it sets the procedures for the immediate removal of harmful and illegal content from the Internet, as well as the reporting and referral pathways for child online abuse, bullying, and sexual exploitation. The impact of this far-reaching outcome will positively affect nearly all children in Albania.

Case study 4: Philippines: Ending Online Sexual Exploitation of Children in Cebu (funded by End Violence Fund)

The Philippines has become a hotspot, and online child sexual exploitation and abuse (CSEA) is growing rapidly. Its government decided that something had to be done.

Challenge

In just one month in 2015, the Philippines received more than 2,600 referrals from the US, notifying it of newly detected Filipino child abuse websites. Until the laws in the Philippines are more effectively enforced, these numbers will continue to climb.

Strategy

The International Justice Mission (IJM), a human-rights NGO, partnered with the government of the Philippines to strengthen its capacity to address online child sexual exploitation and abuse (CSEA), in particular the exchange of live-streaming sexual abuse of children and other child exploitation material between paying customers and child traffickers.

IJM worked with the justice system to rescue and rehabilitate victims, hold perpetrators accountable for crimes, increase the capacity of local authorities, and diagnose specific gaps in the public justice system that resulted in impunity.

The NGO also partnered directly with local and international law enforcement agencies – including police and court systems – to identify and rescue victims, arrest perpetrators, and gather sufficient evidence to support criminal prosecutions.

Outcome

As of July 2019, IJM and the Filipino authorities working together have rescued 123 children from sexual abusers. As well as rescuing victims, IJM has helped police apprehend and charge 20 suspected perpetrators and support prosecutors in filing charges against suspects, while supporting national and local prosecutors in ongoing cases.

IJM further strengthened capacity through the training of more than 50 Filipino law-enforcement officers, and 100 judges and prosecutors on the intricacies of investigating and trying these crimes. IJM continues to advocate with the Philippines Congress and other agencies to deliver on the government's three-year commitment to strengthen personnel and the funding of the national Women and Children's Protection Unit.

Case study 5: 'I Click Sensibly' – Digital Education in Poland

UKE is the regulatory body responsible for overseeing the Internet in Poland. It knew that very young children were often using smartphones with few or no restrictions or guidance.

Challenge

The regulator needed to know what kinds of things children were doing online and what risks might be involved. Beyond that, it needed to find a way to educate children and parents on how to be safer online and how to understand and manage risk.

Strategy

In response to these challenges, UKE created the 'I click sensibly' campaign. This had two parts. The first was a series of classes on Internet safety. During dedicated classes trainers from the Office of Electronic Communications discussed how to surf online responsibly, what they should be aware of when surfing online and how to use telecommunications devices safely.

Children attending the workshops were also taught how to deal with cyberbullying or hate-speech, how to deal with online aggression, and how to protect their data. The classes also taught parents how to filter inappropriate

content and to control how children spend their time on the Internet.

At the same time, UKE surveyed many of the children who attended the classes to find out how they used the Internet and what risks and harms they might be exposed to. Surveys were carried out using computer-assisted personal interviewing.

Outcome

More than 50,000 children benefited directly from the classes. Using the survey, UKE was also able to gather detailed data on how children spent their time online, what risks they were exposed to and how well equipped their parents were to support them. At a time when many national and international agencies don't even have data on children's online lives, UKE has detailed statistics on subjects, such as what percentage of children have been ridiculed or harassed online, how well children are able to evaluate the accuracy of information they find on the Internet, and how many parents exercise control over what their children do and see online.

Case study 6: Peru: Intersectoral and interdisciplinary collaboration to prevent and respond to the reality of online child sexual exploitation in Peru (funded by End Violence Fund)

According to the Institute of National Statistics, around 50% of 6-17-year-olds use the Internet in Peru. The country's

Interior Ministry stated that, between 2014 and 2017, 22% of registered trafficking for sexual exploitation cases began online. This echoes wider findings by the Child Rights International Office cautioning that ICT is being used to groom children online in order to then traffic them for sexual exploitation.

Challenge

Peru already has a relatively robust policy and legal framework for combatting child sexual exploitation when compared with its Latin American counterparts. They have signed the SDG, the CRC, the WPGA Model National Response Statement of Action, and the Budapest Convention on Cybercrime. However, the number of complaints and cases that come to court are low. What's more, none of these policies or frameworks explicitly mentions how to approach and deal with the ever-increasing issue of online CSEA. There are also huge gaps around information on CSEA, the new forms of online exploitation, the resources and mechanisms to protect children, and the coordination between sectors, training, and awareness.

Strategy

With financial support from the End Violence Fund and Capital Humano y Social (CHS) Alternativo, (Alternative Human and Social Capital) — a non-governmental human rights organization based in Peru — the country developed changes to the Peruvian Penal Code that expanded the definition of child sexual exploitation and criminalized this activity in every setting. The most important contribution of CHS was the technical support provided to the Women and Family and the Justice and Human Rights commissions of the Congress of the Republic.

