Child Sexual Abuse Material:

Model Legislation & Global Review

10th Edition, 2023

International Centre™
FOR MISSING & EXPLOITED CHILDREN

A Publication of The Koons Family Institute on International Law & Policy

ICMEC envisions a world where children can grow up safe from exploitation, abuse, or the risk of going missing.

Child Sexual Abuse Material:
Model Legislation & Global Review

Tenth Edition

The opinions, findings, conclusions, and recommendations expressed herein are those of ICMEC and do not necessarily reflect those of the U.S. Department of State or any other donor.

As always, ICMEC extends its continuing gratitude to Jeff and Justine Koons for their unwavering support for our mission.

About Us

The International Centre for Missing & Exploited Children (ICMEC) is a non-governmental organization, headquartered in the United States, with offices representing Asia Pacific, Latin America & the Caribbean, and Australia. ICMEC works to make the world a safer place for children by defending against child sexual exploitation, abuse, and the risk of going missing. ICMEC works with partners around the world to conduct research, develop technologies, and educational resources to aid in the search and recovery of children who are missing, fight child sexual exploitation, and empower professionals, institutions, and communities to safeguard children from all forms of sexual abuse.

The Koons Family Institute on International Law & Policy (The Koons Family Institute) is ICMEC's in-house research arm. The Koons Family Institute defends children against sexual exploitation, abuse, or risk of going missing on multiple fronts by conducting and commissioning original research into the status of child protection laws around the world, creating replicable legal tools, promoting best practices, bringing together great thinkers and opinion leaders, and collaborating with partners to identify and measure threats to children and ways ICMEC can advocate for change.

Our Mission

ICMEC envisions a world where children can grow up safe from exploitation, abuse, or the risk of going missing. We believe every child deserves a safe childhood.

ICMEC's mission is to advance child protection and safeguard vulnerable children around the world. We do this by:

- building and improving systems to prevent and respond to cases of missing children, child sexual exploitation, or abuse;
- advocating for enhanced laws and policies;
- mobilizing industries to secure their technologies and platforms from becoming vehicles for abuse and exploitation;
- providing tools and training for criminal justice professionals to effectively investigate and prosecute cases of exploitation, abuse or children who are missing;
- safeguarding school environments; and
- empowering healthcare professionals to recognize and respond to cases of child abuse and exploitation.

ICMEC is committed to building comprehensive national prevention strategies and responses to cases of missing children, child sexual abuse and exploitation. We foster systemic change through thought leadership and research, capacity building, convening regional technology and financial coalitions, and acting as a partner in implementation efforts to keep children safe. ICMEC strives to influence and inspire the global community – regardless of country, industry, sector, or profession – to achieve the common goal of building a safer world for all children.

Table Of Contents

Foreword

The field of child protection is in a constant state of transformation. On the one hand, new trends in criminal activity and ways to misuse technology to harm children emerge, while on the other hand, innovative solutions and tools are developed with the unwavering support and commitment of child protection professionals the world over. Progress can, at times, seem hard-won, challenging, and slow to come about. It is true, however, that every step forward, even small steps, helps ensure that fewer children suffer and makes the continual effort truly worthwhile.

As ICMEC marks its 25th year, our commitment to safeguarding children as a global imperative remains steadfast. We recognize the persistent need for more robust laws, policies, and mechanisms, ongoing training and capacity building for frontline practitioners, accessible technological and investigative tools for law enforcement, and improved communication across sectors to encourage an exchange of ideas and expertise. We commend child protection entities worldwide for their resilience and adaptability even amidst the challenges posed by the recent pandemic and ever-evolving technological landscape.

We are pleased to release the new 10th edition of ICMEC's *Child Sexual Abuse Material: Model Legislation and Global Review*, first published 17 years ago. We are confident that it remains a valuable resource providing insight into the global legislative landscape. Since the first edition was initially published, there has been significant improvement in global awareness of the issue of CSAM and its impact on children and greater recognition by policymakers of the scope and impact of CSAM in their countries and regions. As a result, more than 156 countries have refined or implemented new legislation combating CSAM. In 2006, we found that only 27 countries had legislation sufficient to combat CSAM (95 countries had no relevant legislation at all) – today, 138 countries now have sufficient anti-CSAM legislation (and only 10 countries have no legislation). With this latest edition, we continue our efforts to improve the legislative landscape and strengthen child protection efforts by introducing new and updated sections in the model law, incorporating additional international as well as regional legal instruments, along with featuring new initiatives related to implementation.

This report is intended to sustain ongoing discussions and ignite proactive measures for safeguarding the well-being of children worldwide. The success of our endeavors hinges on the remarkable collaboration of partners across the globe. Within this collective, we find support from governments, private enterprises, law enforcement, and a multitude of NGO allies, striving to create a safer environment for children. We firmly believe that by channeling our efforts and leveraging every resource at our disposal, we can triumph over the scourge of online child exploitation. We extend our heartfelt gratitude for your involvement.

Bob Cunningham
President and Chief Executive Officer
International Centre for Missing & Exploited Children

Acknowledgements

We wish to thank the following organizations and individuals for their outstanding assistance and guidance in researching national legislation relevant to child sexual abuse material for the 10th Edition of our report:

- Chiefs of Mission and staff of Embassies and Consulates in the United States;
- Chiefs of Mission and staff of Permanent Missions to the United Nations in New York;
- The legal research interns of The Koons Family Institute on International Law & Policy who have worked tirelessly to produce this report: Lucy Campbell, Ryan Lau, Kimberly Mariano, Chelsey Rogers, Cristina Ruiz, Patrick Shea, Priya Singh Collins, Theresa Vaillancourt, Miranda Walker, and Diana Wallens;
- Our staff who have worked for countless hours to produce this report: Simone Bevans, Jewel dela Cruz, Sandra Marchenko, Jessy Ober, Evans Osinaike, Lindsey Parker, and Bindu Sharma; and
- Our donors, without whom our work would not be possible.

Points of view and opinions presented in this publication are those of ICMEC and do not necessarily represent the official position or policies of the other organizations and individuals who assisted with or funded the research.

The findings contained in this report are current and verified as of 30 September 2023.

Executive Summary

The Issue

The rapid growth of the internet, along with other information and communication tools over the past 20 years, has created unparalleled opportunities for children and adults alike to learn and explore the world around them. Today, these technologies are ubiquitous in many countries – permeating every aspect of our personal, professional, and social lives. These tools have simultaneously created a new dimension in which the sexual exploitation of children can flourish if unchecked. Every day, children worldwide endure the sexual abuse and exploitation perpetrated by individuals who actively target them to satisfy their own lascivious desires or to profit from the exploitation of these young victims.

Sexual offenders – and others who commit crimes against children – know that digital technology provides the ability to produce illegal images of children, offers a platform to trade and share images of their own sexual exploits with like-minded individuals, and presents the opportunity to organize, maintain, and increase the size of their collections of child sexual abuse material (CSAM). The internet not only made this both easy and inexpensive but also made it extremely low-risk, enormously profitable, and unhindered by geographical boundaries.

The view that CSAM is a "victimless" crime is a long-held and common misconception.

The reality is that these horrific images are photographic, video, or digital records of the sexual abuse of a child. The victims in the images are real children. They are young, and the images are graphic and violent. Out of all CSAM reports received by the Internet Watch Foundation (IWF), based in the United Kingdom (U.K.) in 2022, 40% of victims appeared to be children 0-10 years of age, and 59% of the victims appeared to be children 11-15 years of age.[1] The IWF reported a 60% increase in content depicting pre-pubescent children (ages 7-10 years). Moreover, the IWF reported there was a 129% increase in "self-generated" imagery for children ages 7-10 years of age in 2022 compared to 2021.[2] Self-generated CSAM is sexually explicit content created and shared intentionally by minors but is often the result of online grooming or sextortion.[3] The IWF also reported that "extreme" online child sexual abuse (i.e., child suffering, rape, bestiality, sadism) has doubled since 2020, with newborn babies and toddlers among the victims of the most severe kinds of sexual abuse.[4] This type of content accounts for 20% of all content analyzed by the IWF.[5]

Similar findings from Project Arachnid, a specialized tool developed by the Canadian Centre for Child Protection (C3P) that detects CSAM by crawling the open web, found that pre-pubescent CSAM was the most actioned material type analyzed. Of the 5.4 million images

---

1 Internet Watch Foundation (IWF), *Annual Report 2022*, *at* https://annualreport2022.iwf.org.uk/wp-content/uploads/2023/04/IWF-Annual-Report-2022_FINAL.pdf [hereinafter *IWF 2022*] (last visited Jun. 21, 2023) (on file with the International Centre for Missing & Exploited Children).

2 *Id.* at 54.

3 *What is self-generated CSAM?*, International Association of Internet Hotlines (INHOPE), *at* https://inhope.org/EN/articles/what-is-self-generated-csam (last visited Jun. 21, 2023) (on file with the International Centre for Missing & Exploited Children).

4 IWF 2022, *supra* note 1, at 40.

5 *Id.* at 47.

verified by Cybertip.ca between 2018 and 2020, almost 63% depicted very young, pre-pubescent children (under the age of 12 years).[6] It further showed that almost 35% of all images reviewed depicted the harmful abuse of children (i.e., sexual assault, sexualized context, physical abuse, torture, and restraint).[7]

INHOPE, the International Association of Internet Hotlines, reported in 2022 that of the 587,852 reports received by their 50-member hotlines that were classified as potentially illegal CSAM, 11% were child sexual abuse images depicting pubescent children (ages 14-17); 88% were of pre-pubescent children (ages 3-13 years); and 1% were of infants (ages 0-2 years).[8]

A 2022 Impact Report by the United States (U.S.) National Center for Missing & Exploited Children (NCMEC) showed similar results: of the images most frequently reported to NCMEC, 33% were of pubescent children, 54% were of pre-pubescent children, and 9% were of infants and toddlers.[9]

While the exact number of victims is difficult to determine, the effects on known child victims are many and far-reaching. Child victims of sexual abuse and exploitation often struggle with psychological, physical, and emotional consequences that can negatively impact their futures. CSAM is the permanent record of their exploitation. When these images reach cyberspace, they are irretrievable and can continue to circulate forever, causing the child to be re-victimized each time the images are viewed.

In recent years, there has been an increase in the trade of this illicit content between individuals and groups via peer-to-peer networks.[10] Today, the Dark Web[11] provides an expansive platform for offenders to easily and anonymously share CSAM. The U.S. Department of Justice noted a "significant volume of offenders using the Tor network to advertise and distribute" CSAM while communicating with one another undetected by law

---

6 *Project Arachnid: Online Availability of Child Sexual Abuse Material*, Canadian Centre for Child Protection, Jun. 2021, *at* https://protectchildren.ca/pdfs/C3P_ProjectArachnidReport_en.pdf (last visited Jul. 11, 2023) (on file with the International Centre for Missing & Exploited Children).

7 *Id.* at 17.

8 International Association of Internet Hotlines (INHOPE), *INHOPE Annual Report 2022* 13, *at* https://inhope.org/media/pages/articles/annual-reports/14832daa35-1687272590/inhope-annual-report-2022.pdf [hereinafter *INHOPE 2022*] (last visited Jun. 21, 2023) (on file with the International Centre for Missing & Exploited Children).

9 National Center for Missing and Exploited Children (NCMEC), *Our 2022 Impact*, *at* https://www.missingkids.org/content/dam/missingkids/pdfs/2022-ncmec-our-impact.pdf (last visited Jul. 25, 2023) (on file with the International Centre for Missing & Exploited Children).

10 Janis Wolak, et al., *Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network*, CHILD ABUSE & NEGLECT (2013), *at* http://unh.edu/ccrc/pdf/Wolak_Liberatore_Levine_2013.pdf (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

11 The Dark Web, also known as the Dark Net, is comprised of websites whose Internet Protocol (IP) addresses are intentionally hidden. Dark Web content is accessed over encrypted overlay networks that use the public Internet but require a special kind of software to act as an overlay network gateway. *See*, Dark Web, *Definition – What Does Dark Web Mean?*, *at* https://www.techopedia.com/definition/31562/dark-web (last visited Jul. 26, 2023).

enforcement.[12] Furthermore, law enforcement reported Tor's hidden services to be the "largest facilitators of CSE content seen in a single online location."[13]

Tor's near anonymity "attracts users willing to post egregious content, adding to the millions of [child sexual abuse] images and videos already available and distributed online."[14] Though several high-profile Tor services hosting CSAM have been shut down following cross-jurisdictional law enforcement operations, one particularly egregious Tor-based website has evaded law enforcement takedown attempts for a decade. As of 2021, the website had over 508,000 registered users and hosted over 1 million images and videos depicting child sexual abuse.[15] A study by the University of Portsmouth that collected data on the traffic flow to Tor hidden services online found that sites hosting child abuse imagery were the most frequently requested.[16] The study revealed that 83% of visits to Tor hidden service websites sought sites related to child abuse, of which there were about 45,000 sites available at any given time.[17] Similarly, the U.S. Department of Justice reported that as of March 2023, there were over 200 forums and other sites on the Dark Web devoted to child exploitation.[18]

The problem of CSAM trading has proven to be persistent, and strong anti-CSAM legislation is needed in every country in order to combat it. Despite this, laws addressing CSAM around the world are often weak, inconsistent, or poorly implemented. Sometimes there are no laws to combat this issue at all.

Nearly 20 years ago, ICMEC recognized the global need to better understand existing legislation addressing CSAM and to gauge where the issue stands on national political agendas globally. In response, we examined national laws on CSAM and developed model legislation in an effort to increase global awareness along with concern and to enable governments around the world to adopt and enact much-needed legislation to protect the most innocent victims.

---

12 The Onion Router (Tor) is an open-source software program that allows users to protect their privacy and security against Internet surveillance or traffic analysis. Tor was designed to protect the personal privacy of network users and is widely used in location-hidden services to provide anonymity to servers. *See*, The Onion Router (Tor), *Definition – What does The Onion Router (Tor) mean*?, *at* https://www.techopedia.com/definition/4141/the-onion-router-tor (last visited Jul. 26, 2023).

13 Jessica N. Owens, Karlene Clapp, et al., *Analysis of topic popularity within a child sexual exploitation Tor hidden service*, AGGRESSION AND VIOLENT BEHAVIOR JOURNAL VOL. 68, Jan.-Feb. 2023, *at* https://www.sciencedirect.com/science/article/abs/pii/S1359178922000891#preview-section-introduction last visited Sep. 18, 2023) (on file with the International Centre for Missing & Exploited Children).

14 *The National Strategy for Child Exploitation Prevention and Interdiction*, U.S. Department of Justice, Apr. 2016, *at* https://www.justice.gov/psc/file/842411/download (last visited Jul. 11, 2023) (on file with the International Centre for Missing & Exploited Children).

15 Roderic Broadhurst and Matthew Ball, *How the world's biggest dark web platform spreads millions of items of child sex abuse material – and why it's hard to stop*, Sep. 2, 2021, THE CONVERSATION, *at* https://theconversation.com/how-the-worlds-biggest-dark-web-platform-spreads-millions-of-items-of-child-sex-abuse-material-and-why-its-hard-to-stop-167107 (last visited Jul. 11, 2023) (on file with the International Centre for Missing & Exploited Children).

16 Gareth Owen and Nick Savage, *Paper Series: No. 20 – September 2015: The Tor Dark Net*, GLOBAL COMMISSION ON INTERNET GOVERNANCE, *at* https://www.cigionline.org/static/documents/no20_0.pdf (last visited Jul. 11, 2023) (on file with the International Centre for Missing & Exploited Children).

17 Gareth Owen and Nick Savage, *Empirical analysis of Tor Hidden Services*. May 1, 2016, *at* https://researchportal.port.ac.uk/en/publications/empirical-analysis-of-tor-hidden-services (last visited Jul. 11, 2023) (on file with the International Centre for Missing & Exploited Children).

18 United States Department of Justice, *National Strategy for Child Exploitation Prevention and Interdiction - Child Sexual Abuse Material*, 2023, *at* https://www.justice.gov/d9/2023-06/child_sexual_abuse_material_2.pdf (last visited Jun. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

The Report

Research began in November 2004, and the 1st Edition of *Child Pornography: Model Legislation & Global Review* was published in April 2006, reviewing legislation in the 184 countries that were then members of INTERPOL. Since then, the report has been updated regularly, although the process was extended between editions this time due to the global pandemic. Now in its 10th Edition, the report includes 196 countries and is often requested and globally utilized by policymakers, law enforcement agencies, child protection experts, as well as organizations, industry partners, and others involved in the fight to combat CSAM.

To gain a comprehensive understanding of national legislation on the issue of CSAM globally, ICMEC's research examines whether a core set of criteria exists in each country. In particular, we search for evidence that national legislation:

(1) exists with specific regard to CSAM;
(2) provides a definition of CSAM;
(3) criminalizes technology-facilitated CSAM offenses;[19]
(4) criminalizes the knowing possession of CSAM, regardless of the intent to distribute; and
(5) requires Internet Service Providers (ISPs)[20] to report suspected CSAM to law enforcement or to some other mandated agency.

The model legislation consists of 13 fundamental provisions that are essential to a comprehensive legislative strategy to combat child sexual abuse material.[21] It is divided into five parts: (1) Definitions; (2) Offenses; (3) Mandatory Reporting; (4) Industry Responsibility; and (5) Sanctions and Sentencing. This is followed by an overview of data retention,[22] and related regional and international law, along with a discussion of the implementation and enforcement of national legislation. The final section contains a global legislative review with country-specific information.

It is essential to emphasize that the purpose of the legislative review accompanying the model legislation is not criticism; rather, it is to assess the current state and awareness of the problem. Additionally, the absence of legislation specific to CSAM does not mean that other forms of child sexual exploitation and child abuse are not criminalized and should not be misconstrued as a complete lack of legal measures to protect children.

---

19 For purposes of this report, the term "computer-facilitated" has been replaced by "technology-facilitated" in recognition that a wide variety of technologies/ICTs can and are used to facilitate child sexual abuse and exploitation online.

20 For purposes of this report, the term "Internet Service Provider" (ISP) includes electronic communication service providers and remote computing service providers.

21 The 13 fundamental topics are listed on page 6.

22 Data retention and preservation provisions have increasingly become a point of discussion in the sphere of child protection online. These provisions help ensure that digital evidence is available to law enforcement when needed for the investigation and prosecution of illicit online activity. With the 8th Edition of this report, which was released in 2016, we included new research on national legislation specific to data retention. However, in May 2018, the EU General Data Protection Regulations (GDPR) came into force with near-global implications. The vague language of the GDPR concerning data retention periods will lead to disparities and inconsistencies from jurisdiction to jurisdiction as countries work to pass new national laws to align with the Regulation. For that reason, we have removed it from the research criteria in the 9th Edition.

Methodology

The review process has remained much the same each year. Open-source research into national anti-CSAM legislation is conducted in-house with the help of a team of legal research interns. Primary sources of information include government submissions to the United Nations (U.N.) Special Rapporteur on the Sale and Sexual Exploitation of Children (formerly the U.N. Special Rapporteur on the Sale of Children, Child Prostitution, and Child Pornography) and the U.N. Committee on the Rights of the Child; national legislative resources; and direct contact with in-country non-governmental organizations (NGOs), as well as law enforcement agencies and officers, and attorneys.

Once the relevant information has been assembled, legal analysis is conducted, and preliminary results are compiled. Letters are then sent to the Chiefs of Mission of each country's Embassy in Washington, D.C.; if no Embassy listing is available, a letter is sent to the Chief of Mission at the Permanent Mission to the UN in New York. All letters consist of a summary of the model legislation project, country-specific results, and a request for confirmation or correction of our research results. Upon receipt of new or corrected information, the information is reviewed and, if warranted, is inserted into the report. In some cases, the response (or an excerpt) may be included in the footnotes in the global review portion to ensure that the information is available even when ICMEC determined that the criteria had not been met.

Terminology

In the 9th Edition of this report, ICMEC made the conscious decision to align terminology with that which is more accepted by the international child protection community – shifting from "child pornography" to "child sexual abuse material" – more aptly describing the true nature and extent of sexually exploitive images of child victims to which children can never consent.[23,24] It should be noted that the term "child pornography" is often still utilized in national legislation despite the widespread international consensus that the term should be replaced with "child sexual abuse material (CSAM)." When "child pornography" is used in this report, it is to maintain the integrity of the source document (i.e., international, and regional legal instruments and Embassy responses) and the language used therein.

For purposes of this report, CSAM includes but is not limited to "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes,"[25] as well as the use of a child to create such a representation.

---

[23] *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse* 47 [hereinafter *Luxembourg* Guidelines], Jan. 28, 2026, Terminology and Semantics Interagency Working Group on Sexual Exploitation of Children, ECPAT International, *at* https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines-396922-EN-1.pdf (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

[24] Janis Wolak, et al., *Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings from the National Juvenile Online Victimization Study* vii, n.1 (Nat'l Ctr. for Missing & Exploited Children ed., 2005) (on file with the International Centre for Missing & Exploited Children).

[25] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, G.A. Res. 54/263, Annex II, U.N. Doc. A/54/49, Vol. III, art. 2, para. c, *entered into force* Jan. 18, 2002 [hereinafter *Optional Protocol*] (on file with the International Centre for Missing & Exploited Children).

Results

The results of this new report, along with comparative information from the 1st and 9th Editions, are presented in the table below.

Criteria	1st Edition (2006)*	9th Edition (2018)	10th Edition (2023)
Legislation sufficient to combat CSAM offenses (sufficient means it meets at least 4 of the 5 criteria)	**27** countries had sufficient legislation ▪ **5** countries met all 5 criteria ▪ **22** countries met 4 of the 5 criteria	**118** countries had sufficient legislation ▪ **21** countries met all 5 criteria ▪ **97** countries met 4 of the 5 criteria	**138** countries have sufficient legislation ▪ **27** countries meet all 5 criteria ▪ **111** countries meet 4 of the 5 criteria
No legislation at all specifically addressing CSAM	**95** countries	**16** countries	**10** countries
Of the remaining 48 countries that have legislation specifically addressing CSAM:			
Do not define CSAM	**54** countries	**51** countries	**34** countries
Do not provide for technology-facilitated CSAM offenses	**27** countries	**25** countries	**15** countries
Do not criminalize the knowing possession of CSAM, regardless of intent to distribute	**41** countries	**38** countries	**28** countries

*The 1st edition of this report looked at the legislation of the 184 INTERPOL member countries. With the 6th Edition, the report was expanded to look at the legislation of 196 countries. This difference may reduce the comparative value between the 1st Edition and later editions of the report.

Topics Addressed

Fundamental topics addressed in the model legislation portion of this report include:

(1) Defining "child" for the purposes of CSAM as anyone under the age of 18, regardless of the age of sexual consent;
(2) Defining "child sexual abuse material" and ensuring that the definition includes technology-specific terminology;
(3) Creating offenses specific to CSAM in the national penal code, including criminalizing the knowing possession of CSAM, regardless of one's intent to distribute, and including provisions specific to knowingly downloading or knowingly viewing images on the internet;
(4) Ensuring criminal penalties for parents or legal guardians who acquiesce to their child's participation in CSAM;
(5) Penalizing those who make known to others where to find CSAM;
(6) Incorporating grooming provisions;
(7) Punishing attempt crimes;
(8) Establishing mandatory reporting requirements for healthcare and social service professionals, teachers, law enforcement officers, photo developers, information technology (IT) professionals, ISPs, and financial and payment services institutions;
(9) Allowing technology companies to utilize technology tools and mechanisms to identify and remove illicit content from their networks;
(10) Creating data retention and/or preservation policies/provisions;
(11) Encouraging cross-sector collaboration between the private sector, law enforcement, and civil society;
(12) Addressing the criminal liability of children involved in CSAM; and
(13) Enhancing penalties for repeat offenders, organized crime participants, and other aggravating factors to be considered upon sentencing.