Thanks to CHS and supporting organizations' efforts, 10 articles of the penal code are set to be modified, and seven others will be added. The proposed changes create specific

criminal offences and sentences relating to the sexual exploitation of children, receiving a benefit from child sexual exploitation, coordinating it, promoting it, or favoring it. Paying to have relations with a child is also covered by the revised code.

In addition to working for systemic change, CHS has also raised awareness of the threat and educated close to 400 children and 600 community members (teachers, parents, and service providers) directly on how to respond to child sexual exploitation, both by engaging the mainstream media and delivering in-person training respectively.

Outcome

Congress approved the bill, and the final version was signed into law by the President of Peru in June 2019.

Case study 7: Online Child Protection in Vietnam (funded by End Violence Fund)

As the number of young people online in Vietnam soared, so did the risks. To tackle the problem of online safety, ChildFund Vietnam instigated the Swipe Safe initiative.

Challenge

By 2018, young people aged 15-24 made up more than one third of Vietnam's 54.7 million Internet users. This has increased their exposure to all forms of online sexual abuse and other dangers online, and led to one in three students suffering from cyberbullying.

This is further exacerbated by low levels of digital literacy in both children and their parents. With a lack of tools and material promoting online safety, there is poor understanding of risky online

behavior and little or no advice on how to stay safe online.

Strategy

In order to help young people navigate the Internet safely, ChildFund Vietnam established the Swipe Safe initiative. This program educates on the potential risks online, such as cyber scams, bullying or sexual abuse, and presents advice on methods to stay safe.

Swipe Safe encourages parents, children, schools, and the private sector to play an active role in the online safety of children. It provides training for parents and Internet café managers to identify and address risks to children. It also supports schools in developing child-friendly policies and guidance on online safety.

A key innovation of the program is to engage young volunteers with extensive knowledge of technology to train others in their local communities. These trainers directly relate to the experiences of other young people and help keep the curriculum up to date.

Outcome

As of June 2019, more than 8,700 adolescents, 1,100 parents and 1,000 “online safety partners” (including government officials, school representatives, and Youth Union members) have received online safety training through the program.

Surveys indicated that 91% of the targeted children demonstrated increased online safety knowledge. This included skills such as privacy setting, information checks, responsible sharing, online searching, and reporting harmful content. Of those surveyed, 89% knew where to go for support and 30% felt safer online.

Case study 8: Using technology to keep children safe: Facebook’s work with NCMEC

Challenge

Child sexual abuse is a horrific crime affecting an estimated 9–19.7% of girls and 3–7.9% of boys. Safety experts, NGOs, governments and companies all have an interest in disrupting and preventing the sexual exploitation of children across online technologies and need to work together when possible to be most effective.

Strategy

As the nation’s clearinghouse and comprehensive reporting center for all issues related to the prevention of and recovery from child victimization, the National Center for Missing and Exploited Children (NCMEC) leads the fight against abduction, abuse, and exploitation.

Since 2016 Facebook hosts an annual cross-industry Child Safety Hackathon for developing new tools and technology for child safety non-profit partners like NCMEC. The two-day event brings together engineers and data scientists from Technology Coalition partner companies and others to develop new technologies that help safeguard children. Hackathons are an exciting way to bring people together from different organizations with a wide range of expertise to build tools that tackle problems such as the online sexual exploitation of children. All open-source code and prototypes developed at the Child Safety Hackathon are donated back to the Technology Coalition and safety partners such as NCMEC to be used in their child-safety efforts.

Building on Microsoft's generous contribution of PhotoDNA to fight child exploitation 10 years ago and the more recent launch of Google Content Safety API, at the 2019 Child Safety Hackathon, Facebook also announced it is open-sourcing two technologies that detect identical and nearly identical photos and videos — sharing some of the tech they use to fight abuse on their platform with others who are working to keep the internet safe. These algorithms are open-sourced on GitHub so industry partners, smaller developers and non-profits can use them to more easily identify abusive content and share hashes — or digital fingerprints — of different types of harmful content. For those who already use their own or other content matching technology, these technologies are another layer of defense and allow hash-sharing systems to talk to each other, making the systems that much more powerful.

Outcomes

Among the prototypes developed at the hackathon are projects that improve efficiency for people working to identify and rescue children by making it easier to rapidly sort through images and data and prioritize cases. For example, in 2019 teams developed a prototype feature that will allow NCMEC's CyberTipline case management tool to query and compare data points within other nonprofit organizations' databases for known hashes and other key information. This will help identify children at risk and highlight high value reports. The prototype that won in 2018, dubbed "Spotting Trends," makes use of clustering analysis and information that is associated with known child sex traffickers to help ensure that these individuals are not able to resurface elsewhere on the internet. And the success and real-world application of the prototype that took home top prize in 2016 — a child finder that matches online photos with those available in NCMEC's database of missing children — confirms the benefit of using technology

to help tackle these challenging issues. Technology of this sort has the potential to reduce law enforcement's response time, getting children who may be vulnerable help faster and more efficiently.

Glossary

13



Glossary

AI – Artificial Intelligence

CAM – Child Abuse Material

COPPA – The US Child Online Privacy Protection Act

CSAM – Child Sexual Abuse Material

CSEA – Child Sexual Exploitation and Abuse

Cyberbullying – Bullying conducted using electronics channels, such as chat rooms, social media, email, and SMS

Darknet – Websites and services which are encrypted to prevent users or publishers being tracked

Deepfake – A highly realistic photo or video simulation that looks like a real person

GDP – Gross Domestic Product

Grooming – The process by which an adult builds a relationship with a child, to facilitate online or offline contact for purposes that will harm the child (for instance, radicalization or sexual abuse)

Hashing – A technology that creates a unique signature for a digital file, used in the automated detection of CSAM

ITU – International Telecommunications Union

LEA – Law-Enforcement Agency

SDG – Sustainable Development Goals

UN – United Nations

UNCRC – United Nations Convention on the Rights of the Child

UNICEF – United Nations Children's Fund

WG – Working Group

WHO – World Health Organization

WPGA – WePROTECT Global Alliance

References

14



References

1. UNICEF DATA. (2019). The State of the World's Children 2017 Statistical Tables. [online] Available at: <https://data.unicef.org/resources/state-worlds-children-2017-statistical-tables/> [Accessed 5 Aug. 2019].
2. Loritz, M. (2019). UK-based Cyan Forensics partners with major US nonprofit to stop child sexual abuse | EU-Startups. [online] Eu-startups.com. Available at: <https://www.eu-startups.com/2019/08/uk-based-cyan-forensics-partners-with-major-us-nonprofit-to-stop-child-sexual-abuse/> [Accessed 25 Aug. 2019].
3. Comparitech. (2019). Cyberbullying Statistics and Facts for 2016 - 2019 | Comparitech. [online] Available at: <https://www.comparitech.com/internet-providers/cyberbullying-statistics/> [Accessed 8 Aug. 2019].
4. Dqinstitute.org. (2019). Outsmart Cyber-Pandemic. [online] Available at: https://www.dqinstitute.org/2018DQ_Impact_Report/ [Accessed 6 Sep. 2019].
5. The Prevalence of Unwanted Online Sexual Exposure and Solicitation Among Youth: A Meta-Analysis, Madigan, Sheri et al. Journal of Adolescent Health, Volume 63, Issue 2, 133 – 141
6. Benoiel, Uri and Becher, Shmuel I., The Duty to Read the Unreadable (January 11, 2019). 60 Boston College Law Review, Forthcoming. Available at SSRN: <https://ssrn.com/abstract=3313837> or <http://dx.doi.org/10.2139/ssrn.3313837>
7. Lu, J. (2019). Here's How Every Country Ranks When it Comes to Child Abuse and Child Safety | UN Dispatch. [online] UN Dispatch. Available at: <https://www.undispatch.com/here-is-how-every-country-ranks-on-child-safety/> [Accessed 8 Aug. 2019].
8. Generation Unlimited: Business Plan for Digital Connectivity, UNICEF, 2019.
9. Itu.int. (2019). Press Release. [online] Available at: <https://www.itu.int/en/mediacentre/Pages/2018-PR40.aspx> [Accessed 3 Aug. 2019].
10. Provider, S., Forecasts, V. and Papers, W. (2019). Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper. [online] Cisco. Available at: <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html> [Accessed 3 Aug. 2019].
11. Katoa 'Utoikamanu, F. and Sanou, B. (2019). CTs, LDCs and the SDGs Achieving universal and affordable Internet in the least developed countries. [online] Unohrlls.org. Available at: <http://unohrlls.org/custom-content/uploads/2018/01/D-LDC-ICTLDC-2018-PDF-E.pdf> [Accessed 3 Aug. 2019].
12. World Bank. (2019). Gains in Financial Inclusion, Gains for a Sustainable World. [online] Available at: <https://www.worldbank.org/en/news/immersive-story/2018/05/18/gains-in-financial-inclusion-gains-for-a-sustainable-world> [Accessed 3 Aug. 2019].
13. Uis.unesco.org. (2019). Sudan | UNESCO UIS. [online] Available at: <http://uis.unesco.org/en/country/sd?theme=education-and-literacy> [Accessed 3 Aug. 2019].
14. 5rightsfoundation.com. (2019). The Internet On Our Own Terms. [online] Available at: <https://5rightsfoundation.com/static/Internet-On-Our-Own-Terms.pdf> [Accessed 6 Sep. 2019].
15. Iwf.org.uk. (2019). Once Upon A Year: The Internet Watch Foundation Annual Report 2018. [online] Available at: <https://www.iwf.org.uk/sites/default/files/reports/2019-04/Once%20upon%20a%20year%20-%20IWF%20Annual%20Report%202018.pdf> [Accessed 5 Aug. 2019].
16. Reyes, I., Wijesekera, P., Reardon, J., Elazari Bar On, A., Razaghpanah, A., Vallina-Rodriguez, N. and Egelman, S. (2019). "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. [online] Petsymposium.org. Available at: <https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf> [Accessed 5 Aug. 2019].
17. Patchin, J. (2019). 2016 Cyberbullying Data - Cyberbullying Research Center. [online] Cyberbullying Research Center. Available at: <https://cyberbullying.org/2019-cyberbullying-data> [Accessed 5 Aug. 2019].