A Complex Web: Factors Influencing the Spread of CSAM

The COVID-19 Pandemic and its Impact

The COVID-19 pandemic, which affected most of the world during 2020 and 2021, presented an increased risk for children online. The pandemic led to a surge in online activity as more people turned to digital platforms for communication, entertainment, and work. Children were forced to stay home due to restrictive measures and lockdowns, which increased their risk of being exploited online. Likewise, as borders and public businesses closed, offenders were forced to take their activities to the internet even more than before and had more opportunities to exploit victims remotely. The IWF's Chief Executive, Susie Hargreaves, stated that the pandemic provided an "online backdoor" into homes to exploit children.[26] In April 2020, ECPAT International reported that offenders were openly discussing in online forums how they could exploit the increase in online activity.[27]

As a result of the pandemic, the quantity of online CSAM skyrocketed.[28] NCMEC's CSAM monthly reports doubled from 1 million in 2019 to 2 million in 2020, increasing a further 35% from 2020 to 2021.[29] Cybertip.ca, which is run by the Canadian Centre for Child Protection (C3P), saw a 120% increase in reports of online child victimization compared to prior to the pandemic.[30]

During the two years of the pandemic, Facebook (Meta) reported over 46 million incidents of CSAM on their platforms; Google reported 1.4 million; Snapchat over 656,000; and TikTok over 177,000.[31] In 2020, Telegram increased the number of groups and channels taken down for child abuse by 26% when compared to 2019.[32] Websites that profit from CSAM have also more than doubled in number since 2020.[33] Insafe, a helpline network that works with INHOPE across Europe, reported a sharp increase in calls received during the second

---

26 Dan Milmo, *Covid lockdowns created 'online backdoor' for child abusers, says charity*, THE GUARDIAN, *at* https://www.theguardian.com/society/2023/jan/27/covid-lockdowns-created-online-backdoor-for-child-abusers-says-charity (on file with the International Centre for Missing & Exploited Children).

27 *Why Children are at risk of Sexual Exploitation during COVID-19*, ECPAT International, Apr. 7, 2020, *at* https://ecpat.org/story/why-children-are-at-risk-of-sexual-exploitation-during-covid-19/ (last visited Sep. 20, 2023).

28 Teresa Huizar, *Child sex abuse content is exploding online. We're losing the fight against it.*, USA TODAY, *at* https://www.usatoday.com/story/opinion/2023/03/10/how-social-media-emboldens-abusers/11413209002/ (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

29 *Id.*

30 Christy Somos, *'Pure evil': How the pandemic has given rise to online child exploitation, livestreamed abuse*, CTV NEWS, Jan. 20, 2022, *at* https://www.ctvnews.ca/sci-tech/pure-evil-how-the-pandemic-has-given-rise-to-online-child-exploitation-livestreamed-abuse-1.5745970 (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

31 Teresa Huizar, *supra* note 28.

32 Olivia Solon, *Child sexual abuse images and online exploitation surge during pandemic*, NBC NEWS, *at* https://www.nbcnews.com/tech/tech-news/child-sexual-abuse-images-online-exploitation-surge-during-pandemic-n1190506 (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

33 Dan Milmo, *One in five child abuse images found online last year were category A - Report*, THE GUARDIAN, *at* https://www.theguardian.com/society/2023/apr/25/one-in-five-child-abuse-images-found-online-last-year-were-category-a-report (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

quarter of 2020.[34] Over 19,000 calls were for online-related issues, representing a 70% increase for the same reporting period in 2019.[35]

In January 2023, the IWF reported that the effects of the pandemic were becoming apparent. For example, the onset of pandemic lockdowns resulted in an increase of more than 1,000% in imagery of primary school-aged children performing sexual acts online. The IWF also reported a 1,058% increase in the number of web pages containing sexual abuse material of children ages 7-10.[36]

The pandemic restrictions and lockdowns resulted in significant challenges for societies globally, particularly as lockdowns forced children and adults alike to spend more time at home and online, making children more vulnerable to exploitation by online offenders looking for CSAM content.[37] In addition, lockdowns, school closures, and movement restrictions meant children were at risk of being confined at home with their abuser without the usual safety mechanisms to support them.

Computer-Generated CSAM

There is no question that easily accessible and often freely available technology could be used to create CSAM. The concept of artificial, computer-generated CSAM (CG-CSAM) is not new, but this type of material has become much more dangerous, especially with the introduction of deepfakes. Deepfakes[38] make it possible to fabricate material through digital alteration so that a person in a video appears to be someone else. Deepfakes use face swapping and puppeteering to maliciously spread false information. Alarmingly, deepfakes are becoming easy to create and even easier to distribute in a policy and legislative vacuum.[39]

Generative artificial intelligence (GenAI) technology[40] is taking this abuse to a new level, and it has those working in the child protection field worried, especially by the speed with which

---

[34] Better Internet for Kids, *Latest helpline trends: Quarter 2, 2020*, Sep. 25, 2020, at https://www.betterinternetforkids.eu/practice/helplines/article?id=6473739 (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

[35] *Id.*

[36] *Sexual abuse imagery of primary school children 1,000 per cent worse since lockdown*, Internet Watch Foundation, Jan. 27, 2023, at https://www.iwf.org.uk/news-media/news/sexual-abuse-imagery-of-primary-school-children-1-000-per-cent-worse-since-lockdown/ last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

[37] *Id.*

[38] Deepfake technology is defined as a "form of artificial intelligence that employs machine learning algorithms to generate realistic media content, including synthetic audio, images, and text." *See*, Flashpoint, *What is Deepfake Technology and How Are Threat Actors Using It?*, Jun. 1, 2023, at https://flashpoint.io/blog/what-is-deepfake-technology/ (last visited Sep. 20, 2023).

[39] Ashish Jaiman, *Deepfakes Harms & Threat Modeling*, TOWARDS DATA SCIENCE, Aug. 19, 2020, at https://towardsdatascience.com/deepfakes-harms-and-threat-modeling-c09cbe0b7883 (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

[40] Generative AI is defined as "a type of artificial intelligence technology that broadly describes machine learning systems capable of generating text, images, code or other types of content, often in response to a prompt entered by a user. Generative AI models are increasingly being incorporated into online tools and chatbots that allow users to type questions or instructions into an input field, upon which the AI model will generate a human-like response." *See*, TechRepublic, *Generative AI Defined: How it Works, Benefits and Dangers*, Aug. 7, 2023, at https://www.techrepublic.com/article/what-is-generative-ai/#section-1 (last visited Sep. 20, 2023) (on file with the International Centre for Missing & Exploited Children).

the technology has been made available, with seemingly no consideration given to what guardrails might be needed.[41]

GenAI initially began appearing in 2017 after a Reddit user utilized artificial intelligence to create pornographic content of non-consenting female celebrities' faces.[42] By 2018, law enforcement was already reporting seeing deepfakes in CSAM cases.[43]

GenAI CSAM is increasingly becoming an issue, especially regarding investigations of potential real-life abuse victims. Using this technology, offenders can replace an abused child's face with another child who has not been explicitly abused. Consequently, law enforcement officers search for the child whose face is shown in the photograph – wasting time and resources that should be put toward finding a child who is being abused. The ability to replace a child's face using this technology can also subsequently endanger the child who was not initially being abused through means of sextortion based on the "fictitious" photograph.[44]

Though research found that less than 1% of CSAM found in known predatory communities was photorealistic computer-generated,[45] GenAI could have dire negative effects on the issue of CSAM. David Thiel, Chief Technologist at the Stanford Internet Observatory, said that "within a year, we're going to be reaching very much a problem state in this area."[46]

The state of AI has been compared to the introduction and rapid expansion of social media platforms, which were left to their own devices to write the rule book.[47] While it appears that some AI companies have already put measures in place to prevent the creation of CSAM using their technology, open-source platforms have been much slower to consider such protections, if at all. And it's these platforms that are enabling the production of GenAI CSAM. These open-source platforms have strong support from those who claim that they will be the vehicle for accelerated innovation.[48] But they also facilitate the easy production of CSAM, using images of real children as source material.

Regulators around the world have acknowledged the potential for harm created by this technology and recognize that we need strong and cohesive regulation worldwide. Several regions, including Australia, Canada, Europe, and the U.S., are at various stages of introducing legislation to regulate AI.[49]

---

41 *What does Generative AI mean for CSE?*, International Centre for Missing & Exploited Children Australia, Jun. 27, 2023, *at* https://icmec.org.au/blog/what-does-generative-ai-mean-for-cse/ (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

42 INHOPE, *What is a Deepfake?*, Jul. 14, 2021, *at* https://inhope.org/EN/articles/what-is-a-deepfake (last visited Jul. 26, 2023).

43 *Id.*

44 David Thiel et al., *Generative ML and CSAM: Implications and Mitigations*, Stanford Internet Observatory, Jun. 24, 2023, *at* https://fsi.stanford.edu/publication/generative-ml-and-csam-implications-and-mitigations (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

45 *Id.*

46 Issie Lapowsky, *The Race to Prevent 'the Worst Case Scenario for Machine Learning'*, NEW YORK TIMES, Jun. 24, 2023, *at* https://www.nytimes.com/2023/06/24/business/ai-generated-explicit-images.html (last visited Jul. 26, 2023).

47 What does Generative AI mean for CSE?, *supra* note 41.

48 Pranshu Verma and Will Oremus, *Meta's new AI lets people make chatbots. They're using it for sex.*, THE WASHINGTON POST, Jun. 26, 2023, at https://www.washingtonpost.com/technology/2023/06/26/facebook-chatbot-sex/ (last visited Jul. 26, 2023).

49 What does Generative AI mean for CSE?, *supra* note 41.

The impact of generative AI on CSAM will depend on how it is harnessed and regulated, and therefore, strong legal frameworks are essential. The harms and impact of GenAI CSAM are significant. The image-based abuse of a child whose picture has been used to create CSAM, the revictimization of children by producing additional and progressively violent computer-generated versions of their abuse, and the potential for the material triggering an interest in CSAM that escalates to contact offending, are all potential issues. The images might be "fake," but the dangers and abuse are real.[50]

Livestreamed Child Sexual Abuse

In recent years, the livestreaming of child sexual abuse has become "an established reality."[51] Live child sexual abuse is streamed over the internet via webcam, enabling the offending viewer to watch the abuse occur in real time.[52] This material can be broadcast on a variety of online platforms, most commonly chatrooms, social media sites, or now-ubiquitous video meeting platforms. In some cases, the specific sexual acts are ordered or directed by the offending viewer.[53] When the streaming stops, evidence of the CSAM is gone unless the offender intentionally records it.[54] Consequently, this type of online sexual abuse "leaves little digital imprint, which makes it more challenging for law enforcement to estimate the scale of it and to take measures to combat it."[55] However, software can be used to create a permanent recording (or "capture") of the livestreamed child sexual abuse (CSA). In these instances, the captured child sexual abuse images can then be re-distributed.[56] Livestreamed child sexual abuse may also be referred to as "distant livestreamed child sexual abuse," as most of this content is streamed transnationally.[57]

The COVID-19 pandemic had a concerning effect on livestreamed child sexual abuse, exacerbating existing challenges and creating new ones. Child sexual offenders seeking new CSAM contributed greatly to the rise in livestreams during the pandemic. [58] The RCMP

---

50 *Id.*

51 Virtual Global Taskforce (VGT) and European Cybercrime Centre (EC3), *Virtual Global Taskforce Child Sexual Exploitation Environmental Assessment Scan 2015*, Oct. 2015, at https://www.europol.europa.eu/sites/default/files/publications/vgt_cse_public_version_final.pdf (last visited Nov. 26, 2018) (on file with the International Centre for Missing & Exploited Children).

52 Luxembourg Guidelines, *supra* note 23.

53 U.S. Department of State, Office to Monitor and Combat Trafficking in Persons, *Factsheet – Online Sexual Exploitation of Children: An Alarming Trend*, Jun. 27, 2017, at https://2017-2021.state.gov/online-sexual-exploitation-of-children-an-alarming-trend/ (last visited Sep. 21, 2023) (on file with the International Centre for Missing & Exploited Children).

54 *Id.*

55 Michael Atkin and Nikki Tugwell, *Australian cyber sex trafficking 'most dark and evil crime we are seeking'*, ABC.NET.AU, Sep. 7, 2016, at https://www.abc.net.au/news/2016-09-07/predators-using-internet-to-direct-live-online-sex-abuse/7819150 (last visited Nov. 26, 2018) (on file with the International Centre for Missing & Exploited Children).

56 "Captures of live-streamed child sexual abuse" are defined as Images or videos permanently recorded from a live broadcast stream; in which the child(ren), consciously interacted with a remote other(s); and which met the IWF threshold for action as child sexual abuse material". See, Internet Watch Foundation, *Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse* 8, May 2018, at https://www.iwf.org.uk/media/23jj3nc2/distribution-of-captures-of-live-streamed-child-sexual-abuse-final.pdf (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

57 NetClean, *NetClean Report 2019: A Report About Child Sexual Abuse Crime*, 2019, at https://www.netclean.com/netclean-report-2019/ (last visited on Sep. 10, 2023) (on file with the International Centre for Missing & Exploited Children).

58 United Nations Office on Drugs and Crime (UNODC), *Online Child Sexual Exploitation and Abuse*, at https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

NCECC reported that the pandemic brought about an uptick in livestreaming with overseas victims because offenders who would have traditionally traveled abroad to abuse victims couldn't because of border closures and lockdown restrictions. Instead, offenders turned to online methods to pursue abuse.[59] The Philippines alone reported a 265% increase in livestreamed CSA from March to May 2020.[60]

Frequently, money is the driving force behind livestreamed content, and most livestreaming occurs in exchange for payments. It is believed that economic hardships caused by the COVID-19 pandemic may have led to an increase in individuals seeking financial stability through illegal activities, including livestreamed child sexual abuse.[61] In investigating livestreamed abuse, the financial exchange is often a key piece of evidence that helps successfully prosecute offenders.

The online environment allows offenders to easily produce, consume, and otherwise engage in livestreamed child sexual abuse. Exchanging and viewing livestreamed child sexual on a global scale is relatively easy, as potential offenders require minimal technology and basic familiarity with popular online services. Websites and online services with robust user privacy policies (e.g., Dropbox, Google, Skype, Snapchat) are preferred by offenders as they can maintain a level of anonymity.[62]

Sextortion

The widespread global transition to online platforms due to the COVID-19 pandemic was accompanied by a troubling rise in reports of sexual extortion involving children. Sexual extortion, also called sextortion, is the coercion of child victims into sending sexualized images to offenders online. Sextortion is considered a feature of online solicitation, and when carried out against children, sextortion involves a process whereby children are coerced into producing sexual material and/or told to perform distressing acts under threat of exposure to others of the material that depicts them. At its core, sextortion is the threat to expose sexual images in order to make a person do something. These threats are an attempt to harass, embarrass, and control victims.[63] In some instances, the abuse spirals so out of control that victims have attempted to self-harm or commit suicide in order to escape it.[64]

Data from Statistics Canada in 2022 showed that sextortion cases reported to law enforcement rose by nearly 300% in the last decade, but the crime of sextortion rose significantly during the pandemic. Cybertip.ca, the national tip line for reporting online child sexual abuse, said it received an unprecedented number of reports regarding children falling

---

59 Christy Somos, *supra* note 30.

60 *Livestreaming child sexual exploitation and abuse*, WeProtect Global Alliance, *at* https://www.weprotect.org/issue/livestreaming/ (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

61 *Id.*

62 *Safe from harm: Tackling webcam child sexual abuse in the Philippines*, UNICEF, *at* https://www.unicef.org/stories/safe-from-harm-tackling-webcam-child-sexual-abuse-philippines (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

63 *What is sextortion?*, Thorn, *at* https://www.thorn.org/sextortion/ (last visited Jul. 26, 2023).

64 *Id.*

prey to aggressive sextortion tactics, amounting to around 300 online extortion cases per month.[65]

As online sexual exploitation of children evolves, sextortion becomes more prevalent. The Australian Centre to Counter Child Exploitation (ACCCE) recorded an average of more than 100 sextortion reports every month in 2022, which is a 100-fold increase from the prior year.[66] In the U.S., there were 3,000 confirmed child victims of sextortion in 2022 alone.[67] Yet the number of victims is likely much higher as this number does not include reports where children complied with the demands of the offender. Only less than a quarter of minors report to law enforcement,[68] with 85% of sextortion victims citing shame as the main reason for not getting help.[69]

Since 2016, NCMEC's CyberTipline has received 262,573 reports of Online Enticement, the reporting category that includes sextortion. Between 2019 and 2021, the number of reports more than doubled.[70]

A study of law enforcement reports from agencies across Australia, Canada, and the U.S. found that 38% of all financial extortion victims are under 18 years of age.[71] A survey of sextortion victims found that 47% experienced threats daily.[72]

Though some offenders demand more sexually explicit content, research shows that 79% seek to extort money from child victims.[73] When victims send offenders money, 93% subsequently demand more money.[74]

Sexual offenders weaponize social media platforms where they can easily create fake accounts and conveniently access the potential victim's personal information. They legitimize their blackmail by sending screenshots of the victim's social media contacts, threatening to share the explicit images with family and friends.[75] In some cases, and particularly in the U.S., sextortion can take a different form. Online offenders lurk in chatrooms and record children who post or livestream sexual images and videos of

---

65 Brieanna Charlebois, *Sextortion boom coincides with pandemic's online shift, as experts raise alarm*, VANCOUVER SUN, Aug. 6, 2022, *at* https://vancouversun.com/news/crime/sextortion-boom-coincides-with-pandemics-online-shift-as-experts-raise-alarm (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

66 Australian Federal Police, *AFP and AUSTRAC target offshore sextortion syndicates preying on Australian youth*, Dec. 1, 2022, *at* https://www.afp.gov.au/news-media/media-releases/afp-and-austrac-target-offshore-sextortion-syndicates-preying-australian (last visited Jul. 26, 2023). See also, U.S. Federal Bureau of Investigation (FBI), *FBI and Partners Issue National Public Safety Alert on Financial Sextortion Schemes*, Dec. 19, 2022, *at* https://www.fbi.gov/news/press-releases/press-releases/fbi-and-partners-issue-national-public-safety-alert-on-financial-sextortion-schemes (last visited Jul. 26, 2023).

67 U.S. FBI, FBI and Partners Issue National Public Safety Alert on Financial Sextortion Schemes, *supra* note 66.

68 *Id.*

69 *The Growing Threat of Sextortion*, Thorn, Nov. 14, 2022, *at* https://www.thorn.org/blog/the-growing-threat-of-sextortion/ (last visited Jul. 26, 2023).

70 National Center for Missing & Exploited Children, *Sextortion: Overview*, *at* https://www.missingkids.org/theissues/sextortion (last visited Jul. 26, 2023).

71 *An Analysis of Financial Sextortion Victim Posts*, Canadian Centre for Child Protection, Nov. 2022, *at* https://www.protectchildren.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

72 What is Sextortion?, *supra* note 63.

73 U.S. Department of Homeland Security, *Sextortion: It's more common than you think*, *at* https://www.ice.gov/features/sextortion (last visited Jul. 26, 2023).

74 An Analysis of Financial Sextortion Victim Posts, *supra* note 71.

75 *Id.*

themselves. These offenders may also hack into electronic devices using malware to gain access to files and to control a child's camera and microphone without the victim knowing it.[76]

Research has identified two core threat groups as sextortion offenders: child sexual offenders and international criminal gangs (located mainly in the Philippines and West Africa).[77] Members of the criminal gangs and networks offshore are holding themselves out as teens and connecting with young people online, asking for naked images and videos, and then demanding that victims pay to keep the images from being circulated amongst family and friends. In one case, a Sri Lankan national contacted girls aged between 12 and 17 years in Australia, the U.S., and the U.K. Upon arrest, financial intelligence investigations identified not only the victims but also a network of offenders targeting children worldwide.[78]

Customarily, offenders involved in the online sexual exploitation of children engage in this crime to achieve sexual gratification. However, offshore criminal networks are fueling a surge in online sexual exploitation, with profiting financially as the primary aim.[79]

Sextortion offenders use various online payment platforms, not limited to money and bank transfers but also gift cards and online gaming credits.[80] The amounts differ, averaging from USD 50 to USD 1,500, and often increase as more demands are made before victims run out of funds. There are, however, cases of demands up to USD 5,000. The payments are made by children at irregular intervals, and often, offenders receive multiple payments in a week, depending on the number of children they are targeting.[81]

In Australia, Operation Huntsman saw the Australian Federal Police (AFP) and the Australian Transaction Reports and Analysis Centre (AUSTRAC) working with the financial sector to shut down more than 500 bank accounts, financial services, and digital currency accounts linked to international organized crime syndicates sexually extorting Australian children. These accounts were sending the money received from victims to offshore syndicates involved in sextortion.[82]

---

76 U.S. Federal Bureau of Investigation, *What is Sextortion?*, *at* https://www.fbi.gov/video-repository/newss-what-is-sextortion/view (last visited Jul. 26, 2023)

77 ActiveFence, *The State of Trust & Safety 2023: Proactively Countering Online Harm*, *at* https://go.activefence.com/the-state-of-trust-safety-2023 (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

78 *Man sentenced after 'sextortion' campaign against young girls*, Australian Federal Police, Mar. 2, 2022, *at* https://www.afp.gov.au/news-media/media-releases/man-sentenced-after-%E2%80%98sextortion%E2%80%99-campaign-against-young-girls (last visited Jul. 26, 2023).

79 Id.

80 AUSTRAC, *Combating the sexual exploitation of children for financial gain*, Dec. 2022, *at* https://www.austrac.gov.au/sites/default/files/2022-12/2022%20AUSTRAC%20Child%20Sexual%20Exploitation%20Financial%20Crime%20Guide.pdf (last visited Sep. 20, 2023) (on file with the International Centre for Missing & Exploited Children).

81 *Id.*

82 Man sentenced after 'sextortion' campaign against young girls, *supra* note 78.

Model Legislation

A comprehensive legislative strategy aimed at combating CSAM that allows law enforcement to aggressively investigate and prosecute offenders must extend beyond just the criminalization of certain actions by child sex offenders. While this is of obvious importance, of equal value are, *inter alia*, adequately defining the terminology that is used in national penal codes; legislating corporate social responsibility; enhancing sanctions; forfeiting assets; and strengthening sentencing provisions.

The model legislation component of this publication is divided into six parts:

(1) Definitions;
(2) Offenses;
(3) Mandatory Reporting;
(4) Industry Responsibility;
(5) Sanctions and Sentencing; and
(6) Law Enforcement Investigations & Data Retention.

Definitions

Define "child," for the purposes of CSAM, as "anyone under the age of 18," regardless of the age of sexual consent.

The legal age at which a person can consent to sexual activity varies from country to country. At the time of publication, only 51 countries had a legal age of sexual consent of 18 or over.[83] This creates a challenging obstacle to obtaining consistent and harmonized protection of children from sexual exploitation on an international level. While a person under the age of 18 may be able to freely consent to sexual relations, legally, a person is not able to consent to any form of sexual exploitation, including CSAM.

Moreover, in circumstances that require "dual criminality" – when a crime committed abroad must also be a crime in an offender's home country in order for the offender to be prosecuted in their home country – agreement on a common age for defining a "child" is crucial. Any discrepancy could prevent a child sex offender from being prosecuted.

For these reasons, "child," for purposes of anti-CSAM legislation, should be defined as "anyone under the age of 18 years."

Define "child sexual abuse material" and include technology-specific terminology.

So that there can be no question in the mind of the offender or on the part of law enforcement, a judge, or a jury, CSAM should be adequately defined in national legislation. It is important to use the term "child sexual abuse material" rather than "child pornography" to

[83] Internal research on the legal age of sexual consent conducted by ICMEC, Sep. 20, 2023.

describe the criminal nature of such material more accurately and to avoid any confusion regarding consent.[84]

The definition should include, at a minimum, the visual representation or depiction of a child engaged in a (real or simulated) sexual display, act, or performance. Additionally, there may be words or phrases within the definition of "child sexual abuse material" that also require explanation. For example, terms such as "simulated sexual conduct," "sexually explicit conduct," "lewd and lascivious exhibition of the genitals," and "sexual display, act, or performance" are all deserving of definitions.