18. Atchoarena, D., Selwyn, N., Chakroun, B. and Fengchun, M. (2019). Working Group on Education: Digital skills for life and work - September 2017. [online] Unesdoc.unesco.org. Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000259013> [Accessed 6 Sep. 2019].
19. World Economic Forum. (2019). Cyber-risk exposure among 8-12-year olds drops by 15%. [online] Available at: <https://www.weforum.org/our-impact/helping-young-people-safely-navigate-the-digital-world> [Accessed 6 Aug. 2019].
20. Byrne, J. and Burton, P. (2019). Children as Internet users: how can evidence better inform policy debate? [online] Taylor & Francis. Available at: <https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1291698?hooPostID=1753d7ca474ab7a748bcee5f22ffe65e> [Accessed 7 Aug. 2019].
21. Mascheroni, G. and Ólafsson, K. (2019). Access and use, risks and opportunities of the internet for Italian children. [online] Globalkidsonline.net. Available at: <http://globalkidsonline.net/wp-content/uploads/2017/10/Executive-summary-Italy-june-2018.pdf> [Accessed 7 Aug. 2019].
22. Globalkidsonline.net. (2019). GLOBAL KIDS ONLINE SERBIA: Balancing between Opportunities and Risks: Results from the Pilot Study. [online] Available at: http://globalkidsonline.net/wp-content/uploads/2016/05/Country-report_Serbia-final-26-Oct-2016.pdf [Accessed 7 Aug. 2019].
23. 5rightsfoundation.com. (2019). Towards An Internet Safety Strategy. [online] Available at: https://5rightsfoundation.com/static/5rights_Towards_an_Internet_Safety_Strategy_FINAL.pdf [Accessed 6 Sep. 2019].
24. Ico.org.uk. (2019). Age appropriate design: a code of practice for online services. [online] Available at: <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/age-appropriate-design-a-code-of-practice-for-online-services> [Accessed 6 Sep. 2019].
25. Office of the eSafety Commissioner. (2019). Safety by Design. [online] Available at: <https://www.esafety.gov.au/esafety-information/safety-by-design> [Accessed 6 Sep. 2019].
26. Courtland, R. (2019). Bias detectives: the researchers striving to make algorithms fair. [online] Nature.com. Available at: <https://www.nature.com/articles/d41586-018-05469-3> [Accessed 8 Aug. 2019].
27. Andrew K. Przybylski and Victoria Nash. Cyberpsychology, Behavior, and Social Networking. Jul 2018. ahead of print <http://doi.org/10.1089/cyber.2017.0466>
28. Unicef.org. (2019). The State of The World's Children 2017: Children In A Digital World. [online] Available at: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf [Accessed 8 Aug. 2019].
29. Itu.int. (2019). ICT Facts and Figures 2017. [online] Available at: <https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx> [Accessed 8 Aug. 2019].
30. Unicef.org. (2019). The State of The World's Children 2017: Children In A Digital World. [online] Available at: https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf [Accessed 8 Aug. 2019].
31. Africanews. (2019). Digital in 2018: Africa's internet users increase by 20% | Africanews. [online] Available at: <https://www.africanews.com/2018/02/06/digital-in-2018-africa-s-internet-users-increase-by-20-percent/> [Accessed 8 Aug. 2019].
32. Quartz Africa. (2019). Gender inequality in tech starts with teenagers on their cellphones. [online] Available at: <https://qz.com/africa/1420938/girls-have-less-access-to-mobile-phones-than-boys-study-shows/> [Accessed 25 Aug. 2019].
33. IWF. (2019). Exposing child victims: The catastrophic impact of DNS-over-HTTPS. [online] Available at: <https://www.iwf.org.uk/news/exposing-child-victims-catastrophic-impact-of-dns-over-https> [Accessed 7 Sep. 2019].
34. Fox News. (2019). Hany Farid: Facebook's plan for end-to-end encryption sacrifices a lot of security for just a little bit of privacy. [online] Available at: <https://www.foxnews.com/opinion/hany-farid-facebook-end-to-end-encryption-security-privacy> [Accessed 7 Sep. 2019].

35. Interpol.int. (2019). International Child Sexual Exploitation database. [online] Available at: <https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database> [Accessed 8 Aug. 2019].
36. Thorn. (2019). The Intersection of Technology and Child Sexual Abuse | Thorn. [online] Available at: <https://www.thorn.org/child-sexual-exploitation-and-technology/> [Accessed 8 Aug. 2019].
37. Puddephatt, A. and Hargreaves, S. (2019). 2018 Annual Report. [online] iwf.org.uk/. Available at: <https://www.iwf.org.uk/report/2018-annual-report> [Accessed 8 Aug. 2019].
38. protectchildren.ca. (2019). Resources & Research: International Survivors' Survey. [online] Available at: <https://protectchildren.ca/en/resources-research/survivors-survey-results/> [Accessed 25 Aug. 2019].
39. Ecpat.org. (2019). Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material. [online] 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> [Accessed 6 Sep. 2019].
40. NetClean.com. (2019). The NetClean Report 2018. [online] Available at: <https://www.netclean.com/netclean-report-2018/> [Accessed 12 Aug. 2019].
41. Rachel Young & Melissa Tully (2019) 'Nobody wants the parents involved': Social norms in parent and adolescent responses to cyberbullying, *Journal of Youth Studies*, 22:6, 856-872, DOI: 10.1080/13676261.2018.1546838
42. Childnet.com. (2019). Young people's experiences of online sexual harassment: A cross-country report from Project Deshame. [online] Available at: https://www.childnet.com/ufiles/Project_deSHAME_Dec_2017_Report.pdf [Accessed 8 Aug. 2019].
43. Icmec.org. (2019). Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review. [online] Available at: https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf [Accessed 8 Aug. 2019].
44. Teliacompany.com. (2019). CHILDREN AND ONLINE PRIVACY: FINDINGS FROM THE CHILDREN'S ADVISORY PANEL 2017/18. [online] Available at: <https://www.teliacompany.com/globalassets/teliacompany/documents/sustainability/children-and-online-privacy.pdf> [Accessed 12 Aug. 2019].
45. Brumfield, B. (2019). 3 girls skipped school to sneak off and join ISIS - CNN. [online] CNN. Available at: <https://edition.cnn.com/2014/10/22/us/colorado-teens-syria-odyssey/index.html> [Accessed 8 Aug. 2019].
46. Martelozzo, E. (2019). A quantitative and qualitative examination of the impact of online pornography on the values, attitudes, belief sand behaviours of children and young people. [online] Mdx.ac.uk. Available at: https://www.mdx.ac.uk/__data/assets/pdf_file/0021/223266/MDX-NSPCC-OCC-pornography-report.pdf [Accessed 9 Aug. 2019].
47. ITV News. (2019). Children report feeling unprotected from inappropriate content on social media sites. [online] Available at: <https://www.itv.com/news/utv/2017-04-27/children-warn-social-media-sites-are-failing-to-shield-them-from-inappropriate-and-dangerous-content/> [Accessed 9 Aug. 2019].
48. Shieber, J. (2019). 2018 really was more of a dumpster fire for online hate and harassment, ADL study finds – TechCrunch. [online] TechCrunch. Available at: <https://techcrunch.com/2019/02/13/2018-really-was-more-of-a-dumpster-fire-for-online-hate-and-harassment-adl-study-finds/> [Accessed 9 Aug. 2019].
49. Kardefelt-Winther, D. CHILD RIGHTS AND ONLINE GAMING: OPPORTUNITIES & CHALLENGES FOR CHILDREN AND THE INDUSTRY – ECPAT International. [Accessed 9 Sep. 2019].
50. Fitzpatrick, C. (2019). Watching violence on screens makes children more emotionally distressed. [online] The Conversation. Available at: <https://theconversation.com/watching-violence-on-screens-makes-children-more-emotionally-distressed-106757> [Accessed 9 Aug. 2019].
51. Livingstone, S., Kirwil, L., Ponte, C. and Staksrud, E. (2019). In their own words: What bothers children online? [online] Lse.ac.uk. Available at: <https://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/Intheirownwords020213.pdf> [Accessed 9 Aug. 2019].