Moreover, it is imperative that with the advent of new technologies, CSAM is recognized to be prevalent in a multitude of forms. For example, CSAM can be found in, including, but not limited to, film, DVD, CD-ROM, diskette, CD-R, data files, data storage devices, online cloud storage, software, information and communication technologies (ICTs), USB drives, along with other electronic or digital media. Similarly, CSAM can be distributed through numerous mechanisms, such as via computer networks, smartphones, and the internet. Moreover, it is also important to consider the ways in which CSAM can be possessed, including by knowingly viewing an image on the internet or knowingly downloading an image to one's computer, tablet, or smartphone.

Offenses

Incorporate CSAM offenses into the penal code.

Mere labor legislation that bans the worst forms of child labor, including CSAM, is insufficient if it does not include specific criminal offenses, criminal sanctions, and criminal punishments. The same is true for national legislation that defines "sexual exploitation" to include CSAM (usually in the child protection code) but, once again, does not enumerate criminal offenses or specify criminal penalties. While such provisions are positive first steps in acknowledging CSAM as an evil that affects child welfare, CSAM is a crime and must be fully recognized as such. CSAM represents nothing less than the memorialization of the sexual degradation, molestation, abuse, and assault of a child.

Further, countries in which there is a general ban on pornography, regardless of whether the individuals being depicted are adults or children, are not considered to have "legislation specific to CSAM" for purposes of this report unless there is also a sentencing enhancement in the national legislation that increases penalties for those who commit offenses against children. A sentencing enhancement for child victims makes the necessary distinction between adult pornography and CSAM.

Criminalize the knowing possession of CSAM, regardless of the intent to distribute.

Every CSAM image that is acquired encourages the further growth of this illicit industry and contributes to the development of alarming trends such as livestreamed child sexual abuse wherein the "offender is in a different location to the victim and requests specific acts to be performed by the child or perpetrated against the child by another individual facilitating the

[84] Luxembourg Guidelines, *supra* note 23.

abuse."[85] Law enforcement agencies around the world have confirmed that offenders are recording live streams to then "'sextort' victims and to create and disseminate CSAM online."[86]

A 2019 study in the U.S. found that 80% of CSAM production offenders were also charged with offenses involving sexual contact with minors.[87] A 2022 study on risk factors for CSAM users found that 42% of respondents reported they had sought direct contact with children through online platforms after viewing CSAM.[88] This same study also found that 10% of respondents said they had sought direct contact with children online weekly or nearly every time after viewing CSAM or illegal violent material.[89] These findings continue to suggest a correlation between the simple possession of CSAM knowingly and committing sexual abuse upon a child.[90] Therefore, criminalizing the knowing possession of CSAM may not only curb industry growth but also prevent further incidents of sexual abuse.

Criminalize knowingly downloading or knowingly viewing CSAM through ICTs and using ICTs to distribute CSAM.

Offenders use ICTs to view, download, distribute, acquire, trade, reproduce, promote, and advertise CSAM daily. Therefore, as stated earlier, specific mention must be made, in some way, of ICTs being used to make, view, possess, distribute, or in some other way commit a CSAM-related offense.

Note that there is a difference between inadvertently viewing an image and actively downloading one. Both knowingly viewing and knowingly downloading should be criminalized as separate and distinct offenses.

Penalize those who make known to others where to find CSAM.

Offering information on where to find CSAM by providing a website address, for example, should be criminalized. An individual who assists in the commission of a crime (i.e., knowingly possessing or knowingly downloading CSAM) through offering advice or taking actions that facilitate knowingly possessing or knowingly accessing and downloading illegal content should be penalized.

---

85 Coen Teunissen and Sarah Napier, *The overlap between child sexual abuse live streaming, contact abuse and other forms of child exploitation*, Trends and issues in Crime and Criminal Justice, Vol. 671, Australian Institute of Criminology, May 2023, at https://www.aic.gov.au/sites/default/files/2023-05/ti671_overlap_between_csa_live_streaming_contact_abuse_and_other_child_exploitation.pdf (last visited Sep. 16, 2023) (on file with the International Centre for Missing & Exploited Children).

86 *Id.*

87 United States Sentencing Commission, *Federal Sentencing of Child Pornography: Production Offenses*, at https://www.ussc.gov/research/research-reports/federal-sentencing-child-pornography-production-offenses (last visited Jul. 25, 2023) (on file with the International Centre for Missing and Exploited Children).

88 Insoll, et al., *Risk Factors for Child Sexual Abuse Material Users Contacting Children Online: Results of an Anonymous Multilingual Survey on the Dark Web*, Journal of Online Trust and Safety, Feb. 2022, at https://trepo.tuni.fi//bitstream/handle/10024/144848/insoll_csam.pdf?sequence=1 (last visited Jun. 27, 2023) (on file with the International Centre for Missing & Exploited Children).

89 *Id.*

90 *Id.*

Criminalize the actions of parents or legal guardians who acquiesce to their child's participation in CSAM.

Similar to aiding and abetting in the commission of a crime, a parent or legal guardian who acquiesces to their child's participation in CSAM is supporting and taking actions towards the commission of multiple crimes: rape, sexual exploitation, sexual assault, sexual abuse, and the manufacture of CSAM, all of which are being committed against their own child.

There can be no transfer of consent from the parent or guardian to the child to participate in CSAM. Just as a parent or guardian cannot lawfully consent to a child driving a motor vehicle underage, neither can a parent or guardian consent on behalf of a child to the child's participation in CSAM.

Investigations into cases of livestreamed CSA have found that "in some cases, the trafficker or facilitator is a mother or other female relative," and even when a parent is not involved in the actual abuse, the "parents are often aware of the abuse because they are benefitting financially from the crimes."[91]

Turning a child over to the CSAM industry, whether or not for monetary profit, is the ultimate betrayal and violation of trust, parental duty, and responsibility. The child's health and overall welfare are endangered. Resultantly, such exposure to abuse and ill-treatment should not go unpunished.

Grooming offenses must be criminalized.

Online grooming of children refers to the use of the internet or other digital technologies to facilitate either online or offline sexual contact with someone under the age of 18.[92] The process of grooming represents the initial actions taken by an individual to sexually abuse a child by developing a relationship of trust. Sex offenders use a variety of ICTs (such as the internet, email, social networking sites, hosting sites and services, instant messaging, gaming systems, forums, and chatrooms) to gain a child's trust and possibly to arrange a face-to-face meeting. The trust relationship diminishes the child's natural resistance to strangers and helps the offender normalize sexual behavior, often with little or no parental supervision. This behavior has immense potential to cause harm thus, must be targeted and criminalized in order to reduce the sexual exploitation of children.

As the relationship develops, child sex offenders may show adult pornography and/or CSAM to the child to lower their inhibitions, desensitize them to sexual activity, normalize this behavior, and teach the child sexual behaviors.[93] Showing pornographic images and videos or CSAM to the child also can increase the child's sexual curiosity, which can lead to sexual

---

91 *Livestreaming and Virtual Child Sex Trafficking*, U.S. Department of Justice, Jun. 2023, *at* https://www.justice.gov/d9/2023-06/livestreaming_and_virtual_child_sex_trafficking_2.pdf (last visited Sep. 18, 2023) (on file with the International Centre for Missing & Exploited Children) (emphasis added).

92 Dr. Mike McGuire and Samantha Dowling, *Cyber crime: A review of the evidence – Research Report 75 Chapter 3: Cyber-enabled crimes – sexual offending against children* 4, Home Office, Oct. 2013, *at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246754/horr75-chap3.pdf (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children) (emphasis added).

93 C. Emmanuel Ahia, et al., *Protecting Children from Online Sexual Predators: Technological, Psychoeducational, and Legal Considerations*, 35 PROFESSIONAL PSYCHOLOGY: RESEARCH AND PRACTICE 67 (on file with the International Centre for Missing & Exploited Children).

discussions that may advance a sexual relationship. Ultimately, this can increase the likelihood of a sexual encounter, physical or virtual, with that child.[94]

Research has shown that children in many countries communicate with strangers online and unwittingly share personal information, which can be one of the first steps in a grooming relationship.[95] Moreover, grooming relationships can have a personal sexual intent or commercial exploitation intent and thus often precede the creation or distribution of CSAM.[96]

Recent reports show that an increasing number of grooming cases take place entirely online; specifically, the offender obtains sexual gratification through non-contact offenses without the intention of meeting the child in person.[97] For example, an offender may send or receive sexually explicit photographs, perform or observe sexual acts over a webcam, or participate in sexually explicit conversations through chat, text, or email. One university study found that offenders, when chatting online with children, introduced sexual topics after just three minutes, and a bond can be formed with a child after only eight minutes.[98] This was supported by INHOPE, which recorded a 97% increase in reports of online communications with children for the purposes of a sexual offense.[99] Online relationships can be quite personal and meaningful for children; alarmingly, Thorn reported that results of a 2021 study showed that of the 9-17 year-olds interviewed, 32% said their closest friendships were formed online.[100] Children also viewed flirting and dating online as common, even when it involved an adult or someone much older than them. While it was more common among teens, 33% of children aged 9-12 years believed it was common to flirt with other minors online, and 25% believed it was common to date a young adult online.[101]

Online grooming often overlaps with incidents of online child sextortion.[102] In such cases, an offender may initiate a relationship with a child, manipulating the child into online or offline sexual contact, often including creating and sending sexual images or videos to the

---

94 Deon Minnie, *The Grooming Process and the Defence of Consent in Child Sexual Abuse Cases* 49, Master of Laws in the Faculty of Law at the Nelson Mandela Metropolitan University (on file with the International Centre for Missing & Exploited Children).

95 Trent Toone, *Kids revealing too much online, study says*, Deseret News, Feb. 6, 2011, *at* https://www.deseret.com/2011/2/6/20369081/kids-revealing-too-much-online-study-says (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

96 United States Department of Justice, Child Exploitation and Obscenity Section (CEOS), *Child Pornography*, *at* https://www.justice.gov/criminal-ceos/child-pornography (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

97 Dr. Mike McGuire and Samantha Dowling, *supra* note 92.

98 Biometrica, *Web of Darkness: Groomed, Manipulated, Coerced, and Abused In Minutes*, Nov. 7, 2017, *at* https://www.biometrica.com/icmec-online-grooming/ (last visited Jun. 28, 2023) (on file with the International Centre for Missing & Exploited Children).

99 INHOPE, *Online grooming: existing legislation and the importance of a global definition recap*, May 25, 2022, *at* https://inhope.org/EN/articles/online-grooming-existing-legislation-and-the-importance-of-a-global-definnition-recap (last visited Jun. 27, 2023) (on file with the International Centre for Missing & Exploited Children).

100 Thorn, *Online Grooming: Examining risk encounters amid everyday digital socialization* 10, Apr. 2022, *at* https://info.thorn.org/hubfs/Research/2022_Online_Grooming_Report.pdf (last visited Jun. 27, 2023) (on file with the International Centre for Missing & Exploited Children).

101 *Id.* at 4.

102 Europol, European Cybercrime Centre, *Online sexual coercion and extortion as a form of crime affecting children: Law Enforcement Perspective* 10, May 2017, at https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

offender. Once the offender has obtained the images and/or videos, they may threaten, intimidate, or coerce the child into sending more images, money, or giving sexual favors under the threat of the child's images being shared with family, friends, and others.[103] Child victims of sextortion are typically between the ages of 14-17 years, but victims as young as eight years old have been documented.[104] In January 2023, the U.S. Federal Bureau of Investigation (FBI) issued a press release warning of the explosion in incidents of children and teens being coerced into sending explicit images online and extorted for additional explicit material or money, and that in the past year, more than a dozen child victims of sextortion had committed suicide.[105]

The enactment of online grooming or online enticement legislation may help to prevent latent or previously undetected sex offenders from targeting children and preclude later victimization as well as exploitation of children. Therefore, online grooming legislation must criminalize all types of grooming, regardless of whether the offender intends for the relationship to progress to an offline setting.[106]

Punish attempt crimes.

The rationale behind criminalizing an attempt to harm a child is to prevent the child from further harm and punish an individual who has demonstrated an inclination to commit such a crime without having to wait for the completion of the crime (i.e., the victimization of a child). Punishing attempt crimes can serve as an early warning to an offender, who is put on notice from their misstep that even incomplete crimes against children will not be tolerated.

Mandatory Reporting

Require ISPs to report suspected CSAM to law enforcement or another mandated agency.

Organizations or corporations, the services of which are being used to proliferate CSAM activities, should exercise a certain amount of industry responsibility in their day-to-day business operations. It is crucial that ISPs report illicit content discovered on their networks to law enforcement or another mandated agency as soon as the company becomes aware of it, whether through content management or reports from their users. A "notice and takedown" requirement should be enacted within national legislation, and consideration should be given to statutory protections that would allow ISPs to fully and effectively report CSAM, including the transmission of images, to law enforcement or another designated agency.

---

103 Luxembourg Guidelines, *supra* note 23, at 52.

104 United States Federal Bureau of Investigation, *How We Can Help You Sextortion*, *at* https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/sextortion (last visited Jul. 25, 2023) (on file with the International Centre for Missing & Exploited Children).

105 United States Attorney's Office Southern District of Indiana, *FBI and Partners Issue National Public Safety Alert on Sextortion Schemes*, Jan. 19, 2023, *at* https://www.justice.gov/usao-sdin/pr/fbi-and-partners-issue-national-public-safety-alert-sextortion-schemes (last visited Jun. 27, 2023) (on file with the International Centre for Missing & Exploited Children).

106 *See*, International Centre for Missing & Exploited Children, *Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review*, 2017, *at* https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

Legislative language providing for sufficient and substantial penalties (i.e., monetary fines, imprisonment) for failure to report illegal content should be given serious consideration. The enforcement of such penalties acts as an incentive for companies to be proactive and responsible. UNODC's Expert Group stated that "the most basic requirement of the State is to create and maintain a legal framework which allows or requires action to protect children from violence by all relevant entities operating within its jurisdiction." [107]

NCMEC's CyberTipline is a mechanism for the public and ISPs to report instances of suspected sexual exploitation. In 2022 alone, NCMEC reported that of the 32 million reports received by the CyberTipline, 31.8 million reports were from ISPs.[108]

Encourage banks, credit card companies, and others in the payments industry to report suspected CSAM to law enforcement or another mandated agency.

In addition to ISPs, credit card companies, banks, and other financial institutions within the payment industry should also be encouraged to report suspected CSAM transactions. The ability to use credit cards, money transfers, digital currency, and other payment methods to purchase CSAM has made it easier than ever to obtain CSAM. Moreover, distribution through ICTs has facilitated instant access to potentially millions of individuals worldwide. In response, financial companies must be vigilant and should be required to report CSAM transactions to law enforcement or other mandated agencies.

The U.S. FCACSE[109], founded in 2006, is an example of banks, credit card companies, electronic payment networks, and third-party payment companies proactively coordinating with law enforcement, ISPs, along with civil society to eradicate the commercial trade of CSAM online. The success of the U.S. FCACSE led to its expansion in Europe[110] and the Asia Pacific[111] region and the opening of an ICMEC Australia office focused on partnering with the financial payments industry to develop tools to better detect and report commercial child sexual exploitation and abuse online.

The FCACSE provides resources and tools to assist payments companies with evaluating their procedures for detecting and preventing individuals from using the company's services to trade in CSAM online.

---

107 UNODC, *Background Paper - Towards Zero: An Initiative to Reduce the Availability of Child Sexual Abuse Material on the Internet*, Jun. 2023, at https://www.unodc.org/pdf/criminal_justice/endVAC/EGM/EGM_CSAM_Removal_Background_Paper.pdf?ref=verifymy.io (last visited Sep. 18, 2023) (on file with the International Centre for Missing & Exploited Children).

108 National Center re for Missing and Exploited Children, *Our 2022 Impact*, at https://www.missingkids.org/content/dam/missingkids/pdfs/2022-ncmec-our-impact.pdf (last visited Jul. 6, 2023) (on file with the International Centre for Missing & Exploited Children).

109 International Centre for Missing & Exploited Children, *U.S. Financial Coalition Against Child Sexual Exploitation*, at Financial Coalition Against Child Sexual Exploitation: https://www.icmec.org/financial-coalitions/ (last visited Jul. 11, 2023).

110 Europol, *Crimes Areas – Child Sexual Exploitation*, at https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/child-sexual-exploitation (last visited Sep. 18, 2023).

111 International Centre for Missing & Exploited Children, *Asia-Pacific Financial Coalition Against Child Sexual Exploitation*, at https://www.icmec.org/apfc-asia-pacific-financial-coalition-against-child-sexual-exploitation/ (last visited Jul. 11, 2023).

Require healthcare and social services professionals, teachers, in addition to others who come into contact with children in their everyday, professional capacity to report suspected CSAM to law enforcement or another mandated agency.

This group may include, but is not necessarily limited to, healthcare and social services professionals, and teachers, school counselors, in addition to others in child-serving professions. As a first line of defense, these child-serving professionals are often the first to notice signs of physical or emotional abuse. Based on daily interactions with children, these individuals may develop well-founded suspicions about potential child victims. A penalty in the form of a fine or imprisonment for failure to report suspected child sexual abuse should be considered.

Require photo developers, IT professionals, website moderators, and others who, in their everyday professional capacity, do not come into contact with children but may potentially be exposed to CSAM as a result of their job responsibilities, to report suspected CSAM to law enforcement or another mandated agency.

Not long ago, this group was comprised of photo developers who may have come across these CSAM while processing film. However, with the increased use of technology, these images are now more likely to be found in digital form. IT professionals may accidentally discover CSAM during their routine work while repairing or servicing a computer or smartphone, monitoring social networking websites or apps, accessing links or pop-ups, or using image-hosting or file-sharing software. This class of individuals should not be required to search for illegal material but rather to report it to the appropriate authorities if found.

Industry Responsibility

Allow companies to deploy technology tools and mechanisms to protect children from online sexual abuse.

Technology companies should be allowed as well as encouraged to utilize technology tools to scan their networks to identify and eliminate CSAM.[112] ISPs may also employ filtering or blocking technologies to impede access to CSAM.[113] Tools like PhotoDNA[114] can detect CSAM being uploaded, shared, and stored on devices connected to a network so that it can be removed. Initiatives like Project Arachnid use technology tools to crawl publicly accessible URLs/media previously reported to Cybertip.ca by the public or participating industry members and certain areas of the dark and clear web known to host CSAM to detect CSAM, and determine where these images and/or videos are available on the internet before issuing a notice to the hosting provider requesting immediate removal of the illegal content.[115] Industry can also use the Arachnid API[116] to quickly detect CSAM on their service,

---

[112] Desiderata (blogpost) by John Carr, *Read this and weep*, Nov. 10, 2018, *at* https://johnc1912.wordpress.com/2018/11/10/read-this-and-weep/ (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children). *See also*, Child Dignity in the Digital World, *supra* note 45, at 7.

[113] Mark Hachman, *How Google handles child pornography in Gmail, search*, PCWORLD, Aug. 5, 2014, *at* https://www.pcworld.com/article/2461400/how-google-handles-child-pornography-in-gmail-search.html (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

[114] Microsoft, *PhotoDNA*, *at* https://www.microsoft.com/en-us/photodna (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

[115] Project Arachnid: Online Availability of Child Sexual Abuse Material, *supra* note 6.

rather than waiting for Project Arachnid to detect material and send a notice.[117] Since it was launched in 2017, Project Arachnid has removed 7 million images and videos of CSAM from more than 1,000 electronic service providers in nearly 100 countries.[118] ISPs can proactively utilize technology tools like these to detect illegal content on their networks and speed up their removal.

Regional legal instruments provide some guidance in this regard. For instance, Article 30 (5) of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) requires each Party to take the necessary legislative or other measures to ensure an effective investigation and prosecution of relevant offenses; and to enable units or investigative services to identify victims by analyzing CSAM including photographs and audio-visual recordings transmitted or made available through the use of ICTs.[119] Likewise, Article 25 of the European Union (EU) Directive on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography requires all Member States to take the necessary measures to promptly remove web pages containing or disseminating CSAM in their territory and "to block access to web pages containing or disseminating [CSAM] towards the Internet users within their territory."[120]

A specific exemption should be incorporated into national legislation allowing businesses to deploy tools like these designed to protect children.

Legislation tackling CSAM should also address the challenge posed by end-to-end encryption (E2EE). E2EE is a method of secure communication that only allows the users communicating with one another to read and view the content and prevents third parties from accessing any of the data.[121] Numerous technology firms have embraced, or are in the process of embracing, E2EE. While implementing E2EE enhances the security of online data, it also carries potentially significant consequences, such as hindering the ability of law enforcement agencies operating within legal parameters to monitor and collect insights into the online activities of individuals engaged in the exploitation of children, resulting in the undetected distribution of CSAM.[122]

---

116 API is the acronym for Application Programming Interface, which is a software intermediary that allows two applications to talk to each other. *See*, Mulesoft, *What is an API (Application Programming Interface)?*, *at* https://www.mulesoft.com/resources/api/what-is-an-api (last visited Jul. 26, 2023).

117 Project Arachnid: Online Availability of Child Sexual Abuse Material, *supra* note 6.

118 Canadian Centre for Child Protection, *Programs & Initiatives - Project Arachnid*, *at* https://protectchildren.ca/en/programs-and-initiatives/project-arachnid/ (last visited Sep. 18, 2023).

119 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201), Oct. 25, 2007, *at* http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm *entered into force Jul. 1, 2010* (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

120 Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, Articles 18-20 (Dec. 13, 2011), *at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:EN:PDF (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children). (Corrigendum to Directive 2011/92/EU, '2011/92/EU' to be read as '2011/93/EU', http://db.eurocrim.org/db/en/doc/1715.pdf (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

121 Riana Pfefferkorn, *EU Member States Still Cannot Agree About End-To-End Encryption*, Stanford Law School, Jun. 8, 2023, *at* https://cyberlaw.stanford.edu/blog/2023/06/eu-member-states-still-cannot-agree-about-end-end-encryption (last visited Jul. 11, 2023) (on file with the International Centre for Missing & Exploited Children).

122 United States Department of Justice, *Technology*, Jun. 2023, *at* https://www.justice.gov/d9/2023-06/technology_2.pdf (last visited Jul. 11, 2023) (on file with the International Centre for Missing & Exploited Children).

The debate around E2EE in relation to the online safety of children has largely focused on whether regulating E2EE might lead to additional encroachments on individual privacy.[123] Sixty-six percent of 8,000 European children between the ages of 13 to 17 years oppose scanning their messages.[124]

Meta has announced it "plans to roll out default end-to-end encryption for its Messenger product" by the end of 2023 and shortly thereafter for Instagram. Meta has stated that it "is committed to providing the ability for people to communicate privately with their friends and loved ones where they have confidence that no one else can see into their conversations."[125] WhatsApp, an encrypted messaging service within the Meta platform, already uses E2EE.

While there is currently no statistical data available that accurately estimates the extent and gravity of child exploitation occurring within encrypted environments, E2EE potentially presents a serious risk to children, especially within platforms where children use the application alongside adults.[126] The U.K.'s National Crime Agency estimates that implementing E2EE – a "privacy-friendly technology" – will lead to sharp reductions in abuse referrals to NCMEC and other hotlines.[127] This will result in countless incidents of online child sexual exploitation remaining hidden and victims going unidentified.[128]

Require the retention and/or preservation of (non-content) data by ISPs.