52. Calado, F., Alexandre, J. & Griffiths, M.D. *J Gambl Stud* (2017) 33: 397. <https://doi.org/10.1007/s10899-016-9627-5>
53. Valentine, G. (2019). Children and Young People's Gambling: Research Review: Report by Professor Gill Valentine for the Responsible Gambling Trust. [online] About.gambleaware.org. Available at: <https://about.gambleaware.org/media/1274/1-june-update-children-young-people-literature-review.pdf> [Accessed 9 Aug. 2019].
54. Karlsson, Anna & Hakansson, Anders. (2018). Gambling disorder, increased mortality, suicidality, and associated comorbidity: A longitudinal nationwide register study. *Journal of Behavioral Addictions*. 7. 1-9. 10.1556/2006.7.2018.112.
55. Howard, J. (2019). What's the age when kids start social media? [online] CNN. Available at: <https://edition.cnn.com/2018/06/22/health/social-media-for-kids-parent-curve/index.html> [Accessed 9 Aug. 2019].
56. BBC News. (2019). Under-age social media use 'on the rise'. [online] Available at: <https://www.bbc.co.uk/news/technology-42153694> [Accessed 9 Aug. 2019].
57. Publications.parliament.uk. (2019). Impact of social media and screen-use on young people's health. [online] Available at: <https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/822/822.pdf> [Accessed 9 Aug. 2019].
58. Sally Power, Chris Taylor & Kim Horton (2017) Sleepless in school? The social dimensions of young people's bedtime rest and routines, *Journal of Youth Studies*, 20:8, 945-958, DOI: 10.1080/13676261.2016.1273522
59. Cramer, S. and Inkster, B. (2019). #Status Of Mind: Social media and young people's mental health and wellbeing. [online] *Rsph.org.uk*. Available at: <https://www.rsph.org.uk/uploads/assets/uploaded/d125b27c-0b62-41c5-a2c0155a8887cd01.pdf> [Accessed 9 Aug. 2019].
60. Marisa Meyer, Victoria Adkins, Nalingna Yuan, Heidi M. Weeks, Yung-Ju Chang, Jenny Radesky. Advertising in Young Children's Apps. *Journal of Developmental & Behavioral Pediatrics*, 2018; 1 DOI: 10.1097/DBP.0000000000000622
61. Binns, Reuben & Lyngs, Ulrik & Van Kleek, Max & Zhao, Jun & Libert, Timothy & Shadbolt, Nigel. (2018). Third Party Tracking in the Mobile Ecosystem. 10.31235/osf.io/u7q mz.
62. Todorovic, N. and Chaudhuri, A. (2019). Using AI to help organizations detect and report child sexual abuse material online. [online] Google. Available at: <https://www.blog.google/around-the-globe/google-europe/using-ai-help-organizations-detect-and-report-child-sexual-abuse-material-online/> [Accessed 10 Aug. 2019].
63. Richter, I. (2019). Automatische Bilderkennung hilft im Einsatz gegen Kinderpornografie | News Center Microsoft. [online] News Center Microsoft Deutschland. Available at: <https://news.microsoft.com/de-de/ki-im-einsatz-gegen-kinderpornografie/> [Accessed 10 Aug. 2019].
64. Vleugels, A. (2019). AI-algorithms identify pedophiles for the police – here's how it works. [online] The Next Police | The Next Web. Available at: <https://thenextweb.com/the-next-police/2018/11/08/ai-algorithms-identify-sexual-child-abuse-for-the-police/> [Accessed 10 Aug. 2019].
65. Griffeye. (2019). Griffeye releases new AI technology trained to aid child abuse investigations. [online] Available at: <https://www.griffeye.com/griffeye-releases-new-ai-technology-press/> [Accessed 10 Aug. 2019].
66. Burgess, M. (2019). AI is helping UK police tackle child abuse way quicker than before. [online] *Wired.co.uk*. Available at: <https://www.wired.co.uk/article/uk-police-child-abuse-images-ai> [Accessed 10 Aug. 2019].
67. Griffeye. (2019). New AI technology trained to aid child abuse investigations. [online] Available at: <https://www.griffeye.com/new-ai-technology-trained-to-aid-child-abuse-investigations/> [Accessed 6 Sep. 2019].

68. Ward, M. and Balian, S. (2019). Combating online radicalisation with expanded AI capabilities. [online] Faculty. Available at: <https://faculty.ai/blog/combating-online-radicalisation-with-expanded-ai-capabilities/> [Accessed 10 Aug. 2019].
69. Boyce, J. (2019). Facebook touts use of artificial intelligence to fight child exploitation. [online] NBC News. Available at: <https://www.nbcnews.com/tech/tech-news/facebook-touts-use-artificial-intelligence-fight-child-exploitation-n923906> [Accessed 10 Aug. 2019].
70. Publications.parliament.uk. (2019). Impact of social media and screen-use on young people's health: Government Response to the Committee's Fourteenth Report - Science and Technology Committee - House of Commons. [online] Available at: <https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/2120/212002.htm> [Accessed 25 Aug. 2019].
71. <https://www.marinusanalytics.com>
72. ComputerWeekly.com. (2019). Thorn CEO on using machine learning and tech partnerships to tackle online child sex abuse. [online] Available at: <https://www.computerweekly.com/news/450415609/Thorn-CEO-on-using-machine-learning-and-tech-partnerships-to-tackle-online-child-sex-abuse> [Accessed 6 Sep. 2019].
73. Minton, L. (2019). What is human trafficking, and how can technology combat it? [online] ASU Now: Access, Excellence, Impact. Available at: <https://asunow.asu.edu/20190313-what-human-trafficking-and-how-can-technology-combat-it> [Accessed 10 Aug. 2019].
74. Phys.org. (2019). Instagram rolls out new features to counter bullying with AI. [online] Available at: <https://phys.org/news/2019-07-instagram-features-counter-bullying-ai.html> [Accessed 10 Aug. 2019].
75. <http://creep-project.eu>
76. Simonite, T., Simonite, T., Matsakis, L., Martineau, P., Tiku, N., Matsakis, L., Schwartz, O. and Martineau, P. (2019). How Facial Recognition Is Fighting Child Sex Trafficking. [online] WIRED. Available at: <https://www.wired.com/story/how-facial-recognition-fighting-child-sex-trafficking/> [Accessed 25 Aug. 2019].
77. Eandt.theiet.org. (2019). Child abuse targeted with upgraded police tech, limiting officer exposure to images. [online] Available at: <https://eandt.theiet.org/content/articles/2019/07/child-abuse-targeted-with-upgraded-police-tech-limiting-officer-exposure-to-indecent-images/> [Accessed 25 Aug. 2019].
78. McIntyre, N. and Pegg, D. (2019). Councils use 377,000 people's data in efforts to predict child abuse. [online] the Guardian. Available at: <https://www.theguardian.com/society/2018/sep/16/councils-use-377000-peoples-data-in-efforts-to-predict-child-abuse> [Accessed 25 Aug. 2019].
79. Europol. (2019). Global action tackles distribution of child sexual exploitation images via WhatsApp: 39 arrested so far. [online] Available at: <https://www.europol.europa.eu/newsroom/news/global-action-tackles-distribution-of-child-sexual-exploitation-images-whatsapp-39-arrested-so-far> [Accessed 25 Aug. 2019].
80. (www.dw.com), D. (2019). Interpol busts international pedophilia ring | DW | 23.05.2019. [online] DW.COM. Available at: <https://www.dw.com/en/interpol-busts-international-pedophilia-ring/a-48841717> [Accessed 25 Aug. 2019].
81. Statistics provided by INHOPE
82. Niels Nagelhus Schia (2018) The cyber frontier and digital pitfalls in the Global South, Third World Quarterly, 39:5, 821-837, DOI: 10.1080/01436597.2017.1408403}
83. Out of the Shadows. (2019). Out the Shadows - Shining light on the response to child sexual abuse and exploitation. [online] Available at: <https://outoftheshadows.eiu.com> [Accessed 25 Aug. 2019].
84. Childrenandbusiness.org. (2019). Children's Rights and Business Principles. [online] Available at: <http://childrenandbusiness.org/> [Accessed 25 Aug. 2019].