Data retention is the obligation of ISPs to retain computer data for a specific period of time. Data can be classified as non-content data (i.e., traffic data such as an IP address, the date, time, size, type, duration, and source of communication[129]; and location data,[130] which is data that helps identify the subscriber) or content data (i.e., the text of users' emails, the "message" that was delivered by communication, or the contents of a file such as an image or film[131]). Data preservation is the obligation to preserve stored data with the probative value of an identified user who is currently under investigation after a request by law

---

123 Joseph Marks, *Lawmakers want to crack down on child porn but there's a cyber downside*, THE WASHINGTON POST, *at* https://www.washingtonpost.com/politics/2022/02/11/lawmakers-want-crack-down-child-porn-there-cyber-downside/ (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

124 Tamas Orban, *European Youth Rejects Mass Surveillance Aimed at Protecting Minors*, The European Conservative, *at* https://europeanconservative.com/articles/news/european-youth-rejects-mass-surveillance-aimed-at-protecting-minors/ (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

125 Makena Kelly, *Meta refreshes promise to roll out default end-to-end encryption in Messenger this year*, THE VERGE, Aug. 22, 2023, at https://www.theverge.com/2023/8/22/23841490/meta-facebook-messenger-instagram-encryption-default (last visited Sep. 20, 2023) (on file with the International Centre for Missing & Exploited Children).

126 United States Department of Justice, Technology, *supra* note 122.

127 Dan Milmo, *Meta encryption plan will let child abusers 'hide in the dark', says UK campaign*, THE GUARDIAN, Sep. 20, 2023, at https://www.theguardian.com/technology/2023/sep/20/meta-encryption-plan-will-let-child-abusers-hide-in-the-dark-says-uk-campaign (last visited Sep. 20, 2023) (on file with the International Centre for Missing & Exploited Children).

128 United States Department of Justice, Technology, *supra* note 122.

129 Convention on Cybercrime, *opened for signature* Nov. 23, 2001, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm *entered into force* Jul. 1, 2004 (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children); European Commission Directorate General for Home Affairs, *Evidence of Potential Impacts of Options for Revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries* 4, Article 1, d (Nov. 2012) (on file with the International Centre for Missing & Exploited Children).

130 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2016 on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending Directive 2002/58/EC, Article 2(2)(a), [hereinafter *EU Data Retention Directive*], at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:en:HTML (last visited Jul. 26, 2023 (on file with the International Centre for Missing & Exploited Children).

131 Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1030 (2010) (on file with the International Centre for Missing & Exploited Children).

enforcement. Guidelines for data retention and data preservation vary widely by country, industry, and type of data.

Effective data retention and preservation frameworks will include legal provisions that harmonize the obligations of ISPs while recognizing that these companies have different capabilities, technologies, and resources available. Legislation should indicate that the purpose for the retention and preservation of specified data is to support law enforcement investigations and the criminal prosecution of technology-facilitated crimes against children.

The law should clearly differentiate between the kinds of data that should and should not be retained (*i.e.*, content vs. non-content data), limit the scope and application of the data, and incorporate sufficient guarantees for the protection of the data against unlawful access and abuse. A minimum specified period also should be defined for the retention of non-content data such as subscriber information, traffic data, and location data.

It is important that ISPs have a process in place for prompt response to subpoenas or law enforcement requests for data. ISPs should be obligated to respond to preservation orders for data as soon as possible. The period of time that requested data must be preserved should also be outlined with the option to request an extension.

Encourage cross-sector coordination and collaboration between industry and law enforcement.

Increased communication and cooperation between law enforcement organizations and the private sector industry – including ISPs, financial institutions, and payments industry – also should be encouraged and supported to better combat online sexual abuse and exploitation of children.[132]

The Lanzarote Convention requires all State Parties to take the necessary measures to ensure local and national coordination between agencies (i.e., education sector, health sector, social services, law enforcement, and judicial authorities) responsible for the protection from and prevention of child sexual abuse and exploitation.[133] It further requires State Parties to encourage cooperation between the competent state authorities, civil society and the private sector, in order to better combat child sexual abuse and exploitation.[134]

One example of ongoing cross-sector coordination can be found in ICMEC's Financial Coalition Against Child Sexual Exploitation (FCACSE)[135] that first launched in the U.S. in 2006, in collaboration with NCMEC. The FCACSE is a groundbreaking alliance between private industry and the public sector in the battle against commercial child sexual exploitation, to advocate for, support, and sustain the efforts of financial services companies to better protect children.

---

132 Kate Dean, *Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes* 8, Jan. 25, 2011 (on file with the International Centre for Missing & Exploited Children).

133 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201), *supra* note 119, at Article 10 (1).

134 *Id.* at Article 10 (3).

135 *Financial Coalition Against Child Sexual Exploitation*, ICMEC, at https://www.icmec.org/financial-coalitions/ (last visited Sep. 20, 2023).

The FCACSE is made up of leading banks, credit card companies, electronic payment networks, third-party payments companies, and internet services companies. The Coalition endeavors to follow the flow of funds and shut down the payment accounts used by these illicit enterprises or individual offenders. As a result of the FCACSE's efforts, the use of credit cards to purchase CSAM online has been drastically reduced globally. Innovations in the payments industry have increased the range of digital and electronic payment options, creating a complex web of financial transaction chains across multiple financial institutions and jurisdictions. Websites containing CSAM now favor these over traditional payment methods like credit cards where it is easier to trace the transaction to potential purchasers.

Through their participation, member companies have developed and fine-tuned existing transaction due diligence to better detect and report instances of child sexual exploitation and abuse, and work toward prevention. In addition, the FCACSE enables member companies to learn from each other and facilitates the sharing of knowledge and insights across a diverse stakeholder group and across countries and regions. ICMEC and the FCACSE continue to fight those who seek to profit from the sexual exploitation of children through expanded areas of focus, such as child sex trafficking, sextortion, livestreamed CSA, and the use of new digital payment methods and cryptocurrencies to purchase CSAM.

The WeProtect Global Alliance is another example of cross-sector collaboration. The Global Alliance is a public-private partnership consisting of governments, private sector companies, civil society organizations, and intergovernmental organizations working together to transform the global response to child sexual exploitation and abuse online.[136] WeProtect's Model National Response (MNR) provides countries with a roadmap for collaborative, multi-disciplinary national responses to address child sexual exploitation and abuse online.[137]

Sanctions and Sentencing

Address the criminal liability of children involved in CSAM.

There should be no criminal liability for children involved in CSAM. This should be clearly stated in national legislation. Regardless of whether a child is a compliant victim or a non-cooperative witness, the fact remains that they are a child victim. Criminal liability must focus on the adult offender, who is responsible for the exploitation of the child, and on the crimes committed against the child.

Legal provisions should be enacted to allow for protection of the child victim as a witness in any judicial proceedings that may occur. This includes permitting closed-circuit testimony in certain circumstances and establishing guidelines for the presence of victim advocates in the courtroom.

---

136 WeProtect Global Alliance, *The Alliance*, at https://www.weprotect.org/alliance/ (last visited Sep. 20, 2023).

137 WeProtect Global Alliance, *The Model National Response*, at https://www.weprotect.org/the-model-national-response/ (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

Enhance penalties for repeat offenders, organized crime participants, and other factors that may be considered upon sentencing.

All violations of enacted anti-CSAM legislation should carry strict sentences that will be enforced, thereby guaranteeing a true deterrent effect.[138] Mere fines and misdemeanor classifications are not enough.

Sentencing provisions should take into account aggravating factors and enhancements.[139] Aggravating factors may include the number of images manufactured, produced, distributed, and possessed; the severity of the offender's existing criminal record; the sexual violence toward the children (including rape, torture, and bondage) being depicted in the images that were manufactured, produced, distributed, and possessed; and any potential threat or risk the offender may pose to the community upon release.

Media outlets have reported that criminals other than sex offenders, including terrorists, organized criminals, and gangs, have been found with CSAM. For instance, there have been reports of terrorists manufacturing CSAM to send concealed messages and data[140] and finance their activities,[141] and organized criminals and gangs involved in human trafficking generating additional revenue by producing sexually exploitative images of their victims, blackmailing victims into compliance, and advertising commercial sexual services.[142] The FBI reports that several sophisticated online criminal organizations using the Dark Web have written security manuals, including security protocols and encryption techniques, to help their members elude law enforcement and facilitate the sexual abuse of children.[143]

These examples suggest that CSAM may be connected to crimes beyond child sexual abuse. A sentencing enhancement for other criminal activities, such as human trafficking, could have a deterrent effect or disrupt the flow of organized crime.

Assets must be forfeited.

Convicted defendants should be subject to forfeiture provisions that allow for the confiscation of property, proceeds, or assets that resulted from CSAM activities.[144] Confiscated funds could, in turn, be used to support programs for formerly sexually exploited children, children at risk of being sexually exploited, and child victims who are in need of special care.[145]

---

138 Eva J. Klain, *Prostitution of Children and Child-Sex Tourism: An Analysis of Domestic and International Responses* 47 (Nat'l Ctr. for Missing & Exploited Children ed., 1999) (on file with the International Centre for Missing & Exploited Children).

139 *Id.*

140 Richard Kerbaj and Dominic Kennedy, *Link Between Child Porn and Muslim Terrorists Discovered in Police Raids*, TIMES ONLINE, Oct. 7, 2008 (on file with the International Centre for Missing & Exploited Children).

141 Sergey Stefanov, *Russia Fights Child Porn and Terrorism on the Internet*, PRAVDA, Dec. 4, 2002, *at* http://english.pravda.ru/hotspots/terror/04-12-2002/1620-porn-0/ (on file with the International Centre for Missing & Exploited Children); *see also*, Richard Kerbaj and Dominic Kennedy, *supra* note 140.

142 Tania Branigan, *Criminal gangs moving into child internet porn*, THE GUARDIAN ONLINE, Jul. 30, 2006, *at* http://www.theguardian.com/uk/2006/jul/31/immigration.ukcrime (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

143 U.S. Department of Justice – CEOS, *supra* note 96.

144 Eva J. Klain, *supra* note 138, at 130.

145 *Id.*

Law Enforcement Investigations & Data Retention

In the U.S., there has been ongoing discussion for many years concerning the importance of computer data to law enforcement investigations of online CSAM. The discussion has focused on the need for legal provisions requiring ISPs to retain and preserve data. To effectively conduct investigations in cases of online child sexual abuse, law enforcement regularly requires access to computer data, but often discovers that it has been deleted, making it more difficult or even impossible to find and prosecute the offender.[146]

According to the U.S. Department of Justice 2023 National Strategy for Child Exploitation Prevention and Interdiction, "[f]or over two decades, investigations have been stymied because internet service providers do not retain data that can be used to identify individuals using a particular internet protocol address on a given date and time, or they do not retain it long enough such that the data is gone even when law enforcement quickly serves legal process. Obtaining that information is critical because it often provides the bridge between online sexual abuse and the real-world abuser."[147] Furthermore, the Strategy notes that "many apps have short or non-existent data retention policies, which are a discretionary decision of each company, leave law enforcement with little room for delay in initiating a legal process. Data retention, or the lack thereof, is one of the biggest barriers to the successful identification of a potential offender."[148]

Individual ISPs generally have the ability and technological capacity to retain and preserve users' data to make it available for purposes of criminal prosecution. Thus, the purpose of mandating data retention is to prevent loss or modification of stored computer data for a specific period of time so that it can be used as evidence during an investigation.[149] The suggestion, however, that data retention by ISPs should be mandatory has spurred active debate as opponents raised privacy and free speech concerns.[150]

The 2020 Interim Code of Practice on Online Child Sexual Exploitation and Abuse by the U.K. Home Office provides guidance for companies to combat online child sexual abuse. Under Reporting Guidance, the Code recommends that when reporting suspected CSAM, companies "should retain all available account data related to the report, including content and metadata, where the company has the capacity and capability, in accordance with national data protection legislation. Law enforcement may request this data through a lawful process at a later stage to support an investigation or prosecution."[151]

---

146 Jason Weinstein, *Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes* 5, Statement before the Committee on Judiciary Subcommittee on Crime, Terrorism, and Homeland Security United States House of Representatives (Jan. 25, 2011) (on file with the International Centre for Missing & Exploited Children).

147 U.S. Department of Justice, *2023 National Strategy for Child Exploitation Prevention and Interdiction*, *at* https://www.justice.gov/psc/national-strategy-child-exploitation-prevention-and-interdiction (last visited Sep. 27, 2023) (on file with the International Centre for Missing & Exploited Children).

148 *Id.*

149 Department of Justice of Canada, *Lawful Access FAQ* 4 (2005) (on file with the International Centre for Missing & Exploited Children).

150 *Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes*, CDT, Jan. 24, 2011, *at* https://cdt.org/insight/data-retention-as-a-tool-for-investigating-internet-child-pornography-and-other-internet-crimes/ (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

151 UK Home Office, *Interim code of practice on online child sexual exploitation and abuse*, Dec. 15, 2020, *at* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944034/1704__HO__INTERIM_CODE_OF_PRACTICE_CSEA_v.2.1_14-12-2020.pdf (last visited Sep. 27, 2023) (on file with the International Centre for Missing & Exploited Children).

Until recently, the primary international instruments addressing this matter were the Council of Europe Convention on Cybercrime (Budapest Convention), adopted in 2001, which incorporates recommendations for data preservation measures,[152] and the 2006 EU Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks (Data Retention Directive). The Budapest Convention sought to address internet and computer crime by harmonizing national laws, improving legislative techniques, and increasing cross-border cooperation. The Data Retention Directive focused on the retention of non-content data (i.e., traffic data like IP address, the date, time, size, type, duration, and source of communication[153]; and location data[154]).[155] The objective of the Data Retention Directive is to harmonize the obligations of providers to retain this type of data (i.e., traffic and location data) by requiring all Member States to adopt a standard set of data retention policies.[156] The Directive was issued with the recognition that data retention is "a necessary and effective investigative tool for law enforcement…" for the "prevention, investigation, detection and prosecution of criminal offences, in particular organized crime and terrorism."[157] These laws significantly influenced national legislation concerning cybercrime and data processing, protection, and retention.

In April 2014, the European Court of Justice (ECJ) invalidated the Data Retention Directive and reaffirmed its ruling in 2016.[158] While the ECJ upheld the value of data retention for law enforcement investigations of serious crimes and recognized its appropriateness given the growing importance of electronic communication,[159] the Directive as a whole was held to be invalid with regard to the right to privacy as protected by the Charter of Fundamental Rights of the EU.[160] Far from abandoning the concept of data retention, the ECJ suggested that EU Member States choosing to alter existing national legislation or introducing new laws on data retention should do so in contemplation of its ruling and recommendations.[161] Following the ECJ ruling, data retention laws in numerous countries were voided.

---

152 Convention on Cybercrime (CETS 185), Nov. 23, 2001, at https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 *entered into force Jul. 1, 2004* (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

153 Convention on Cybercrime (CETS 185), *supra* note 143; European Commission Directorate General for Home Affairs, *Evidence of Potential Impacts of Options for Revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries* 4, Article 1, d (Nov. 2012) (on file with the International Centre for Missing & Exploited Children).

154 EU Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks, Article 2, §2, a (Mar. 15, 2006), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:en:HTML (last visited Jul. 26, 2023) [hereinafter *EU Data Retention Directive*] (on file with the International Centre for Missing & Exploited Children).

155 *Id.*

156 *Id.*

157 *Id.* at recitals (7) and (9).

158 Judgment of the European Court of Justice (Grand Chamber), 8 April 2014, in joined Cases C-29 3/12 and C-594/12, at 43-44, 49 and 51 (on file with the International Centre for Missing & Exploited Children). *See also,* Judgment of the CJEU (Grand Chamber) of 21 December 2016, joined cases C-203/15 and C-698/15 (on file with the International Centre for Missing & Exploited Children).

159 *Id.*

160 Charter of Fundamental Rights of the European Union 2000/C 364/01, Articles 7, 8, and 52(1), at http://www.europarl.europa.eu/charter/pdf/text_en.pdf; *See also,* Judgment of the European Court of Justice (Grand Chamber), *supra* note 158, at 69 (on file with the International Centre for Missing & Exploited Children).

161 Judgment of the European Court of Justice (Grand Chamber), *supra* note 158, paragraphs 39-45.

Since then, a global paradigm shift in data privacy regulation has occurred.[162] In 2016, the General Data Protection Regulation (GDPR) was approved by the EU Parliament.[163] The GDPR, which replaced the earlier EU Data Protection Directive,[164] is more heavily focused on protecting individual users' right to privacy and regulating how data is handled.[165] The GDPR enables EU citizens to have better control of their personal data. Moreover, this forces companies to think carefully about the data they hold, while simultaneously making them accountable for how they use and store the data.[166] Since the GDPR is a regulation, under EU law it is legally binding and directly applicable. Consequently, it does not require national implementation. EU Member States were required to comply with the GDPR by 25 May 2018.[167]

Alongside the GDPR came the introduction of the new EU Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data.[168] Directive 2016/680 governs the handling of data in law enforcement situations.[169] EU Member States were required to adopt the laws, regulations, and administrative provisions

---

162 Dr. Rao Papolu, *In the Wake of GDPR, It Can't Be Business As Usual With Consumer Data Privacy*, FORBES, Sep. 18, 2018, at https://www.forbes.com/sites/forbestechcouncil/2018/09/18/in-the-wake-of-gdpr-it-cant-be-business-as-usual-with-consumer-data-privacy/ (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

163 EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (last visited Jul. 26, 2023).

164 EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

165 For information regarding children's personal data protection and the GDPR, see the Information Commissioner's Office, *UK GDPR Guidance and Resources, Children's Information*, at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/ (last visited Sep. 10, 2023) (on file with the International Centre for Missing & Exploited Children).

166 According to Article 3 of the GDPR, the regulation may also protect individuals located outside of the EU when: 1) a controller or processor is established in the EU and processes personal data in the context of the activities of that establishment; 2) a controller or processor is not established in the EU but processes personal data relating to the offering of goods or services to individuals in the EU; or 3) a controller or processor is not established in the EU but monitors the behavior of individuals in the EU. See, Hunton Andrews Kurth LLP, Privacy & Information Security Law Blog, *EDPB Publishes Guidelines on Extraterritorial Application of the GDPR*, Nov. 27, 2018, at https://www.huntonprivacyblog.com/2018/11/27/edpb-publishes-guidelines-on-extraterritorial-application-of-the-gdpr/ (last visited Jul. 26, 2023). *See also*, European Data Protection Board, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation*, adopted Nov. 16, 2018, at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

167 EU General Data Protection Regulation (GDPR), *supra* note 163.

168 EU Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680 (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

169 International Association of Privacy Professionals, *GDPR, Directive 2016/680, PNR officially published*, May 5, 2016, at https://iapp.org/news/a/gdpr-directive-2016680-pnr-officially-published/ (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

necessary to comply with the Directive by 6 May 2018.[170] As of 15 November 2018, 16 countries have adopted the Directive into national law.[171]

Under the GDPR and Directive 2016/680, "personal data" is defined as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[172] This definition is slightly expanded from that of the prior Data Protection Directive, which defined "personal data" as "any information relating to an identified or identifiable natural person ('data subject')" including "reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[173] Moreover, this identifying data is a departure from the approach of the Data Retention Directive that defined "data" only as traffic data and location data and the related data necessary to identify the subscriber or user.[174]

The GDPR further dictates specific rules on its territorial scope.[175] It applies not only to businesses established in the EU, but also to controllers and processors outside the EU that monitor or offer goods and services to EU residents, exponentially expanding the reach and applicability of the GDPR.[176] Article 2 of the GDPR provides for data processing "by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."[177]

The GDPR and Directive 2016/680 provide limitations on how long personal data may be kept. Under the GDPR, personal data can be retained for "no longer than is necessary for the purposes for which the personal data are processed."[178] Moreover, Directive 2016/680 gives Member States the ability to "provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for storage of personal data."[179] These limitations are in place to ensure that irrelevant, excessive, inaccurate, or out-of-date information is no longer being stored.[180]

---

170 *Id.* at Article 63.

171 EUR-Lex, *National Transposition by Member State*, *at* https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32016L0680 (last visited Nov. 26, 2018).

172 EU General Data Protection Regulation (GDPR), *supra* note 163 at Article 4 – Definitions.

173 EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *supra* note 164, at Article 2 – Definitions.

174 EU Data Retention Directive, *supra* note 153, at Article 2 – Definitions.

175 EU General Data Protection Regulation (GDPR), *supra* note 163, at Article 3 – Territorial Scope.

176 A&L Goodbody, *The GDPR: A Guide for Businesses* 6, Oct. 5, 2016, *at* https://www.algoodbody.com/media/The_GDPR-AGuideforBusinesses1.pdf (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children)

177 EU General Data Protection Regulation (GDPR), *supra* note 163, at Article 2 – Material Scope.

178 Information Commissioner's Office, For organisations / Guide to the General Data Protection Regulation (GDPR) / Principles, *Principle (e): Storage limitation*, *at* https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/ (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

179 *Id.*

180 *Id.*

In relation to law enforcement efforts in CSAM cases, Article 10 of the GDPR allows for the "processing of personal data relating to criminal convictions and offences" so long as there are lawful grounds for processing, including the performance of a task carried out in the public interest or for legitimate interests pursued by the data controller.[181]

The GDPR has had a global impact, requiring compliance from companies around the world. In response, many countries have worked to update domestic legislation to align more closely with the EU's privacy-based approach.[182] As of 2023, 17 countries outside of the EU have implemented data protection laws similar to the GDPR[183], while others continue to rely on existing legislation.

The need for data regarding CSAM has not diminished over the years. In 2017, in a hearing before the Subcommittee on Crime and Terrorism of the U.S. Senate Committee on the Judiciary, Deputy Assistant Attorney General Brad Wiegmann gave testimony concerning the need for law enforcement to be able to access data held by U.S. communications service providers outside of the U.S.[184] Specifically, he emphasized that "(t)he need for effective, efficient, and lawful access to data in criminal investigations is paramount in the digital age. Obstacles to obtaining such electronic evidence jeopardize investigations into every category of criminal activity – including terrorism, financial fraud, drug trafficking, child sexual exploitation, human trafficking, and computer hacking."[185]

As countries adapt or introduce new legislation and companies revamp internal policies to comply with the GDPR, the handling of data concerning investigations of criminal offenses like online child sexual abuse may become clearer. It remains imperative that law enforcement have the proper tools to fight online crime and protect children from abuse, molestation, and exploitation. Moreover, it is necessary that related laws strike a balance between child protection and the protection of privacy.

---

181 EU General Data Protection Regulation (GDPR), *supra* note 163, at Article 6 – Lawfulness of processing; Article 10 – Processing of personal data relating to criminal convictions and offences.

182 Mark Scott and Laurens Cerulus, *Europe's new data protection rules export privacy standards worldwide*, Politico, Feb. 6, 2018, at https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/ (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

183 GDPR Advisor, *GDPR Countries 2023*, at https://www.gdpradvisor.co.uk/gdpr-countries (last visited Sep. 28, 2023).

184 Hearing before the Subcommittee on Crime and Terrorism of the Committee of the Judiciary of the U.S. Senate, *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights*, May 24, 2017, at https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Wiegmann%20Testimony.pdf (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

185 *Id.*

Regional and International Law

Successfully combating CSAM and child exploitation on a global scale requires uniform legislation; laws that vary from country to country weaken the stance against child sexual exploitation and allow child predators to concentrate efforts in countries where they know they can best exploit children. A uniform approach is the most effective means of combating the sexual exploitation of children because it, among other things, allows for consistency in criminalization and punishment; raises public awareness of the problem; increases services available to assist victims; and improves overall law enforcement efforts at the national and international levels. Complying with international legal standards is an initial step in addressing CSAM, which should be followed by implementing national legislation and the creation of a national legislative scheme to combat CSAM.

The main international legal instrument that addresses CSAM is the Optional Protocol to the UN Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.[186] Another critical international treaty is the International Labour Organization (ILO) Convention Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour also includes the use of children for the production of pornography as one of the worst forms of child labour.[187]

In addition to these international legal instruments, there are several regional legal instruments that are relevant in the fight against CSAM. The Council of Europe's Convention on Cybercrime[188] and Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[189] are effective tools for combating the sexual exploitation and abuse of children because they contain specific definitions of offenses as well as provisions requiring punishment for criminalized behavior.

The EU adopted the Directive on combating the sexual abuse and sexual exploitation of children and child pornography, which came into force upon adoption.[190] EU Member States were required to come into compliance with the Directive by transposing into their national law the obligations imposed by the Directive by the end of 2013. To date, 26 EU Member States have taken steps to implement this Directive under their national law.[191]

---

186 Optional Protocol, *supra* note 25.

187 *Convention concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour (ILO 182)*, 1999 2000, at https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C182 *entered into force Nov. 19, 2000* (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

188 Convention on Cybercrime (CETS 185), *supra* note 151.

189 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201), *supra* note 119.

190 Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, Articles 18-20 (Dec. 13, 2011), at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:EN:PDF (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children). (Corrigendum to Directive 2011/92/EU, '2011/92/EU' to be read as '2011/93/EU', http://db.eurocrim.org/db/en/doc/1715.pdf (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

191 National Implementing Measures (NIM) communicated by the Member States concerning**:** Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, at http://eur-lex.europa.eu/legal-

In comparison to the Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, the Directive establishes more explicit guidelines for criminal legislation on sexual abuse and exploitation of children. In particular, the Directive provides recommendations for terms of imprisonment for certain offenses, describes measures for the treatment of offenders, and contains provisions on supporting and protecting child victims with a focus on the best interests of the child.[192]

The African Charter on the Rights and Welfare of the Child[193] and the African Union Convention on Cyber Security and Personal Data Protection[194] serve to promote the best interests of children in the region and protect them from sexual abuse and exploitation.

Like the African Union Convention, the Arab Convention on Combating Information Technology Offences focuses on the use of ICTs to commit offenses such as the production, publication, and sale of CSAM.[195]

While not a binding legal instrument, the Association of Southeast Asian Nations (ASEAN) Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN[196] bears mentioning. The Declaration was adopted at the 35th ASEAN Summit in November 2019 by all 10 ASEAN Member States. It notes concern at the emerging global threats that are making more children vulnerable to the production and sharing of online CSAM and other forms of online child exploitation. It reaffirms the ASEAN Member States' commitment to the UN 2030 Agenda for Sustainable Development. The Declaration makes seven recommendations meant to better protect children from online harm, including strengthening legislation, enhancing law enforcement capacity, establishing national specialized units, increasing the effectiveness of child protection and support services, strengthening data collection and monitoring, reporting, and referral mechanisms, promoting national education programs, and mobilizing engagement with the private sector and others.

In conjunction with international and regional legal instruments, there have been several notable global initiatives that support cross-border coordination and collaboration to end the abuse, exploitation, trafficking, and all forms of violence against children. For example, the UN Sustainable Development Goals (SDGs) of the 2030 Agenda for Sustainable

---

content/EN/NIM/?uri=CELEX:32011L0093 (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

192 Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, *supra* note 190.

193 African Charter on the Rights and Welfare of the Child, 1990, at https://au.int/sites/default/files/treaties/36804-treaty-african_charter_on_rights_welfare_of_the_child.pdf *entered into force Nov. 29, 1999* (last visited Sep. 18, 2023) (on file with the International Centre for Missing & Exploited Children).

194 African Union Convention on Cyber Security and Personal Data Protection, 2014, at https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

195 League of Arab States, Arab Convention on Combating Information Technology Offences (Arab Convention), 2010, at https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf (last visited Sep. 18, 2023) (on file with the International Centre for Missing & Exploited Children).

196 Association of Southeast Asian Nations (ASEAN), Declaration on the Protection of Children from all Forms of Online Exploitation and Abuse in ASEAN, 2019, at https://asean.org/wp-content/uploads/2021/01/3-Declaration-on-the-Protection-of-Children-from-all-Forms-of-Online-Exploitation-and-Abuse-in-ASEAN.pdf (last visited Oct. 8, 2023) (on file with the International Centre for Missing & Exploited Children).

Development were adopted in September 2015 by world leaders and officially came into force on 1 January 2016.[197] The 17 Sustainable Development Goals are a collection of interlinked objectives designed to serve as a "shared blueprint for peace and prosperity for people and the planet, now and into the future."[198] The SDGs apply universally to all people and act as a call to action for all countries.[199] SDG 16 focuses on promoting peaceful and inclusive societies for sustainable development, providing access to justice for all, and building effective, accountable, and inclusive institutions at all levels. Specifically, SDG 16.2 aims to ensure the protection of children's rights and well-being and targets ending abuse, exploitation, trafficking, torture, and all forms of violence against children.[200]

In July 2023, the UN High-Level Political Forum on Sustainable Development (HLPF) convened to assess and map the progress that countries have made toward Agenda 2030 and achieving each of the SDGs. Though progress is being made to meet SDG 16 at large, progress towards SDG 16's sub-goals has been slow and uneven and, in many cases, backsliding; action is not yet advancing at the speed or scale required.[201] A recent report cites the biggest challenges to achieving the goal to be funding, accountability, and transparency, lack of data, and lack of inclusivity of marginalized communities.[202] It makes urgent recommendations for governments and the international community to improve data, financing, cooperation, and action towards SDG 16 and the 2030 agenda.[203] Progress in reducing sexual violence against children has likely been hindered by the increase in conflicts, natural disasters, and other humanitarian crises, as well as the increasing use of digital technologies by children, all of which put children at greater risk.[204] The COVID-19 pandemic and its related quarantine restrictions, lockdowns, and school closures have also likely contributed to delays, as some 85 million children were determined to be at greater risk of violence and more susceptible to sexual exploitation during the pandemic.[205]

With only seven years left to achieve the Sustainable Development Goals, the SDG 16Now campaign was launched, bringing together civil society, governments, UN agencies, philanthropic groups, and the private sector to work together to accelerate progress towards SDG 16.[206] At the September 2023 SDG Summit, the SDG16Now campaign aims to reinvigorate commitments and financing for SDG16 and bring progress towards the SDGs back on track.[207]

---

197 *The Sustainable Development Agenda*, United Nations, *at* https://www.un.org/sustainabledevelopment/development-agenda/ (last visited Jul. 26, 2023).

198 *Id.*

199 *Id.*

200 United Nations Sustainable Development Goals, *Goal 16: Peace, Justice and Strong Institutions*, *at* https://www.un.org/sustainabledevelopment/peace-justice/ (last visited Jul. 11, 2023).

201 United Nations, *The Sustainable Development Agenda*, *at* https://www.un.org/sustainabledevelopment/development-agenda/ (last visited Jul. 11, 2023).

202 Transparency, Accountability & Participation for 2030 Agenda, *Halfway to 2030: Report on SDG 16+*, *at* https://www.sdg16now.org/wp-content/uploads/2023/05/Halfway-to-2030-Report-Digital.pdf (last visited Jul. 24, 2023) (on file with the International Centre for Missing & Exploited Children).

203 *Id.*

204 *Id.*

205 End Violence Against Children, *Progress on SDG 16.2 to End Violence Against Children is Backsliding Finds new Analysis*, Jul. 20, 2023, *at* https://www.end-violence.org/articles/progress-sdg-162-end-violence-against-children-backsliding-finds-new-analysis (last visited Jul. 24, 2023) (on file with the International Centre for Missing & Exploited Children).

206 SDG16Now, *#SDG16Now Campaign*, *at* https://www.sdg16now.org/ (last visited Jul. 24, 2023).

207 *Id.*

Another notable initiative is the WeProtect Model National Response (MNR), which supports the implementation of the SDGs with a particular focus on ending abuse, exploitation, trafficking, and all forms of violence against children.[208] The MNR is intended to help "countries to establish and develop coordinated national responses to online child sexual exploitation" by detailing specific capabilities needed for an effective child protection approach, highlighting existing good practices, and identifying resources for further guidance and support.[209]

As online child sexual exploitation and abuse continue to grow and diversify, the WeProtect Global Alliance and UNICEF worked together to conduct a review of the MNR, capturing an extensive body of experience across 42 countries. The review and subsequent report, documented good practices and lessons learned and illustrated how, over the last six years since its introduction, the MNR has become integral to support the building of coordinated, comprehensive, and multistakeholder national responses.[210]

Collectively, these diverse legal frameworks, along with the targeted global initiatives, signify a heightened awareness and acknowledgment of online child sexual abuse and exploitation. Moreover, these global and regional legal agreements underscore a growing commitment to undertaking united and coordinated action in response to the escalating challenges posed by these growing harms.

---

208 WeProtect Global Alliance, Model National Response, *supra* note 137.

209 *Id.*

210 WeProtect Global Alliance, *Framing the future: How the Model National Response framework is supporting national efforts to end child sexual exploitation and abuse online*, May 2022, at https://www.unicef.org/media/121066/file/Framing%20the%20Future.pdf (last visited Jul. 24, 2023) (on file with the International Centre for Missing & Exploited Children).

Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography

While the Convention on the Rights of the Child[211] (CRC) aims to ensure a broad range of human rights for children – including civil, cultural, economic, political, and social rights[212] – there are Articles within the CRC and the CRC Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography[213] (Optional Protocol) that explicitly address child sexual exploitation. Article 34 of the CRC clearly states that preventive measures should be taken to address the sexual exploitation of children:

> States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall, in particular, take all appropriate national, bilateral and multilateral measures to prevent … [t]he exploitative use of children in pornographic performances and materials.

The Optional Protocol was adopted by the UN General Assembly and opened for signature on 25 May 2000, and entered into force on 18 January 2002. Specific to CSAM:

- Article 2 (c) defines "child pornography" as "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes."
- Article 3 (1) requires States Parties to criminalize acts and activities including "producing, distributing, disseminating, importing, exporting, offering, selling or possessing…child pornography", whether committed domestically or transnationally, on an individual or organized basis.
- Article 3 (4) addresses the liability of legal persons and encourages each State Party to establish such liability for offenses specific to CSAM. This article reflects the notion that a comprehensive approach requires industry involvement.
- Article 10 (1) addresses the need for international cooperation. As mentioned above, CSAM is readily distributed across borders. Without international cooperation, many offenders may evade apprehension.

---

211 Convention on the Rights of the Child, G.A. Res. 44/25, 61st plen. mtg., U.N. Doc. A / RES / 44 / 25 (Nov. 20, 1989), *entered into force* Sep. 2, 1992, https://www.ohchr.org/en/professionalinterest/pages/crc.aspx (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

212 *See*, UNICEF, *Convention on the Rights of the Child*, *at* http://www.unicef.org/crc/ (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

213 Optional Protocol, *supra* note 25.

Convention Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour

Recognizing the need to adopt new instruments to protect children from harmful labour practices, the ILO established the Convention Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour (ILO No. 182).[214] The Convention, known as the Worst Forms of Child Labour Convention, was adopted unanimously on 17 June 1999 by the International Labour Conference and opened for signature by ILO Members. It came into force on 19 November 2000. All 187 ILO Member states have ratified the Convention.[215]

States parties are dedicated to the immediate elimination of dangerous forms of child labor.[216] Convention No. 182 defines the worst forms of child labor as slavery, debt bondage, prostitution, pornography, forced recruitment of children for use in armed conflict, use of children in drug trafficking and other illicit activities, and all other work harmful or hazardous to the health, safety or morals of girls and boys under 18 years of age.[217]

- Article 1 requires that each ratifying Member take immediate and effective measures to secure the prohibition and elimination of the worst forms of child labor as a matter of urgency.
- Article 2 defines "child" as any person under the age of 18.
- Article 3 (b) includes in the definition of "the worst forms of child labour" the use, procuring or offering of a child for prostitution, for the production of pornography or for pornographic performances.
- Article 6 mandates that each Member design and implement programs of action to eliminate as a priority the worst forms of child labor in consultation with relevant government institutions and employers' and workers' organizations, taking into consideration the views of other concerned groups as appropriate.
- Article 7 (1) states that all necessary measures to ensure the effective implementation and enforcement of the provisions giving effect to this Convention including the provision and application of penal sanctions or, as appropriate, other sanctions should be undertaken by Member States.

---

214 Convention concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour (ILO 182), 1999 2000, at https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C182 *entered into force Nov. 19, 2000* (last visited Jun. 23, 2023) (on file with the International Centre for Missing & Exploited Children).

215 See Convention concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour (ILO 182): Chart of Ratifications, *at* https://www.ilo.org/dyn/normlex/en/f?p=1000:11300:0::NO:11300:P11300_INSTRUMENT_ID:312327 (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

216 European Commission, The Convention concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour (ILO 182), 1999 at https://ec.europa.eu/anti-trafficking/legislation-and-case-law-international-legislation-united-nations/convention-concerning-prohibition_en *entered into force Nov. 19, 2000* (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

217 International Labour Organization (ILO), *The worst forms of child labour*, *at* https://www.ilo.org/ipec/Campaignandadvocacy/Youthinaction/C182-Youth-orientated/worstforms/lang--en/index.htm (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

Convention on Cybercrime

Developments in technology have enabled cyber-criminals to be located in different jurisdictions (i.e., countries) from the victims who are affected by their criminal behavior. As a result, the Council of Europe established the Convention on Cybercrime[218] (Budapest Convention) with the goal of implementing a cooperative and uniform approach to the prosecution of cybercrime. The Budapest Convention opened for signature on 23 November 2001 and entered into force on 1 July 2004. It is open for signature by the Council of Europe member States and the non-member States that have participated in its elaboration, and for accession by other non-member States. Currently, 68 countries (45 member States and 23 non-member States) have ratified the Budapest Convention, and 2 other countries (1 member States and 1 non-member State) have signed, but not ratified it.[219]

Title 3 of the Convention on "Content-related Offences" is pertinent to the area of child sexual exploitation. Specifically, Article 9 deals with "offences related to child pornography":

- Article 9 (1) recommends each State Party make it a criminal offense to: produce child pornography for the purpose of its distribution through a computer system; offer or make available child pornography through a computer system; distribute or transmit child pornography through a computer system; procure child pornography through a computer system for oneself or for another person; and possess child pornography in a computer system or on a computer-data storage medium.
- Article 9 (2) recommends "child pornography" be defined to include "pornographic material that visually depicts…a minor engaged in sexually explicit conduct[,]…a person appearing to be a minor engaged in sexually explicit conduct[, or]…realistic images representing a minor engaged in sexually explicit conduct."
- Article 9 (3) states that the term "minor' shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years."
- Article 11 requires States Parties to enact legislation necessary to address attempt crimes as well as aiding and abetting.
- Article 12 (1) addresses corporate liability.
- Article 13 (1) mandates States Parties adopt legislative measures to ensure that criminalized offenses "are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty."
- Article 23 addresses the issue of international cooperation.

---

218 Convention on Cybercrime (CETS 185), *supra* note 151.

219 See, Convention on Cybercrime (CETS 185): Chart of Signatures and Ratifications, at http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (last visited Jun. 23, 2023) (on file with the International Centre for Missing & Exploited Children).

Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse

The Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[220] (Lanzarote Convention) focuses on ensuring the best interests of children through the prevention of abuse and exploitation, providing protection and assistance for victims, punishing offenders, and promoting national and international law enforcement cooperation. The Lanzarote Convention was opened for signature on 25 October 2007 and entered into force on 1 July 2010. The Lanzarote Convention is open for signature by member States, non-member States that have participated in the Convention's elaboration, and by the European Community, and for accession by other non-member States. Currently, 46 Member States and 2 Non-member States have ratified the Lanzarote Convention.[221]

With regard to CSAM:

- Article 20 (1) requires States Parties to criminalize: producing child pornography; offering or making available child pornography; distributing or transmitting child pornography; procuring child pornography for oneself or for another person; possessing child pornography; and knowingly obtaining access, through information and communication technologies, to child pornography.
- Article 20 (2) defines "child pornography" as "any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes."
- Article 21 (1) recommends States Parties adopt legislation criminalizing the activities of those who recruit or coerce a child into participating in pornographic performances or knowingly attending pornographic performances.
- Article 23 defines the solicitation of children for sexual purposes (grooming) through information and communication technologies, and requires States Parties to take necessary measures to criminalize the conduct.
- Article 24 addresses attempt crimes as well as aiding and abetting.
- Article 26 addresses the issue of corporate responsibility.
- Article 38 addresses the general principles and measures for international cooperation.

220 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201), *supra* note 119.

221 See, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201): Chart of Signatures and Ratifications, at http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201/signatures (last visited Jun. 23, 2023) (on file with the International Centre for Missing & Exploited Children).

EU Directive on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography

On 13 December 2011, the European Parliament and the Council of the EU adopted Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, which replaced Council Framework Decision 2004/68/JHA.[222] The Directive improves and updates the 2010 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

The Directive harmonizes the definition of a number of criminal offenses such as child sexual abuse, sexual exploitation, child pornography, and grooming, and increases the applicable minimum penalties. The Directive also acknowledges the role of the internet and new technologies in the spread of child sexual exploitation. With this acknowledgment, the Directive requires Member States to take necessary measures to prevent the use of the Internet for child sexual abuse, exploitation, or the dissemination of child pornography.[223]

The Directive describes measures that may be taken to identify and treat those who would become offenders[224] or recidivists,[225] and prevent offenders from maintaining professions involving regular contact with children.[226] Moreover, the Directive also introduces provisions to protect the child victim during investigations and legal proceedings.[227] Furthermore, it encourages enhanced cooperation between Member States and non-Member States to ensure the removal of CSAM from servers in non-Member States,[228] along with tackling child sex tourism.[229]

The Directive entered into force upon publication on 13 December 2011. To be in compliance, Member States that ratified the Directive were required to bring into force the necessary laws, regulations, and administrative provisions by 18 December 2013. At the time of publication. 26 Member States had taken steps to implement this Directive under their national law.[230]

With regard to the text of the Directive itself, CSAM is addressed in the following articles:

- Article 2 (c) defines "child pornography" as "(i) any material that visually depicts a child engaged in real or simulated sexually explicit conduct; (ii) any depiction of the sexual organs of a child for primarily sexual purposes; (iii) any material that visually

---

222 Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, *supra* note 190.

223 *Id.* at paragraphs 3 and 12, and Articles 6 and 25.

224 *Id.* at Article 22.

225 *Id.* at Article 24.

226 *Id.* at Article 10.

227 *Id.* at Article 20.

228 *Id.* at paragraph 46.

229 *Id.* at paragraph 29.

230 National Implementing Measures, *supra* note 191. Denmark did not take part in the adoption of the Directive, thus is not bound by or subject to its application. See Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, *supra* note 190, at paragraph 52.

depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; or (iv) realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes."

- Article 2 (e) defines "pornographic performance" as "a live exhibition aimed at an audience, including by means of information and communication technology, of: (i) a child engaged in real or simulated sexually explicit conduct; or (ii) the sexual organs of a child for primarily sexual purposes."
- Article 4, paragraphs 2-4, states that "Member States shall take the necessary measures to ensure" that the following intentional conduct is punished: causing or recruiting a child to participate in pornographic performances; profiting from or otherwise exploiting a child for such purposes; coercing or forcing a child to participate in pornographic performances; threatening a child for such purposes; or knowingly attending pornographic performances involving the participation of a child.
- Article 5, paragraphs 2-6, states that "Member States shall take the necessary measures to ensure" that the following intentional conduct is punished: acquiring or possessing child pornography; knowingly obtaining access to child pornography by means of information and communication technology; distributing, disseminating or transmitting child pornography; offering, supplying or making available child pornography; and producing child pornography.
- Article 6, paragraph 2, states that "Member States shall take the necessary measures to ensure" that the following intentional conduct is punished: the solicitation of a child, through the use of information and communication technology, by an adult seeking to acquire pornography depicting the child.
- Article 7 addresses attempt crimes as well as incitement and aiding and abetting.
- Article 9 describes aggravating circumstances for sentencing purposes.
- Article 11 recommends that Member States take the necessary measures to seize and confiscate instrumentalities and proceeds from the offenses of child sexual abuse and sexual exploitation.
- Article 12 addresses the liability of legal persons and encourages each State Party to establish such liability for offenses specific to child sexual abuse and sexual exploitation.
- Article 14 ensures that child victims of sexual abuse and sexual exploitation are not prosecuted or penalized for their involvement in criminal activities.
- Article 15 provides recommendations regarding the investigation and prosecution of offenses.
- Articles 18 and 19 describe provisions for assistance, support, and protection measures for child victims.
- Articles 22, 23, and 24 discuss intervention and prevention programs and measures.
- Article 25 describes measures that should be taken regarding websites that contain or disseminate child pornography.

EU ePrivacy Directive

The EU established Directive 2002/58/EC (the ePrivacy Directive) to address privacy protection and the processing of personal data.[231] The Directive was amended in 2009 and replaced with Directive 2009/136/EC, which addressed electronic tagging and requirements for data breach notifications and strengthened enforcement of the Directive.[232]

Directive 2009/136/EC focuses on the privacy and confidentiality of online communications, and the rules of tracking and monitoring. The Directive addresses the confidentiality of communications that take place in public networks, as well as where the responsibility lies in cases where harmful or unlawful content is shared or discussed online.

With regard to child protection and CSAM:

- Article 20 describes the right of Member States to require user contracts when subscribing to public networks that address the use of electronic communications for unlawful activities and dissemination of harmful content.
- Article 26 addresses providing information to the public on unlawful uses, dissemination of harmful content, and the availability of accessible software that protects children.
- Article 30 states that providers do not hold responsibility for monitoring communication or pursuing action against unlawful uses.
- Article 31 states that Member States, not providers, are responsible for deeming content unlawful.

The ePrivacy Regulation is a proposed EU regulation aimed at updating and replacing the existing ePrivacy Directive (Directive 2002/58/EC). The ePrivacy Regulation aims to address modern challenges related to privacy and electronic communications in the digital age. The objectives of the ePrivacy Regulation are to enhance the protection of privacy in electronic communications, adapt the rules to new technological developments, and harmonize regulations across EU member states. It also imposes stricter rules on companies that collect or process this data. The ePrivacy Regulation applies to all electronic communications services and networks accessible by the public and that provide publicly available electronic communications services, including social media platforms, email, instant messaging, and Voice over IP (VoIP) calls. It will also cover cookies and other tracking technologies used by websites and apps.[233]

The ePrivacy Regulation has been in the legislative process for several years and has faced many delays and revisions. Implementation of the ePrivacy Regulation is not expected before the latter part of 2023, and there is a provision for a 24-month transition period.[234]

---

231 European Data Protection Supervisor, *ePrivacy Directive*, at https://edps.europa.eu/data-protection/data-protection/glossary/e_en#e-privacy_directive2009-136-ec (last visited Jul. 11, 2023) (on file with the International Centre for Missing & Exploited Children).

232 *Id.*

233 Secure Privacy, *EU's ePrivacy Regulation: 2022 Updates*, Nov. 2, 2022, at https://secureprivacy.ai/blog/eu-eprivacy-regulation-2022-updates (last visited Jul. 11, 2023) (on file with the International Centre for Missing & Exploited Children).

234 *Id.*

African Charter on the Rights and Welfare of the Child

The African Charter on the Rights and Welfare of the Child[235] (African Charter) was introduced to promote and protect the rights of children on the African continent. The African Charter focuses on ensuring the best interests of children through the prevention of abuse and exploitation, protection and assistance for victims, punishment of offenders, and promotion of national and international law enforcement cooperation.

The African Charter was adopted 1 July 1990 by the Assembly of Heads of State and Government of the Organization of African Unity and entered into force on 29 November 1999. The African Charter is open for signature by Member States of the African Union. As of 14 February 2023, Currently, 50 countries have ratified the African Charter, and 4 other countries have signed, but not ratified.[236]

With regard to CSAM:

- Article 16 requires State Parties to take specific legislative, administrative, social and educational measures to protect children from all forms of torture, inhuman or degrading treatment and especially physical or mental injury or abuse, neglect or maltreatment including sexual abuse.
- Article 27 (1) requires State Parties to undertake to protect children from all forms of sexual exploitation and sexual abuse and take measures to prevent:

    (a) the inducement, coercion or encouragement of a child to engage in any sexual activity;
    (b) the use of children in prostitution or other sexual practices;
    (c) the use of children in pornographic activities, performances and materials.