85. Unctad.org. (2019). UNCTAD | Cybercrime Legislation Worldwide. [online] Available at: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx [Accessed 11 Aug. 2019].
86. Unicef.org. (2019). COP Guidelines for Industry. [online] Available at: <https://www.unicef.org/csr/COPguidelines.htm> [Accessed 7 Sep. 2019].
87. Out of the Shadows. (2019). Out the Shadows - Shining light on the response to child sexual abuse and exploitation. [online] Available at: <https://outoftheshadows.eiu.com> [Accessed 25 Aug. 2019].
88. Publicsafety.gc.ca. (2019). Child Pornography Offenders: A Review. [online] Available at: <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2018-s001/index-en.aspx> [Accessed 25 Aug. 2019].
89. Thorn.org. (2019). Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims. [online] Available at: https://www.thorn.org/wp-content/uploads/2018/03/Production-and-Active-Trading-of-CSAM_FullReport_FINAL.pdf [Accessed 13 Aug. 2019].
90. NetClean.com. (2019). The NetClean Report 2017 - There is no such thing as a typical offender (The consumer of child sexual abuse material). [online] Available at: <https://www.netclean.com/netclean-report-2017/insight-3/> [Accessed 25 Aug. 2019].
91. Stop It Now (2006) Let's talk: speaking up to prevent child sexual abuse. [online] Available at: https://www.stopitnow.org/sites/default/files/documents/files/lets_talk.pdf
92. Stone, J. and Stone, J. (2019). The dark web isn't as big as you think.. [online] CyberScoop. Available at: <https://www.cyberscoop.com/dark-web-marketplaces-research-recorded-future/> [Accessed 25 Aug. 2019].
93. Ecpat.org. (2019). Emerging Global Threats Related To The Online Sexual Exploitation Of Children. [online] Available at: https://www.ecpat.org/wp-content/uploads/2018/08/Briefing-Paper-Emerging-Issues-and-Global-Threats-Children-online-_06.06.17.pdf [Accessed 10 Aug. 2019].
94. Stop It Now. (2019). Understanding What Makes Kids Vulnerable to Being Sexually Abused. [online] Available at: <https://www.stopitnow.org/ohc-content/understanding-what-makes-kids-vulnerable-to-being-sexually-abused> [Accessed 11 Aug. 2019].
95. Nice.org.uk. (2019). NICE Guideline NG76: Child abuse and neglect: recognising, assessing and responding to abuse and neglect of children and young people. [online] Available at: <https://www.nice.org.uk/guidance/ng76/evidence/full-guideline-pdf-4607478261> [Accessed 25 Aug. 2019].
96. Who.int. (2019). Child abuse and neglect by parents and other caregivers. [online] Available at: https://www.who.int/violence_injury_prevention/violence/global_campaign/en/chap3.pdf [Accessed 25 Aug. 2019].
97. Unicef.org. (2019). 'Shame and pain': Vietnam starts to grapple with child abuse epidemic. [online] Available at: <https://www.unicef.org/vietnam/stories/shame-and-pain-vietnam-starts-grapple-child-abuse-epidemic> [Accessed 11 Aug. 2019].
98. BBC News. (2019). Instagram 'biggest for child grooming online'. [online] Available at: <https://www.bbc.co.uk/news/uk-47410520> [Accessed 12 Aug. 2019].
99. The Conversation. (2019). YouTube's paedophile problem is only a small part of the internet's issue with child sexual abuse. [online] Available at: <https://theconversation.com/youtubes-paedophile-problem-is-only-a-small-part-of-the-internets-issue-with-child-sexual-abuse-94126> [Accessed 12 Aug. 2019].
100. Ditchthelabel.org. (2019). Anti-Bullying Survey 2017. [online] Available at: <https://www.ditchthelabel.org/wp-content/uploads/2017/07/The-Annual-Bullying-Survey-2017-1.pdf> [Accessed 12 Aug. 2019].
101. Economicgraph.linkedin.com. (2019). LinkedIn Workforce Report | United States | August 2018. [online] Available at: <https://economicgraph.linkedin.com/resources/linkedin-workforce-report-august-2018> [Accessed 25 Aug. 2019].