[235] African Charter on the Rights and Welfare of the Child, 1990, *supra* note 193.

[236] See, African Charter on the Rights and Welfare of the Child: Ratification Table, at https://au.int/sites/default/files/treaties/36804-sl-AFRICAN_CHARTER_ON_THE_RIGHTS_AND_WELFARE_OF_THE_CHILD.pdf (last visited Jun. 23, 2023) (on file with the International Centre for Missing & Exploited Children).

African Union Convention on Cyber Security and Personal Data Protection

The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) focuses primarily on addressing the challenges posed by criminal activities committed through the use of ICTs.[237] The Malabo Convention seeks to establish in each State Party a modern mechanism capable of combating violations of privacy resulting from personal data collection, processing, transmission, storage, and use.[238] The Malabo Convention aims to strengthen and harmonize existing cybersecurity legislation to repress cybercrime in Member States.[239]

The Malabo Convention was adopted on 27 June 2014 and has not yet entered into force.[240] The Convention is open for signature by Member States of the African Union. Currently, 14 countries have ratified the African Union Convention, and 12 other countries have signed, but not yet ratified it.[241]

With regard to CSAM:

- Article 1 defines "child pornography" as any visual depiction, including photograph, film, video, image, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where:
  - (a) the production of such visual depiction involves a minor;
  - (b) such visual depiction is a digital image, computer image, or computer-generated image where a minor is engaging in sexually explicit conduct or when images of their sexual organs are produced or used for primarily sexual purposes and exploited with or without the child's knowledge;
  - (c) such visual depiction has been created, adapted, or modified to appear that a minor is engaging in sexually explicit conduct.
- Article 29 (3) (1) requires State Parties to take the necessary legislative and/or regulatory measures to make it a criminal offense to:
  - (a) Produce, register, offer, manufacture, make available, disseminate, and transmit an image or a representation of child pornography through a computer system;
  - (b) Procure for oneself or for another person, import or have imported, and export or have exported an image or representation of child pornography through a computer system;

---

237 Nikoleta Lydaki Simantiri, *Online Child Sexual Abuse and Exploitation: Current forms and good practice for prevention and protection* 55, ECPAT, Jun. 2017, at http://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2017/09/revue-SECO_EN-interactif.pdf (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

238 *Id.*

239 African Union Convention on Cyber Security and Personal Data Protection, 2014, *supra* note 194.

240 See, African Union Convention on Cyber Security and Personal Data Protection: Ratification Table, at https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf (last visited Jun. 23, 2023) (on file with the International Centre for Missing & Exploited Children).

241 *Id.*

(c) Possess an image or representation of child pornography in a computer system or on a computer data storage medium;
(d) Facilitate or provide access to images, documents, sound or representation of a pornographic nature to a minor.

- Article 29 (3) (2) states that State Parties shall take the necessary legislative and/or regulatory measures to make the offenses provided for under the Convention criminal offenses.
- Article 29 (3) (3) addresses confiscation of materials, equipment, instruments, computer programs, and all other devices or data used to commit the offenses provided for in the Malabo Convention.
- Article 30 (2) addresses the liability of legal persons.
- Article 31 calls upon State Parties to ensure the offenses under the Malabo Convention are punishable by effective, proportionate, and dissuasive criminal penalties.

Arab Convention on Combating Information Technology Offences

The League of Arab States' Arab Convention on Combating Information Technology Offences (Arab Convention) was developed to encourage cooperation between Arab countries to adopt a common policy to protect Arab society against information technology offenses.[242] The Arab Convention aims to combat technology offenses to ensure the safety of individuals and communities. The Arab Convention was adopted on 21 December 2010 and came into force in February 2014.

The Arab Convention is open for signature by all 21 Member States of the League of Arab States. Currently, Since 2014, 7 Arab States had ratified the Arab Convention, and 18 others had signed.[243]

With regard to CSAM:

- Article 5 requires State Parties to commit to the criminalization of the acts set forth in the Arab Convention.
- Article 12 details the "offences of pornography" that should be criminalized to include the production, display, distribution, provision, publication, purchase, sale, import of pornographic material through information technology. It further provides an aggravated penalty for offenses related to CSAM. The aggravated penalty is also applicable for acquiring CSAM through information technology or a storage medium for such technology.
- Article 13 makes note of "other offenses related to pornography" including gambling and sexual exploitation without further detail.
- Article 20 addresses criminal responsibility of natural and juridical persons.

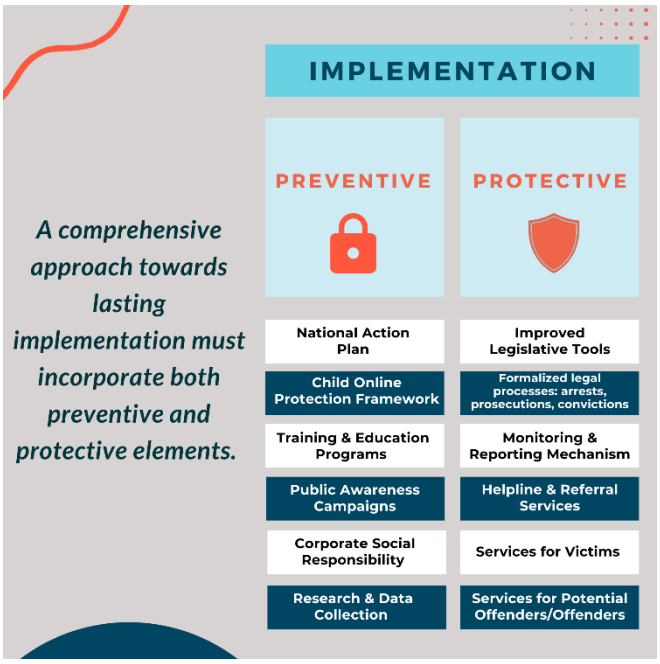
---

242 League of Arab States, *Arab Convention on Combating Information Technology Offences* (Arab Convention), 2010, *supra* note 195. See also, Joyce Hakmeh, *Cybercrime and the Digital Economy in the GCC Countries* 11-12, Chatham House, Jun. 2017, at https://www.chathamhouse.org/sites/default/files/publications/research/2017-06-30-cybercrime-digital-economy-gcc-hakmeh.pdf (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

243 UN Economic and Social Commission for Western Asia, *Policy Recommendations on Cybersafety and Combating Cybercrime in the Arab Region: Summary*, 2015, at https://www.unescwa.org/sites/www.unescwa.org/files/uploads/policy-recommendations-cybersafety-arab-region-summary-english.pdf (last visited Jul. 26, 2023).

Implementation

Over the past 17 years, there has been significant legislative change as more countries have developed laws to protect children from sexual abuse and exploitation with a focus on CSAM. As the number of countries with relevant legislation steadily grows, increasingly two questions are asked – are the countries with laws in place actually enforcing them, and are the penalties that are provided sufficient to act as a deterrent? It is crucial that countries not only enact child protection legislation, but that concerted and comprehensive cross-sectoral efforts are made to ensure the laws are supported, implemented, and enforced.



Enforcement can include not only the application of civil and criminal penalties for certain conduct articulated in the law (i.e., arrests, prosecutions, and convictions) but can also encompass various other actions that embody a more comprehensive framework and promote/support legislative provisions. Together, these measures can serve as important building blocks, enabling a country to frame child protection as a national priority and drive legislation towards effective and lasting implementation. Effectively assessing the status of countries' implementation processes can be difficult, particularly as many countries either do not possess or collect data, and/or information is not widely available in the public domain.

Consistent with the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, a comprehensive approach to implementation must incorporate both preventive and protective elements.[244]

Preventive and protective measures that may demonstrate a country's willingness to address CSAM through more than legislative action include (1) investigations, arrests, prosecutions, and convictions; (2) a national strategy/action plan; (3) reporting mechanisms; (4) awareness building campaigns; (5) capacity building programs; (6) provision of services for victims; and (7) research and data collection.[245]

---

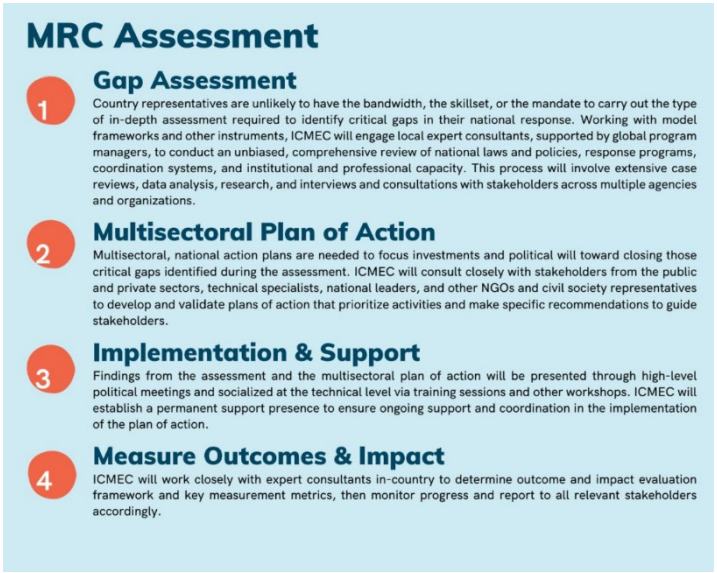
244 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201), *supra* note 119, at Chapters II and IV.

245 International Centre for Missing & Exploited Children, *Framing Implementation – A Supplement to Child Pornography: Model Legislation & Global Review*, 8th *Edition*, 2017, at https://www.icmec.org/wp-content/uploads/2017/02/Framing-Implementation_2017.pdf (last visited Jul. 26, 2023) (on file with the International Centre for Missing & Exploited Children).

With a view to assisting countries in identifying and addressing the challenges they face to fully implement child protection legislation, in 2020, ICMEC developed a rigorous, evidence-based methodology – the Multisectoral Response and Capacity Assessment (MRC) – using the capacities of the WeProtect MNR[246] as a foundation.[247] ICMEC began work at the national level, coordinating with countries to assess their responses and capacities for the prevention, attention, and investigation of online child sexual exploitation and abuse cases. ICMEC's MRC Assessment helps identify gaps that exist in a national response, highlights the progress that has been made, and provides corresponding recommendations and tailored guidance to strengthen and build capacities.

The analysis methodology of the MRC Assessment provides guidance and support to countries and organizations to fulfill their commitment to prevent and mitigate child sexual exploitation and abuse and requires the participation of various actors to ensure a comprehensive national response. The methodology includes (1) virtual and physical forms and interviews – conducted directly with officials from each institution – to identify and evaluate the capacities of an entity according to their responsibilities; (2) specific requests for information to an entity through video calls and e-mails; (3) searching for information in open sources; and (4) open-source data collection and analysis to complement the information collected. Upon completion of the assessment, a series of findings are generated with concrete suggestions for improvements that can be made through effective coordination between different sectors, including the government and its agencies, and other entities involved in the protection of children.

ICMEC's MRC Assessment provides a comprehensive roadmap for countries that seek to fully implement existing legislation and improve their response to online child sexual exploitation.



Effective implementation is fostered by cross-border and cross-sectoral collaboration and partnerships. This alliance amongst stakeholders helps to maximize resources, avoid duplication of efforts, facilitate the exchange of information, and aid in the swift identification of child victims and the offenders who harm them. Of course, all of these efforts must be tailored to a country's political, social, cultural, religious, and economic dynamics, while taking into account unique factors in its history and development. When aligned, these factors can serve as important motivators for a country to frame child protection as a national priority and drive legislation toward effective and lasting implementation.

---

246 WeProtect Global Alliance, *Model National Response*, *supra* note 137, at 2.

247 *Multisectoral Response and Capacity Assessments*, International Centre for Missing & Exploited Children, *at* https://www.icmec.org/assessments/ (last visited Sep. 27, 2023).

Global Legislative Review

✓ = Yes | ✗ = No

Country	Legislation Specific to CSAM[248]	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses[249]	Simple Possession[250]	ISP Reporting[251]
Afghanistan	✓	✗	✓	✓	✗
Albania	✓	✓	✓[252]	✓	✗
Algeria	✓	✓	✓[253]	✓	✗
Andorra	✓	✓	✓	✓	✗
Angola	✓	✓	✓	✓	✗

[248] For the purposes of this report, we were looking for specific laws that proscribe and/or penalize CSAM offenses. Mere labor legislation that simply bans the "worst forms of child labor," among which is CSAM, is not considered "legislation specific to child sexual abuse material." Further, countries in which there is a general ban on pornography, regardless of whether the individuals being depicted are adults or children, are not considered to have "legislation specific to child sexual abuse material," unless there is a sentencing enhancement provided for offenses committed against a child victim.

[249] In order to qualify as a technology-facilitated offense, we were looking for specific mention of a computer, computer system, Internet, ICT, or similar language (even if such mention is of a "computer image" or something similar in the definition of "child sexual abuse material"). In cases where other language is used in national legislation, an explanatory footnote is provided.

[250] "Simple possession," for the purposes of this report, refers to knowing possession regardless of the intent to distribute.

[251] While some countries may have general reporting laws (i.e., anyone with knowledge of any crime must report the crime to the appropriate authorities), only those countries that specifically require ISPs to report suspected CSAM to law enforcement (or another mandated agency) are included as having ISP reporting laws. Note that there are also provisions in some national laws (mostly within the European Union) that limit ISP liability as long as an ISP removes illegal content once it learns of its presence; however, such legislation is not included in this section.

[252] Article 117 of the Criminal Code of Albania states that the production, distribution, advertisement, export, import, sale, and publication of pornographic materials in environments with children, **by any means or form**, shall constitute criminal contravention and shall be punishable by imprisonment of up to two years. *Emphasis added.*

[253] Article 333 bis 1 of the Penal Code of Algeria imposes a criminal penalty for anyone who represents, **by any means whatsoever**, a person under eighteen (18) years engaged in explicit sexual activities, real or simulated, or represents the sexual organs of a minor, for primarily sexual purposes, or is involved in the production, distribution, dissemination, propagation, import, export, offer, sale or possession of pornographic material featuring minors. *Emphasis added.*

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Antigua & Barbuda	✓	✓	✓	✓	✗
Argentina	✓	✓	✓[254]	✓	✗
Armenia	✓	✓	✓	✓	✗
Aruba	✓	✓	✓	✓	✗
Australia	✓	✓	✓	✓	✓
Austria	✓	✓	✓	✓	✗[255]
Azerbaijan	✓	✓	✗	✓	✗
Bahamas	✓	✓	✓	✓	✓
Bahrain	✓	✓[256]	✓	✓	✗[257]

[254] Article 128 of Penal Code of Argentina punishes anyone who "produces, finances, offers, sells, publishes, facilitates, discloses or distributes, **by any means**, any representation of a child under eighteen (18) years engaged in explicit sexual activities…." *Emphasis added.*

[255] The Austrian legislation foresees the need for mandatory deletion of child pornography on the Internet on basis of paragraph 16 of the E-Commerce Law, paragraph 26 of the Austrian criminal code and paragraph 110 of the Austrian code of criminal procedure. Paragraph 16 of the E-Commerce Law obligates host providers, as soon as they have knowledge about unlawful content, to immediately delete said content and to block the access to said content respectively… For private persons there is no obligation to notify the police, therefore, internet service providers are not obligated to notify law enforcement or other institutions in case of suspicion of child pornography. Letter from Thomas Stölzl, Counselor, Embassy of Austria, Washington, D.C., to the International Centre for Missing & Exploited Children (Sep. 4, 2012) (on file with the International Centre for Missing & Exploited Children).

[256] Article 40 of Law No. 4 of 2021 Promulgating the Restorative Justice Law for Children and their Protection from Maltreatment states, "Sexual abuse means the exposure of the child to any sexual activity, including exposure to nudity, harassment, or penetration (vulvar or anal), or the exposure of the child to watch, use, produce or distribute pornographic films or pictures in any way."

[257] Although ISPs are not specifically mentioned, Article 44 of Law No. 4 of 2021 Promulgating the Restorative Justice Law for Children and their Protection from Maltreatment states that anyone who comes to knowledge that a child is facing one of the situations of endangerment mentioned in Article (40) (i.e., the exposure of the child to any sexual activity, including exposure to nudity, harassment, or penetration (vulvar or anal), or the exposure of the child to watch, use, produce or distribute pornographic films or pictures in any way) shall immediately notify any of the authorities stipulated in Article (45), and to provide them with any information they may have.

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Bangladesh	✓	✓	✓	✓	✗
Barbados	✓	✓	✓	✓	✗
Belarus	✓	✓	✓	✗[258]	✗
Belgium	✓	✓	✓	✓	✓[259]
Belize	✓	✓	✓	✓	✗
Benin	✓	✓	✓[260]	✓	✗
Bhutan	✓	✓	✓[261]	✓	✓

[258] [T]he Ministry of Internal Affairs [MVD] sent a letter to the state body of the Republic of Belarus with a proposal to set out a new version of Article 343-1 of the Criminal Code (the production and distribution of pornographic materials or objects of a pornographic nature with images of a child). On behalf of the Council of Ministers No. 33/14120r of 30.12.2022 with the objective of implementing the stated initiative of the MVD, with the direct participation of the professors of the teaching staff of the Academy of the MVD of the Republic of Belarus, has developed a structural form of Article 343-1 of the Criminal Code and prepared justifications for the need for criminal liability for collecting child pornography. As a result of the consideration of the project on Article 343-1 of the Criminal Code, the government organs submitted their position on the issue under consideration, of which the MVD has informed the Council of Ministers (*translated*). Email from Pavel Shidlovsky, Charge d'Affaires, a.i., Embassy of Belarus, Washington, D.C., to the International Centre for Missing & Exploited Children (Feb. 10, 2023) (on file with the International Centre for Missing & Exploited Children).

[259] Internet Service Providers are not required by Belgian law to actively monitor pre-emptively what is available on their servers. The Belgian law on electronic commerce however determines that when they are made aware of illegal content, they should immediately report it to the authorities and, whilst awaiting a decision there-of, they can block access to the content and remove it. Email from Paul Lambert, Counselor (political), Embassy of Belgium, Washington, D.C., to the International Centre for Missing & Exploited Children (Oct. 15, 2015) (on file with the International Centre for Missing & Exploited Children).

[260] Article 385 of the Children's Code of Benin criminalizes producing, distributing, importing, exporting, offering, selling possessing any material representing **by any means** a child engaged in explicit sexual activities, real or simulated, or representing a child's sexual organs. *Emphasis added.*

[261] According to Article 225(b) of the Penal Code of Bhutan, "[a] defendant shall be guilty of the defense of pedophilia if the defendant … sells, manufactures, distributes, or **otherwise deals** in material that contains any depiction of a child engaged in sexual contact." *Emphasis added.*

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Bolivia	✓	✓	✓[262]	✓	✗
Bosnia-Herzegovina	✓	✗	✓[263]	✓	✗
Botswana	✓	✓	✓	✓	✗
Brazil	✓	✓	✓	✓	✗[264]
Brunei Darussalam	✓	✓	✓	✓	✗[265]
Bulgaria	✓	✓	✓	✓	✗
Burkina Faso	✓	✓	✓	✓	✗

[262] Article 281 cuater of the Penal Code of Bolivia states that "whoever, by himself or through a third person, **by any means,**, promotes, produces, exhibits, commercializes or distributes pornographic material, or promotes obscene performances that involve children or adolescents, shall be punished with imprisonment of three (3) to six (6) years." *Emphasis added.*

[263] Article 211 of the Penal Code of the Federation of Bosnia and Herzegovina (amended 2016) references "**other pornographic materials**" in addition to photographs and audio-visual tapes. *Emphasis added.*

[264] The Children and Adolescents' Act criminally punishes those who provide means or services to disseminate photos or images of child pornography. Criminal punishment is required if those who provide means or services fail to interrupt the access to said photos or images upon being informed by the enforcement agencies that their means or services are being used to disseminate child pornography. In short, ISPs can be brought to justice if they disseminate child pornography and do not cooperate with enforcement agencies. Letter from Alexandre Ghisleni, Embassy of Brazil, Washington, D.C., to the International Centre for Missing & Exploited Children (May 13, 2009) (on file with the International Centre for Missing & Exploited Children).

[265] While there is no mandatory reporting requirement specific to ISPs, under the laws of Brunei all ISPs and Internet Content Providers (ICPs) licensed under the Broadcasting (Class License) Notification of 2001 must comply with the Code of Practice set forth in the Broadcasting Act (Cap 181). ISPs and ICPs are required to satisfy the Minister responsible for broadcasting matters that they have taken responsible steps to fulfill this requirement. Under the Broadcasting Act, such Minister has the power to impose sanctions. Content that should not be allowed includes, *inter alia*, that which depicts or propagates pedophilia. The Licensee must remove or prohibit the broadcast of the whole or any part of a program included in its service if the Minister informs the Licensee that the broadcast of the whole or part of the program is contrary to a Code of Practice applicable to the Licensee, or if the program is against the public's interest, public order, or national harmony, or offends against good taste or decency. The Licensee must also assist the Minister responsible for broadcasting matters in the investigation into any breach of its license or any alleged violation of any law committed by the Licensee or any other person; and shall also produce such information, records, documents, data, or other materials as may be required by the Minister for the purposes of the investigation. Email from Salmaya Salleh, Second Secretary, Embassy of Brunei, Washington, D.C., to the International Centre for Missing & Exploited Children (Mar. 21, 2006) (on file with the International Centre for Missing & Exploited Children).

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Burundi	✓	✗	✗	✗	✗
Cambodia	✓	✓	✓	✓	✗
Cameroon	✓	✓	✓	✓	✗
Canada	✓	✓	✓	✓	✓
Cape Verde	✓	✓	✓	✓	✗
Central African Republic	✓	✓	✗	✗	✗
Chad	✓	✓	✓[266]	✓	✗
Chile	✓	✓	✓	✓	✗

[266] Article 362 of the Penal Code 2017 of Chad criminalizes the production, distribution, importation, exportation, supply, making available, sale, obtaining or handing over to others, possession of any material, **by any means whatsoever**, of a child engaged in explicit sexual activities, real or simulated, or representing a child's sexual organs. *Emphasis added.*

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
China[267]	✓[268]	✗	✓	✓	✓[269]
Colombia	✓	✓	✓	✓	✓
Comoros	✓	✗	✓	✓	✓
Congo	✓	✓	✓[270]	✓	✗
Costa Rica	✓	✓	✓[271]	✓	✗

[267] CSAM legislation in Hong Kong differs from that in China.
Legislation in **Hong Kong**:
- defines CSAM;
- criminalizes technology-facilitated CSAM offenses; and
- criminalizes simple possession of CSAM.

Taiwan has legislation specific to CSAM that:
- defines CSAM;
- criminalizes technology-facilitated CSAM offenses;
- criminalizes simple possession of CSAM; and
- mandates ISPs to report CSAM.

Macau has legislation specific to CSAM and criminalizes technology-facilitated offenses ("in any capacity or by any means") but has not yet fulfilled the remaining criteria.

[268] Article 367 stipulates the definition of "obscene articles", i.e., sex-propagating books, periodicals, films, video- and audio-tapes, pictures and other obscene articles which concretely describe sexual acts or openly publicize sex. Given that the above provisions in the Criminal Law of China include child pornography, there is no separate law or definition exclusively on child pornography. That said, it is important to note that child pornography is covered by China's criminal legislation and relevant crimes are subject to severe punishment. Letter from HU Binchen, Police Counselor, Police Liaison Office, Embassy of the People's Republic of China, Washington D.C., to the International Centre for Missing & Exploited Children (Sep. 4, 2012) (on file with the International Centre for Missing & Exploited Children).

[269] Article 80 of the Law on the Protection of Minors 2020 specifies that where network service providers discover that users have used their network services to carry out illegal or criminal conduct against minors, they shall immediately stop providing the network services to the user, store relevant records, and report to the public security organs.

[270] Article 66 of the Law on the Protection of the Child of the Republic of Congo (Law No. 4-2010) states that no person shall manufacture, distribute, disseminate, import, operate, supply, sell, or have possession of any material **by any means whatsoever** representing a child engaged in explicit, actual, or simulated sexual activities or representative of the sexual organs of a child. *Emphasis added.*

[271] Article 174 of the Costa Rican Penal Code imposes a penalty on anyone who "exhibits, disseminates, distributes, finances or commercializes, **by any means**..., pornographic material in which minors appear, or possesses it for this purpose." *Emphasis added.*

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Côte d'Ivoire	✓	✓	✓	✓	✓
Croatia	✓	✓	✓	✓	✗
Cuba	✓	✗	✓[272]	✗	✗
Cyprus	✓	✓	✓	✓	✗[273]
Czech Republic	✓	✗	✓	✓	✗
Democratic Republic of Congo	✓	✓	✓[274]	✓	✗
Denmark	✓	✓	✓	✓	✗[275]

[272] Article 399 of the Cuban Penal Code of 2020 criminalizes producing, offering, trading, procuring, disseminating, or transmitting, **in any type of support or medium**, publications, images, recordings or other objects of a pornographic nature of persons under eighteen years of age.

[273] Law 91(I)/2014 of Cyprus "requires that when Internet Service Providers are made aware of such illegal content, they must block access to the content. Email from Constantinos Constantinou, Political Counsellor, Embassy of Cyprus to the United States of America, Washington, D.C., to the International Centre for Missing & Exploited Children (Jan. 23, 2023) (on file with the International Centre for Missing & Exploited Children).

[274] Section 174m of the Penal Code of the Democratic Republic of Congo criminalizes the production of "any representation **by any means whatever** of a child engaged in explicit sexual activity, real or simulated, or any representation of the sexual organs of a child. for primarily sexual purposes." *Emphasis added.*

[275] There is currently no Danish legislation that requires ISPs to report suspected child pornography to the Danish authorities. However, the Department of Justice has since 2005 implemented a model based on voluntary agreements and close cooperation with a majority of internet distributors to prevent access to a material of child pornographic nature via the internet. This effort is operationalized through so-called 'net-filters', which are established based on specific agreements between the authorities and the individual internet distributors. These agreements enable the Danish authorities to forward suspicious web addresses to the distributors and request that access to them is blocked. Email from Kristine Sorgenfri Hansen, Intern, Royal Danish Embassy, Washington, D.C., to the International Centre for Missing & Exploited Children (Aug. 30, 2012) (on file with the International Centre for Missing & Exploited Children).

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Djibouti	✓	✗	✓[276]	✗	✗
Dominica	✓	✓	✓	✓	✗
Dominican Republic	✓	✓	✓	✓	✗[277]
Ecuador	✓	✓	✓	✓	✗[278]
Egypt	✓	✗	✓	✓	✗
El Salvador	✓	✓	✓	✓	✗
Equatorial Guinea	✗[279]	✗	✗	✗	✗
Eritrea	✓	✗	✗	✗	✗

[276] Article 463(1) of the Penal Code of Djibouti criminalizes "the distribution, set[ting], sav[ing] or send[ing] of the image of a minor when the image is pornographic in nature…" including such images "broadcast **by any means whatsoever**…." *Emphasis added.*

[277] [T]he Embassy would like to provide a general overview of the most relevant provisions pertaining to the Dominican legal framework related to the obligation of reporting CSAM. For example, Law No. 136-03, that establishes the Code for the Protection of Fundamental Rights of Children, on its article 14 confirms the right to report abuses, stating that "professionals and officials in the areas of health, pedagogy, psychology, social work and public order agents, directors and officials, both public and private, and any other person who, in the performance of his duties or while off duty, has knowledge or suspicion of a situation of abuse or violation of the rights of boys, girls and adolescents, they are obliged to report it to the competent authorities." Moreover, Law No. 136-03, also article 238 affirms that, "anyone who has information or was the victim of a criminal act committed by an adolescent may denounce it before the Public Ministry of Boys, Girls and Adolescents, who will be empowered to initiate the investigation, except as previously stated for those cases that require the prior presentation of a private instance." Email from the Embassy of the Dominican Republic, Washington, D.C. to the International Centre for Missing & Exploited Children (Feb. 13, 2023) (on file with the International Centre for Missing & Exploited Children).

[278] Article 72 of the Code of Children and Adolescents of Ecuador requires that "People who, because of their profession or position, have knowledge of a fact/event that has characteristics of maltreatment, abuse, sexual exploitation, trafficking or the loss of a child victim, must report it within 24 hours after having this knowledge, to whatever competent prosecutor's office, judicial authority or administrative body, is the entity that upholds fundamental human rights."

[279] Equatorial Guinea passed its first Penal Code with Law No. 4/2022 (dated Aug. 17, 2022) which came into force in January 2023. The law reportedly addresses CSAM; however, the law was not available for review.

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Estonia	✓	✓[280]	✓[281]	✓	✓
Eswatini	✓	✓	✓	✓	✓
Ethiopia	✓	✗	✓	✓	✓
Fiji	✓	✓	✓	✓	✗
Finland	✓	✓	✓[282]	✓	✗
France	✓	✓	✓	✓	✓
Gabon	✓	✓	✓	✓	✗
Gambia, The	✓	✗	✓[283]	✗	✗

[280] According to the Supreme Court of Estonia ruling in Case number 1-16-5792, dated Nov. 9, 2017, "pornography is a form of representation that puts other human relationships aside or in the background, leaving sexual acts in the foreground vulgarly and intrusively." Furthermore, "[p]ornography and erotica can be distinguished on the basis of whether and how prominently sexuality is depicted in the work. As in the case of a work depicting a pornographic situation, the work with erotic content also predominantly depicts the erogenous part of the body related to sexuality, for example, the erogenous body of the person posing, but not vulgarly and obtrusively as in the work with pornographic content." See also, "The distinction between pornographic and erotic material is made based on the degree and the obtrusiveness of sexuality.... The pornographic situation holds any representations of the child either in actual or simulated sexual activities or depiction of a child's sexual organs for sexual purposes in an intrusive and obscene demeanour." *Sexual Exploitation of Children in Estonia Submission for the Universal Periodic Review of the Human Rights situation in Estonia,* Estonian Sexual Health Association and ECPAT International, Oct. 15, 2020, at https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=8471&file=EnglishTranslation#:~:text=53%20Unfortunately%2C%20Estonian%20legislation%20does,committed%20in%20an%20online%20environment (last visited Oct.1, 2023).

[281] Article 178 of the Estonian Penal Code criminalizes the "manufacture, acquisition or storing, handing over, displaying or making available to another person **in any other manner** of pictures, writings or other works or reproductions of works depicting a person of less than eighteen years of age in a pornographic situation, or a person of less than fourteen years of age in a pornographic or erotic situation." *Emphasis added.*

[282] Chapter 17, Section 18 of the Finnish Criminal Act criminalizes "a person who manufactures, offers for sale or for rent or **otherwise offers or makes available**, keeps available, exports, imports to or transports through Finland to another country, or **otherwise distributes** pictures or visual recordings that factually or realistically depict... a child, violence, or bestiality." *Emphasis added.*

[283] Article 144B of the Criminal Code (Amendment) Act, 2014 No. 11 of 2014 criminalizes "a person who produces or participates in the production of, trafficks, publishes, broadcasts, procures, imports, exports or **in any way** abets pornography depicting images of children." *Emphasis added.*

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Georgia	✓	✓	✓[284]	✓	✗[285]
Germany	✓	✓	✓	✓	✗[286]
Ghana	✓	✓	✓	✓	✓
Greece	✓	✓	✓	✓	✗
Grenada	✓	✓	✓	✓	✗
Guatemala	✓	✓	✓[287]	✓	✗
Guinea	✓	✓	✓	✓	✓
Guinea Bissau	✓	✗	✗	✗	✗
Guyana	✓	✓	✓	✓	✓

[284] The Note in Article 255 of the Criminal Code of Georgia specifies that "video or audio-visual material produced **by any method**,...that depicts the participation of minors or of characters with the appearance of a minor in the actual, simulated or computer-generated sexual scenes or displays genitalia of a minor..." shall be considered pornographic material. *Emphasis added.*

[285] In 2010 Memorandum of Understanding (MoU) was concluded between the Law Enforcement Agencies and Internet Service Providers (ISPs). Within the framework of MoU, ISPs undertake the obligation to cooperate and provide all relevant information to the law enforcement agencies for the purpose of investigation in accordance with Georgian legislation. Furthermore, this Memorandum is still open to all other future ISPs wishing to sign it. Email from Ms. Ketevan Sarajishvili, Legal Adviser, Public International Law Department, Ministry of Justice of Georgia, to the International Centre for Missing & Exploited Children (Oct. 24, 2015) (on file with the International Centre for Missing & Exploited Children).

[286] German legislation does not require Internet Service Providers (ISP) to report suspected child pornography or to retain digital user data. Instead, a specialized department of the Federal Criminal Police (BKA), the Central Unit for Random Internet Searches (ZaRD), scans the internet systematically in an effort to track down perpetrators and enforce prosecution. Letter from Holger Scherf, Consul General and Legal Adviser, Embassy of the Federal Republic of Germany, Washington, D.C., to the International Centre for Missing & Exploited Children (Nov. 11, 2015) (on file with the International Centre for Missing & Exploited Children).

[287] Article 193 ter of the Penal Code of Guatemala criminalizes "Whoever, **in any way and through any means**, produces, manufactures, or creates pornographic material that contains the real or simulated image or voice of one or more minors...." *Emphasis added.*

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Haiti	✓	✓	✓	✓	✗
Holy See	✓	✓	✓[288]	✓	✗[289]
Honduras	✓	✓	✓	✓	✗
Hungary	✓	✓	✓[290]	✓	✗[291]
Iceland	✓	✓	✓	✓	✗
India	✓	✓	✓	✓	✓
Indonesia	✓[292]	✗	✓[293]	✓	✗

[288] Article 10 of Law N. VIII: Supplementary Norms on Criminal Law Matters of 2013 of the Vatican City State criminalizes anyone who "transmits, imports, exports, offers or sells child pornography, **through any means, even electronically...."** *Emphasis added.*

[289] The Holy See has no Internet Service Provider external to it and the navigation from the internal provider has filters which impede not only access to any sites related to child pornography, but also online distribution of pornographic material. Given that the Holy See's website is institutional, only those issues which are inherent to its mission...can be found there. Letter from Archbishop Pietro Sambi, Apostolic Nuncio, Apostolic Nunciature, United States of America, to the International Centre for Missing & Exploited Children (Jun. 5, 2006) (on file with the International Centre for Missing & Exploited Children).

[290] Article 369 of the Hungarian Criminal Code criminalizes "Any person who reproduces, transports, obtains, makes available **or otherwise distributes** pornographic images of a child." *Emphasis added.*

[291] The National Media and Information Communications Authority (NMHH) recently launched an Internet Hotline service which is a platform to report illegal or fraudulent activities, including pedophilia, online harassment, and child pornography. If NMHH receives such notification and the content is indeed illegal, the NMHH requires the service provider or the editor of the website to remove said content. Email from Anna Stumpf, Political Officer, Congressional Affairs, Embassy of the Republic of Hungary, Washington, D.C., to the International Centre for Missing & Exploited Children (Aug. 17, 2012) (on file with the International Centre for Missing & Exploited Children).

[292] Indonesia passed a new Penal Code – Law No. 1 of 2023 regarding Criminal Code, dated 2 January 2023, that is set to take effect in 2026.

[293] Article 1 of the Indonesian Anti-Pornography Law defines pornography as "a picture, sketch, illustration, photo, writing, sounds, sounds, moving images, animations, cartoons, conversations, gestures, **or other forms of message through various forms of communication media** and/or public performance, which contains obscenity or sexual exploitation...." Pornographic services are defined as "all types of pornographic services provided by individuals or corporations through live shows, cable television, television terrestrial, radio, telephone, **internet, and communication other electronics** ...." Article 4 criminalizes the production, duplication, dissemination, etc. of pornography that explicitly contains child pornography. Article 5 prohibits "downloading" child pornography which is further described as "to retrieve files from internet networks or other communication networks." *Emphasis added.*

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Iran	✓	✓ [294]	✓	✓	✗
Iraq	✗ [295]	✗	✗	✗	✗
Ireland	✓	✓	✓	✓	✗ [296]
Israel	✓	✗	✓ [297]	✓	✗
Italy	✓	✓	✓	✓	✓
Jamaica	✓	✓	✓	✓	✗
Japan	✓	✓	✓	✓	✗
Jordan	✓	✓	✓	✗	✗

294 Iran's 2019 Law on the Protection of Children and Adolescents does not use the term CSAM (or child pornography), rather it defines content that is "obscene" as "any content, whether audio or image, that represents the complete nudity of a woman or a man, in a real or unreal way, intercourse, a sexual act, or the human sexual organ."

295 Article (403) of the Iraqi Penal Code states that (Any person who produces, imports, publishes, possesses, obtains or translates a book, printed or other written material, drawing, picture, film, symbol or another thing that violates the public integrity or decency with intent to exploit or distribute such material shall be punished with imprisonment or a fine. The same penalty applies to any person who advertises such material or displays it in public or sells, hires, or offers it for sale or hire even though it is not in public or to any person who distributes or submits it for distribution by any means. If the offense is committed with intent to deprave, it is considered to be an aggravating circumstance. Email from the Ministry of Justice, Department of Human Rights, Embassy of the Republic of Iraq, Washington, D.C., to the International Centre for Missing & Exploited Children (Feb. 13, 2023) (on file with the International Centre for Missing & Exploited Children).

296 The research correctly states that Irish legislation does not require Internet Service Providers (ISPs) to report suspected child pornography to law enforcement or to some other mandated agency. The internet service providers in Ireland are not required to seek out illegal content on their networks. In line with the EU Ecommerce Directive (2000/31), the ISPs are 'mere conduits' and they are not required to police the content carried on their networks. Where illegal content is drawn to the notice of an ISP then the ISP takes content down. This is referred to as 'notice and takedown'. The mechanism that is used for dealing with notice and takedown is Hotline.ie. Hotline.ie is the confidential service for reporting illegal content in the internet in Ireland. It is operated by the Internet Service Providers Association of Ireland and it is funded by them and also by EU funding under the EU Safer Internet Programme. Email from Joe Gavin, Counsellor, Justice and Home Affairs, Embassy of Ireland, Washington, D.C., to the International Centre for Missing & Exploited Children (Oct. 29, 2015) (on file with the International Centre for Missing & Exploited Children).

297 Article 14 of the Penal Code of Israel criminalizes publishing "an obscene publication [that] includes the likeness of a minor." Article 34X of the Penal Code defines "publication" to include "computer material, or any other visual representation, as well as any audiovisual means capable of presenting words or ideas, whether alone or by any means."

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Kazakhstan	✓	✗	✗	✗	✗
Kenya	✓	✓	✓	✓	✗ [298]
Kiribati	✓	✓	✓	✓	✗
Kosovo	✓	✓	✓	✓	✗
Kuwait	✓	✗	✓	✗	✗
Kyrgyzstan	✓	✗	✗	✗	✗
Laos	✓	✗	✓	✓	✗
Latvia	✓	✓	✓ [299]	✓	✗ [300]

[298] Article 58 of Kenya's Computer and Cybercrimes Act, 2018, on Confidentiality and limitation of liability, provides that "a service provider shall not be subject to any civil or criminal liability, unless it is established that the service provider had actual notice, actual knowledge, or willful and malicious intent, and not merely through omission or failure to act, had thereby facilitated, aided or abetted the use by any person of any computer system controlled or managed by a service provider in connection with a contravention of this Act or any other written law."

[299] Article 166(2) of the Criminal Law of Latvia criminalizes "the downloading, acquisition, importation, production, public demonstration, advertising, or **other distribution** of such pornographic materials as relate or portray the sexual abuse of children." *Emphasis added.*

[300] The Law on Information Society Services, Section 11, obliges all the intermediaries (also internet service providers) to report immediately to monitoring agencies on all the illegal actions performed by service user or their information stored. Also Section 10, point 5 of the Law provides for the responsibility of the intermediary service provider, meaning that if someone has reported on illegal content on the platform of the service provider, the service provider should act (report, delete). If not, he will be co-responsible for the content. Email from Viktorija Boļšakova, Senior Expert of the Child and Family Policy Department, Ministry of Welfare of the Republic of Latvia, to the International Centre for Missing & Exploited Children (Aug. 8, 2018) (on file with the International Centre for Missing & Exploited Children).

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Lebanon	✓	✓	✓	✗	✗
Lesotho	✗	✗	✗	✗	✗
Liberia	✓	✗	✓[301]	✓	✗
Libya	✗	✗	✗	✗	✗
Liechtenstein	✓	✓	✓	✓	✗[302]
Lithuania	✓	✗	✓	✓	✗
Luxembourg	✓	✗	✓	✓	✗

[301] Article 18.16 of the Children's Law of Liberia 2011 criminalizes storing, keeping or distributing "**in any form or manner**…any content of indecent images of any child or depicting any form of illegal sexual activity against a child." *Emphasis added.*

[302] While there is no specific mention of ISP reporting in the Penal Code of Liechtenstein, the Children & Youth Act, in force since February 1, 2009, stipulates a notification requirement that applies to anyone learning of the endangerment of the welfare of a child or young person (Article 20 Children and Youth Act). Also, it is worth mentioning that Liechtenstein has a cooperation agreement with the Swiss Cybercrime Coordination Unit CYCO, a special unit of the Swiss Federal Police. According to that agreement, CYCO is in charge of monitoring also Liechtenstein's range of IP numbers. Letter from Claudia Fritsche, Ambassador, Embassy of Liechtenstein, Washington, D.C., to the International Centre for Missing & Exploited Children (Nov. 4, 2015) (on file with the International Centre for Missing & Exploited Children).

The Liechtenstein legislation foresees the mandatory deletion of child pornography. Article 16 of the E-Commerce Law in conjunction with paragraph 219 of the Criminal Code requires host providers to delete or block access to unlawful content such as child pornography as soon as they acquire knowledge of its existence. Letter from Kurt Jaeger, Ambassador, Embassy of Liechtenstein, Washington, D.C., to the International Centre for Missing & Exploited Children (Sep. 4, 2018) (on file with the International Centre for Missing & Exploited Children).

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Madagascar	✓	✓	✓[303]	✓	✗
Malawi	✓	✓	✓	✓	✓
Malaysia	✓	✓	✓[304]	✓	✗
Maldives	✓	✗	✗	✗	✗
Mali	✓	✗	✗	✗	✗
Malta	✓	✓	✓	✓	✗
Marshall Islands	✓	✗	✗	✗	✗
Mauritania	✓	✗	✓	✓	✗
Mauritius[305]	✓	✓	✓	✓	✗

[303] Article 346 of the Penal Code of Madagascar criminalizes the dissemination of pornographic images of a child "**by any means whatsoever**". *Emphasis added.*

[304] Article 5 of the Sexual Offences Against Children Act of 2017 defines child pornography as "any description, whether in visual, audio or written form or in a combination of visual, audio or written form, or **in any other manner"** of a child who is doing sexually explicit conduct. *Emphasis added.*

[305] Following the recommendations of the Committee on the Rights of the Child in 2006, Government has taken measures to prepare a Children's Bill that will incorporate the spirit of the Convention on the Rights of the Child, include all its main principles and obligations, and bring together the different pieces of legislation dealing with children under one single legislation… Provisions will be made therein to address web related offences where children are involved. Letter from S. Phokeer, Ambassador, Embassy of Mauritius, Washington, D.C., to the International Centre for Missing & Exploited Children (Nov. 9, 2018) (on file with the International Centre for Missing & Exploited Children).

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting
Mexico	✓	✓	✓	✓	✗
Micronesia	✗	✗	✗	✗	✗
Moldova	✓	✓	✓	✓	✓
Monaco	✓	✓	✓	✓	✗
Mongolia	✓	✓[306]	✓	✓	✗
Montenegro	✓	✓	✓	✓	✗[307]
Morocco	✓	✓	✓[308]	✓	✗[309]

306 Article 1.2 paragraph 4 of the Criminal Code of Mongolia states, "Definitions and norms specified in the laws of Mongolia and international treaties, which Mongolia has ratified in its laws and is party to, shall be adhered to in determination of terms and concepts of this law." Mongolia ratified the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography in 2003. The definition of "child pornography" in Article 2 of the Optional Protocol is, therefore, applicable under Mongolian law.

307 Montenegrin law does not require ISPs to report suspected child pornography to law enforcement agencies but relation between ISPs and law enforcement is regulated with some Protocol of understanding and supporting, not by law. Email from Marija Petrovic, Charge d' Affaires a.i., First Secretary, Embassy of Montenegro, Washington, D.C., to the International Centre for Missing & Exploited Children (Aug. 27, 2012) (on file with the International Centre for Missing & Exploited Children).

308 Article 503-2 of the Penal Code of Morocco (consolidated version as of 5 July 2018) criminalizes "caus[ing], incit[ing] or facilitat[ing] the exploitation of children under the age of eighteen in pornography of any kind, **by any means whatsoever**, of a real, simulated or perceived sexual act or of any representation of the sexual organ of a child for sexual purposes." *Emphasis added.*

309 While in Morocco there is no explicit provision on the legal responsibility of Internet Service Providers to report child pornography sites to the police, or of web hosts or telephone operators to share details of abusers, Morocco has taken some very strong steps to combat child pornography. I would like to turn your attention to the following:

- Article 17 of Law n°24-96 concerning post and telecommunications states that commercial exploitation of value-added services – the list of which is set by regulation upon proposal of the National Agency of Telecommunications Regulation (ANRT) – can be provided freely by any physical or moral person after filing a declaration of intention to open the service. This declaration should contain the following information: a) opening terms of service; b) the geographical coverage; c) access conditions; d) nature of the services provided; e) rates to be charged to users;
- Article 18 of the same law states that "…without prejudice to the criminal sanctions, if it appears, following the provision of the service mentioned in the declaration, that it affects the security or the public order or is contrary to moral and ethics, the competent authorities may immediately cancel the declaration."

Email from Hichame Dahane, Political Counselor, Embassy of the Kingdom of Morocco, Washington, D.C., to the International Centre for Missing & Exploited Children (Sep. 1, 2012) (on file with the International Centre for Missing & Exploited Children).

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Mozambique	✓	✗	✓[310]	✓	✓
Myanmar	✓	✓	✓	✗	✗
Namibia	✓	✗	✗[311]	✓	✗
Nauru	✓	✓	✓	✓	✓
Nepal	✓	✓	✓[312]	✓	✗
Netherlands	✓	✓	✓	✓	✗[313]
New Zealand	✓	✓	✓	✓	✗[314]
Nicaragua	✓	✓	✓	✓	✗

[310] Article 226 Penal Code 2015 of Mozambique makes it an offense to "possess, acquire distribute, import, export, display or assign, **in any capacity or by any means**" child pornography. *Emphasis added.*

[311] Namibia continues to refine the draft Cybercrime Bill (2019), which is expected to address CSAM (child pornography).

[312] Article 2(m) of The Act Relating to Children, 2075 (2018) defines "child pornography" as "an act to take or make video or picture of children showing their sex organ or making them participate involve in imaginary sexual activities, to demonstrate vulgar picture through newspaper, poster, print, movie **or other medium of communication,** and this term also includes activities of production, sale, import, export, collection or dissemination of such materials." *Emphasis added.*

[313] While there is no legal or contractual obligation for ISPs to report suspected child pornography to law enforcement, Netherlands-based ISPs do have a practice of reporting their findings of child pornography immediately to law enforcement and the ISPs remove the content from the concerned website. Further, on the request of law enforcement, ISPs hand over their logs concerning the website(s) under suspicion. Emails from Richard Gerding, Counselor for Police and Judicial Affairs, Royal Embassy of the Netherlands, Washington, D.C., to the International Centre for Missing & Exploited Children (Feb. 8, 2006) (on file with the International Centre for Missing & Exploited Children).