102. Digital Single Market - European Commission. (2019). Final results of the European Data Market study measuring the size and trends of the EU data economy - Digital Single Market - European Commission. [online] Available at: <https://ec.europa.eu/digital-single-market/en/news/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy> [Accessed 25 Aug. 2019].

103. Anon, (2019). Data Science and Analytics Skills Shortage: Equipping the APEC Workforce with the Competencies Demanded by Employers. [online] Available at: <https://www.apec.org/Publications/2017/11/Data-Science-and-Analytics-Skills-Shortage> [Accessed 25 Aug. 2019].

104. Thorn. (2019). Sound Practices Guide to Stopping Child Sexual Abuse | Thorn. [online] Available at: <https://www.thorn.org/sound-practices-guide-stopping-child-abuse/> [Accessed 7 Sep. 2019].

105. NetClean.com. (2019). Benchmarking Index on the response to child sexual abuse and exploitation. [online] Available at: <https://www.netclean.com/2019/01/11/benchmarking-index-response-to-child-sexual-abuse-and-exploitation/> [Accessed 7 Sep. 2019].

106. Legislation.gov.uk. (2019). Data Protection Act 2018. [online] Available at: <http://www.legislation.gov.uk/ukpga/2018/12/section/123/enacted> [Accessed 7 Sep. 2019].

107. INHOPE Annual Report 2017: http://88.208.218.79/libraries/annual_reports/inhope_annual_report_2017.sflb.ashx

Resources

15



Resources

Contigo Conectados Online Safety Resources (ES)

<https://contigoconectados.com/resultados/riesgos/>

Economist Intelligence Unit: Out of the Shadows

<https://outoftheshadows.eiu.com/>

End Violence Against Children: Keeping Children Safe Online

<https://www.end-violence.org/keeping-children-safe-online>

Facebook: Photo Video Matching

<https://newsroom.fb.com/news/2019/08/open-source-photo-video-matching/>

Facebook: New technology to fight child exploitation

<https://newsroom.fb.com/news/2018/10/fighting-child-exploitation/>

Griffeye

<https://www.griffeye.com/>

GSMA European Framework for Safer Mobile Use by Younger Teenagers and Children

<https://www.gsma.com/publicpolicy/consumer-affairs/children-mobile-technology/myouth>

IMEC Child Sexual Abuse Material: Model Legislation & Global Review

<https://www.icmec.org/wp-content/uploads/2018/12/CSAM-Model-Law-9th-Ed-FINAL-12-3-18.pdf>

Inhope Global Internet Hotlines

<http://www.inhopefoundation.org/>

ITU Guidelines for Policy Makers on Child Protection

<https://www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf>

Luxembourg Terminology Guidelines for The Protection of Children from Sexual Exploitation and Sexual Abuse

<http://luxembourgguidelines.org/english-version/>

Microsoft Digital Skills

<https://www.microsoft.com/en-us/digital-skills/online-safety>

Microsoft Online Safety Resources

<https://www.microsoft.com/en-us/digital-skills/online-safety-resources>

Microsoft PhotoDNA

<https://www.microsoft.com/en-us/photodna>

NetClean

<https://www.netclean.com/>

OECD: The Future of Education and Skills

[https://www.oecd.org/education/2030/E2030%20Position%20Paper%20\(05.04.2018\).pdf](https://www.oecd.org/education/2030/E2030%20Position%20Paper%20(05.04.2018).pdf)

The #ENDviolence Youth Manifesto

<https://www.unicef.org/end-violence/youth-manifesto>

Thorn

<https://www.thorn.org>

UK Online Harms White Paper

<https://www.gov.uk/government/consultations/online-harms-white-paper>

UN Convention on the Rights of the Child

<https://www.ohchr.org/en/professionalinterest/pages/crc.aspx>

UNICEF & GSMA: NOTICE AND TAKEDOWN — Company policies and practices to remove online child sexual abuse material
https://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/notice_and_takedown_gsma_unicef_april_2016.pdf

WeProtect Model National Response Guidance Document
<https://www.weprotect.org/the-model-national-response>

The ITU Global Cybersecurity Index.
<https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>.