[314] New Zealand does not mandate ISPs to report suspected child pornography; however, in cooperation with ISPs, the Department of Internal Affairs is in the process of implementing a website filtering system, the Digital Child Exploitation Filtering System, to block access to known websites containing child sexual abuse images. While participation by ISPs is voluntary, the Department fully anticipates that most ISPs will join the initiative and that the vast majority of New Zealand Internet users will be subject to the Digital Child Exploitation Filtering System. Letter from His Excellency Roy Ferguson, Ambassador, Embassy of New Zealand, Washington, D.C., to the International Centre for Missing & Exploited Children (Dec. 11, 2009) (on file with the International Centre for Missing & Exploited Children).

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Niger	✓	✓	✓	✓	✗
Nigeria	✓	✓	✓	✓	✓
North Korea	✗	✗	✗	✗	✗
North Macedonia	✓	✓	✓	✓	✗
Norway	✓	✓	✓[315]	✓	✗
Oman	✓	✗	✓	✓	✗
Pakistan	✓	✓	✓	✓	✗
Palau	✓	✓	✓	✓	✗
Panama	✓	✓	✓	✓	✗[316]

[315] Article 311 of the Penal Code of Norway (*Depiction of sexual abuse of children or depiction which sexualises children*) states, "A penalty of a fine or imprisonment for a term not exceeding three years shall be applied to any person who... (b) publishes, offers, sells, supplies to another person, makes available **or otherwise seeks to disseminate** depictions as specified...." *Emphasis added.*

[316] The Criminal Code of Panama was amended by Law 21 of 2018, enacted on March 2018. This law modified certain articles related to crimes of Corruption of Minors and Sexual Commercial Exploitation. ***Article 189.*** *Anyone who has knowledge of the use of minors in the execution of any of the crimes contemplated in this Chapter, whether this knowledge has been obtained by reason of his/her office, position, business or profession, or by any other source and omits to report it to the competent authorities shall be punished with imprisonment from one to three years.* In virtue of the above, since the Internet Service Providers (ISP) can obtain knowledge of suspected child sexual abuse material through the internet due to its business, it is stated in the law that they must report this situation to our law enforcement authorities. Otherwise, they can be prosecuted without exceptions since the regulation is broad. Letter from Francisco Olivardia, Second Secretary, Embassy of Panama, Washington, D.C., to the International Centre for Missing & Exploited Children (Aug. 2, 2018) (on file with the International Centre for Missing & Exploited Children).

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Papua New Guinea	✓	✓	✓	✓	✗
Paraguay	✓	✓	✓[317]	✓	✗[318]
Peru	✓	✓	✓	✓	✗
Philippines	✓	✓	✓	✓	✓
Poland	✓	✓[319]	✓	✓	✗[320]
Portugal	✓	✓	✓[321]	✓	✓
Qatar	✓	✗	✓	✓	✓

317 Article 1 of Paraguayan Law Number 2.861/06 imposes sanctions on "whoever, **by any means**, produces, or reproduces" child pornography. *Emphasis added.*

318 Although ISPs are not specifically mentioned, Article 7 of Paraguayan Law Number 2.861/06 states that anyone who witnesses child pornography offenses is required to "report these offenses immediately to the Police or the Public Minister, provide, if held, the data for the location, seizure, and eventual destruction of the image, and for the identification, apprehension and punishment of the perpetrators. Anyone who fails to fulfill these obligations shall be sentenced to deprivation of liberty for up to three years or with a fine."

319 Interpretation of the term "child pornography" is based on the case law and a legal doctrine (e.g. a judgment of the Supreme Court of 23 November 2010, ref. IV KK 173/10; M. Mozgawa (edit.) M. Budyn-Kulik, Mr. Kozłowska-Kalisz, M. Kulik, Criminal Code: Reference, ed. Oficyna 2010). Letter from Maciej Pisarski, Charge d'affaires, Embassy of the Republic of Poland, Washington, D.C., to the International Centre for Missing & Exploited Children (Aug. 29, 2012) (on file with the International Centre for Missing & Exploited Children). In that case, the Supreme Court held that "pornographic content will include, whether in a recorded form (e.g. film, photos, magazines, books, paintings) or not (e.g. live shows), presentations of human sexual activities (especially showing sexual organs in their sexual functions)."

320 Internet Service Providers (ISPs) are not obliged to monitor the data which are transmitted, stored or made available by these entities (article 15 of *the Act of 18 July 2002 on Providing Services by Electronic Means*). It means ISPs are not required to verify if the data comply with the law. However, in case of having been informed or having received a message on unlawful nature of data or activity related to it, it immediately makes the access of the data impossible (article 14 of the abovementioned Act). Letter from Maciej Pisarski, Charge d'affaires, Embassy of the Republic of Poland, Washington, D.C., to the International Centre for Missing & Exploited Children (Aug. 29, 2012) (on file with the International Centre for Missing & Exploited Children).

321 Article 176 of the Penal Code of Portugal criminalizes the "use of a minor in pornographic photography, film or recording, to…produce, distribute, import, export, disclose, display or assign, under any title **or by any means.**" *Emphasis added.*

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Romania	✓	✓	✓	✓	✗ [322]
Russia	✓	✓	✓	✗	✗
Rwanda	✓	✗	✓	✗	✓
St. Kitts & Nevis	✓	✓	✓	✗	✗
St. Lucia	✓	✓	✓	✓	✗
St. Vincent & the Grenadines	✓	✓	✓	✓	✗
Samoa	✓	✓	✓	✓	✗
San Marino	✓	✓	✓	✗	✗
Sao Tome & Principe	✓	✗	✓ [323]	✓	✗

[322] There is no particular piece of legislation in Romania that requires ISPs to report suspected child pornography; however, there are several laws that require ISPs to report all suspected illegal activities to public authorities. Reports are given to the Ministry of Communications and Information Society, which can then decide what judicial steps need to be taken. Letter from Serban Brebenel, Third Secretary, Embassy of Romania, Washington, D.C., to the International Centre for Missing & Exploited Children (Dec. 4, 2009) (on file with the International Centre for Missing & Exploited Children).

[323] Article 180 of the Penal Code 2012 of Sao Tome & Principe criminalizes those who "produce, distribute, import, export, publish, display or give **in any capacity or any means**, photograph, film or pornographic recording representing a minor 14 years, **irrespective of the medium**...." *Emphasis added.*

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Saudi Arabia	✓	✗ [324]	✓	✓ [325]	✗ [326]
Senegal	✓	✓	✓	✓	✗
Serbia	✓	✓	✓ [327]	✓	✗
Seychelles	✓	✓	✓	✓	✗

[324] The Child Protection Law states in Article (12): It shall be prohibited to produce, publish, display, trade, and possess any printed, visual, or audio works targeting children and inciting them to engage in any behavior contrary to the provisions of Sharia, public order, or public decency, or works which may encourage delinquency. The Executive Regulations of Child Protection Law states in Article (1) - Item (9): that the Sexual Exploitation is: Child's exposure to prostitution performance or displays, or to any sexual practice that violate the Sharia or law, whether directly or indirectly, paid, or unpaid, and with or without the consent of the Child. The Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, to which the Kingdom acceded, states in Article (2) the definition of the Sale of Children, Child prostitution and Child pornography. Email from Political and Congressional Affairs Department, The Embassy of Saudi Arabia, Washington, D.C., to the International Centre for Missing & Exploited Children (Feb. 23, 2023) (on file with the International Centre for Missing & Exploited Children).

[325] The Child Protection Law states in Article (12): It shall be prohibited to produce, publish, display, trade, and possess any printed, visual, or audio works targeting children and inciting them to engage in any behavior contrary to the provisions of Sharia, public order, or public decency, or works which may encourage delinquency. The Anti-Cyber Crime Law states that any person who commits one of the following cybercrimes shall be subject to imprisonment for a period not exceeding five years and a fine not exceeding three million riyals or to either punishment: 1. Production, preparation, transmission, or storage of material impinging on public order, religious values, public morals, and privacy, through the information network or computers. The Islamic Law criminalizes spreading immorality and sexual content and it is a general crime including crimes related to the children, and the legislations stated that the punishment is Intensified if the victim is a child. Email from Political and Congressional Affairs Department, The Embassy of Saudi Arabia, Washington, D.C., to the International Centre for Missing & Exploited Children (Feb. 23, 2023) (on file with the International Centre for Missing & Exploited Children).

[326] In accordance with the Council of Ministers Resolution No. 229 dated 13/08/1425 H, the Communications and Information Technology Commission (CITC) is the official Saudi body that is charged with overseeing the internet service providers. It is also authorized to block electronic websites, which are found to be in violation of the Commission's regulations such as the ones that contain child pornography materials. The role of the CITC includes receiving reports by internet users in the Kingdom of websites containing child pornography materials and forcing service providers to block such websites; informing law enforcement in the Kingdom of any child pornography materials documented on the internet so as the appropriate legal measure may be taken; and receiving requests for blocking pornographic material and such websites and electronic pages that contain pornographic and child sexual exploitation materials through the following Commission's internet link: (http://internet.sa) and directing the service providers in the Kingdom to block such websites. Email from Hanouf T. Khallaf, Political Advisor, Office of Political and Congressional Affairs, Embassy of the Kingdom of Saudi Arabia, Washington, D.C., to the International Centre for Missing & Exploited Children (Sep. 28, 2018) (on file with the International Centre for Missing & Exploited Children).

[327] Article 185 of the Penal Code of Serbia criminalizes one who "**electronically or otherwise** makes accessible images, audio-visual or other objects of pornographic content created by the exploitation of a minor." *Emphasis added.*

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Sierra Leone	✓	✓	✓[328]	✓	✗
Singapore	✓	✓	✓	✓	✗
Slovak Republic	✓	✓	✓	✓	✗
Slovenia	✓	✗	✓	✓	✗[329]
Solomon Islands	✓	✓	✗	✓	✗
Somalia	✗	✗	✗	✗	✗
South Africa	✓	✓	✓	✓	✓
South Korea	✓	✓	✓	✓	✗[330]

[328] Section 1 of the Sexual Offences Act of Sierra Leone states that "child pornography" means – any photograph, film, video or **other visual representation** that shows a person who is or who is depicted as being under the age of 18 and is engaged in or is depicted as engaged in sexual activity." It further criminalizes anyone who "makes, produces, distributes, transmits, prints or publishes child pornography." *Emphasis added.*

[329] Article 280(1) of Criminal Code states: "Any person who is aware of preparation for a commission of an offence which is punishable by a prison sentence of at least three years and does not report this offence at a time it could be prevented, and the offence was attempted or committed, shall be punished by a prison sentence of up to one year." As the possession of child sexual abuse material is an offence punishable by a prison sentence of up to 8 years, the ISP are normally required to report the suspected cases involving such materials to the competent authorities. Email from Aljaž Zupan, Minister Plenipotentiary, The Embassy of the Republic of Slovenia, Washington, D.C., to the International Centre for Missing & Exploited Children (Feb. 15, 2023) (on file with the International Centre for Missing & Exploited Children).

[330] Korean legislation does not require ISPs to report suspected child pornography to law enforcement or to some other mandated agency. Recently the Korean National Assembly, however, amended "The Act on the protection of children and juveniles from sexual abuse" and added some provisions that require ISPs to take measures in order to find the child pornography on its network. And these amendments also require ISPs to erase and delete the child pornography immediately after the ISP finds it. Moreover, the ISP has to set up technical measures in order to prevent and stop the transmission or dissemination the child pornography. Email from Yun Kyu Park, Counselor, Broadcasting & Telecommunications, Embassy of the Republic of Korea, Washington, D.C., to the International Centre for Missing & Exploited Children (Aug. 30, 2012) (on file with the International Centre for Missing & Exploited Children).

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
South Sudan	✓	✗	✓	✗	✓
Spain	✓	✓	✓	✓	✗
Sri Lanka	✓	✗	✗	✓	✓
Sudan	✓	✓	✗	✓	✗
Suriname	✓	✓	✓	✓	✗
Sweden	✓	✓[331]	✓[332]	✓	✗[333]

[331] The definition for child pornography is articulated in the Preparatory Work and is referred to and applied by the courts in practice. In Chapter 16, Section 10a, of the Criminal Code there is a definition of the word *child*. There is no legal definition of *child pornography* in the legislation. Nevertheless, there are statements in the preparatory works to the effect that an image is to be regarded as pornographic when it, without any scientific or artistic values, depicts a sexual motif in an unconcealed and offensive way. Email from Magdalena Wikstrand Danelius, Legal Adviser, Division for Criminal Law, Ministry of Justice of Sweden, Washington, D.C., to the International Centre for Missing & Exploited Children (Nov. 18, 2011) (on file with the International Centre for Missing & Exploited Children).

Government Bill 1997/98: 43 Freedom of the Press Ordinance and Speech Constitution scopes - pornography issue, etc. p. 56 "The image should, according to common use of language and general values, be pornographic in its content for it to be considered criminal in court....By pornographic, according to the statement of grounds in this section, the image under investigation should not have scientific or artistic value. The image is clearly intended to arouse a sexual reaction (Bill 1970:125 P. 79 f.). It is not required that the image depicts a child engaged in sexual conduct in order for it to be covered by the law. The criminal area, which regulates whether an image is considered to be pornographic, also includes images which in any other way portray one or several children in a way that is likely to appeal to an individual's sex drive."*(translation)*

[332] Chapter 16 Section 10a of the Penal Code of Sweden criminalizes portraying a child in a pornographic nature, disseminating, transferring, granting use, exhibiting or **"in any other way"** making such a picture of a child available to some other person. *Emphasis added.*

[333] In Act (1998:112) on responsibility for Electronic Bulletin Boards (the BBS Act) there are rules that aim to prevent the spread of child pornography. A supplier of an electronic bulletin board is obliged to supervise the service to an extent that is reasonable considering the extent and objective of the service. The supplier is also obligated to remove a message, or in some other way make it inaccessible, if it is obvious that the content constitutes certain crimes, for example child pornography. A person who intentionally or by gross negligence, violates this obligation can be sentenced to a fine or to imprisonment for not more than six months, or, if the offence is grave, to imprisonment for not more than two years. It is also important to acknowledge the extensive preventive work that is carried out by the authorities. For example, there is an established and successful voluntary cooperation between the Police and the Internet Service Providers, which leads to the blocking of commercial Internet web sites that contain child pornography. Around 90 % of subscribers to the Internet in Sweden are covered in this voluntary cooperation. Email from Anne-Charlotte Merrell Wetterwik, Assistant to the Ambassador, Embassy of Sweden, Washington, D.C., to the International Centre for Missing & Exploited Children (Aug. 17, 2018) (on file with the International Centre for Missing & Exploited Children).

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Switzerland	✓	✓	✓	✓	✗ [334]
Syria	✗ [335]	✗	✗	✗	✗
Tajikistan	✓	✗	✓	✗	✗
Tanzania	✓	✓	✓	✗	✓
Thailand	✓	✓	✓	✓	✗
Timor Leste	✓	✓	✓ [336]	✓	✗
Togo	✓	✓	✓ [337]	✓	✓
Tonga	✓	✓	✓	✓	✗

[334] ISPs do not have a legal obligation to monitor and report suspected child pornography; however, Switzerland has created a special entity – the Cybercrime Coordination Unit Switzerland (CYCO) – where persons can report suspicious Internet subject matter. The Coordination Unit cooperates closely with ISP's and may, on a case to case basis, ask them to take appropriate measures to block respectively delete certain content. CYCO also actively searches for criminal subject matter on the Internet and is responsible for in-depth analysis of cybercrime. It is possible for the public to report child pornography cases to CYCO. Today about 80% of ISPs in Switzerland have agreements with CYCO. Letter from Urs Ziswiler, Ambassador, Embassy of Switzerland, Washington, D.C., to the International Centre for Missing & Exploited Children (Jan. 22, 2010) (on file with the International Centre for Missing & Exploited Children).

[335] In July 2021, Syria issued Law No. 21 of 2021, The Child Rights Law. Article 32 reads: **"**It is prohibited to produce, publish, display, circulate, promote, import, photograph, or copy visual, readable, or audio materials, means, or products, electronic or non-electronic, related to children if they harm him or encourage delinquent behavior." While it does not explicitly prohibit CSAM, it may be applied in such cases.

[336] Article 176 (1) of the Penal Code of Timor Leste criminalizes "Any person who, for predominantly sexual purposes, uses, exposes or represents a minor aged less than 17 years performing any sexual activity, whether real or stimulated, **or by any other means**, exhibits the sexual activity or sexual organs of a minor." *Emphasis added.*

[337] Article 392 of the Law No. 2007-017 of 6 July 2007 constituting the Children's Code of Togo states that "child pornography means, any representation, **by any means whatsoever,** of a child engaged in explicit sexual activities, real or simulated, or any representation of the sexual parts of a child, for primarily sexual purposes." *Emphasis added.*

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Trinidad & Tobago	✓	✓	✓	✓	✗
Tunisia	✓	✗	✓	✗	✗
Turkey	✓[338]	✗	✓	✓	✓
Turkmenistan	✓	✗	✗	✗	✗
Tuvalu	✗	✗	✗	✗	✗
Uganda	✓	✓	✓	✓	✓
Ukraine	✓	✓	✓	✓	✗
United Arab Emirates	✓	✓	✓	✓	✓

[338] While the Turkish Criminal Code does not use the terms "child pornography" or "child sexual abuse material", Article 226 (3) refers to the use of children in the production of obscene written or audio-visual materials. The General Criminal Assembly of the Supreme Court of Appeals, with its decision numbered 2015/66, expressed the use of children in the production of obscene products as follows: "The first sentence of the 3rd paragraph of Article 226 of the Turkish Penal Code, which also regulates the crime of obscenity against children, does not impose any restrictions on the formal conditions of obscene products or the way and purposes of production of these products. The obscene product here refers to visual or audio products such as pictures, films, videos, photographs, graphics, images, sculptures, cartoons, animations, and written products such as lyrics, novels, and stories, in which children are used as the obscene element." *See*, Av. Baran Doğan, *Obscenity Crime, Conditions and Punishment (TCK 226)*, at https://barandogan.av.tr/blog/ceza-hukuku/mustehcenlik-sucu-cezasi-nedir-tck.html (last visited Sep. 22, 2023).

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
United Kingdom[339]	✓	✓	✓	✓	✗[340]
United States	✓	✓	✓	✓	✓
Uruguay	✓	✓	✓[341]	✗	✗

[339] For the purposes of this report, the United Kingdom includes **England** and **Wales**.

In **Northern Ireland**, the Protection of Children (Northern Ireland) Order 1978, Section 3, criminalizes one who takes, permits to be taken, distributes, shows, possesses with a view to its distribution, or publishes an indecent photograph or pseudo-photograph of a child under the age of 18. The term "indecent photograph" includes film, a copy of an indecent photograph or film, and an indecent photograph comprised in a film. An "indecent pseudo-photograph" includes a copy of an indecent pseudo-photograph and data stored on a computer disc or by other electronic means which is capable of conversion. A "pseudo-photograph" means an image, whether produced by computer-graphics or otherwise, which appears to be a photograph. The Sexual Offences (Northern Ireland) Order 2008 addresses causing or inciting child prostitution or pornography (Art. 38), controlling a child involved in child prostitution or pornography (Art. 39), and arranging or facilitating child prostitution or pornography (Art. 40).

In **Scotland**, Section 52 of the Civic Government (Scotland) Act 1982 (amended), the law criminalizes one who takes, permits to be taken, distributes, shows, possesses with a view to its distribution, or publishes an indecent photograph or pseudo-photograph of a child under the age of 18. The term "indecent photograph" is not defined. A "pseudo-photograph" means an image, whether produced by computer-graphics or otherwise, which appears to be a photograph. Section 52A further criminalizes possession of indecent photographs or pseudo-photographs of children.

[340] The United Kingdom does not explicitly state that ISPs must report suspected child abuse images to law enforcement or to some mandated agency; however, ISPs may be held liable for third party content if it hosts or caches content on its servers and possession may possibly occur in the jurisdiction where the serve is located. In the United Kingdom, possession is an offense and as such ISPs will report suspected child abuse material to law enforcement once they are aware of it. Letter from Nick Lewis, Counselor, Embassy of Great Britain, Washington, D.C., to the International Centre for Missing & Exploited Children (Dec. 16, 2009) (on file with the International Centre for Missing & Exploited Children).

I can confirm that child pornography in the United Kingdom is covered by the Protection of Children Act 1978, which makes it illegal to take, make, distribute, show or possess an indecent photograph or pseudo-photograph of someone under the age of 18. In the context of digital media, saving an indecent image to a computer's hard drive is considered "making" the image, as it causes a copy to exist which did not exist before. This law is in force in England, Wales and Northern Ireland…The prohibition of content on the Internet, that is potentially illegal under this law by British internet service providers, is however self-regulatory, coordinate by the non-profit charity Internet Watch Foundation (who has partnerships with many major ISPs in the country). The IWF operates in informal partnership with the police, government, public and Internet service providers. Letter from James Eke, Foreign Policy and Security Group, British Embassy, Washington, D.C., to the International Centre for Missing & Exploited Children (Jul. 31, 2012) (on file with the International Centre for Missing & Exploited Children).

[341] Article 3 of Law 17.815 of 2004 of the Oriental Republic of Uruguay criminalizes "one that **in any way** facilitates…the marketing, dissemination, exhibition, import, export, distribution, offer, storage or acquisition of pornographic material that contains the image or any other representation of one or more minors." *Emphasis added.*

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Uzbekistan	✓	✓[342]	✓	✗	✗
Vanuatu	✓	✓	✓	✓	✗
Venezuela	✓	✓	✓	✗	✗
Vietnam	✓	✓[343]	✓	✗	✓
Yemen	✗	✗	✗	✗	✗
Zambia	✓	✓	✓	✓	✗
Zimbabwe	✓	✓	✓	✓	✓

[342] The Criminal Code of Uzbekistan was amended in December 2020, adding a definition for "**pornographic products**" in Paragraph 38 of Section III. A "pornographic product" is a pornographic work, as well as materials and objects, whether created with the help of computer technology, that have no artistic value and do not have a scientific, medical or educational purpose, containing a description, or photo, video, or other image of a person's genitals or an actual act person or simulated sexual intercourse. Article 130 criminalizes the production, import, distribution, advertising, and demonstration of "pornographic products with a description or image of a minor, or involvement of a minor as a performer in acts of a pornographic nature."

[343] While Vietnam's law does not use the terms child pornography or CSAM, Art. 147(1) of the Criminal Code of 2017 defines **"pornographic performance"** as "using gestures, actions, words, writing, symbols, pictures and sound to sexually stimulate a person under 16; exposing a reproductive organ or private part, completely or partially undressing or committing other acts that imitate sexual activities (including sexual intercourse, masturbation and other sexual activities) in any shape or form."

Conclusion

For nearly two decades, ICMEC's research on global anti-CSAM legislation has consistently revealed gradual yet steady progress. Numerous international and regional legal instruments are in place, effectively raising awareness and instilling a sense of urgency in addressing this critical issue. This heightened awareness has fueled a collective determination to find enduring solutions. In response to this determination, collaborative initiatives have emerged, uniting child protection professionals across various sectors who share a common objective: safeguarding children from sexual violence in all its forms. While numerous legislative improvements have been achieved, they represent just one component of a comprehensive response, albeit a crucial one.

To ensure a safer future for children worldwide, it is imperative that more countries take decisive action. The challenge of combatting CSAM domestically and internationally is formidable, but it can be surmounted through harmonized legal measures, technological innovations, and sustained collaborative efforts. Together, we can make the world safer for all children.

International Centre™
FOR MISSING & EXPLOITED CHILDREN

icmec.org @icmec_official /icmecofficial @ICMEC_official

2318 Mill Road, Suite 1010 Alexandria, Virginia 22314 USA