CHILD SEXUAL ABUSE MATERIAL:

Model Legislation & Global Review

9th Edition, 2018

International Centre
FOR MISSING & EXPLOITED CHILDREN

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

Child Sexual Abuse Material:
Model Legislation & Global Review

[This report was previously called *Child Pornography: Model Legislation & Global Review*]

Ninth Edition

This project was initially funded in part through Grant Number S-INLEC-04-GR-0015 of the U.S. Department of State. ICMEC remains grateful for this funding.

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) works around the world to advance child protection and safeguard children from abduction, sexual abuse and exploitation. Headquartered in Alexandria, Virginia, U.S.A., ICMEC also has regional representation in Brazil and Singapore. Together with an extensive network of public and private sector partners, ICMEC's team responds to global issues with tailored local solutions.

The Koons Family Institute on International Law & Policy (The Koons Family Institute) is ICMEC's in-house research arm. The Koons Family Institute combats child abduction, sexual abuse and exploitation 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, building international coalitions, bringing together great thinkers and opinion leaders, and collaborating with partners in the field to identify and measure threats to children and ways ICMEC can advocate change.

Our Mission

For nearly 20 years, ICMEC has been identifying gaps in the global community's ability to properly protect children from abduction, sexual abuse and exploitation, and expertly assembling the people, resources, and tools needed to fill those gaps.

ICMEC works every single day to make the world safer for children by eradicating child abduction, sexual abuse and exploitation. We focus on programs that have an impact on addressing these complex issues, and we offer support to governments, policymakers, law enforcement, prosecutors, industry, civil society, and many others across the globe.

We ADVOCATE **for children around the world** by proposing changes to laws, treaties, and systems based on rigorous research and the latest technology.

We TRAIN **partners on the front lines** by providing tools to professionals who interface with children to improve prevention, facilitate treatment for victims, and increase the efficacy of the identification and prosecution of people who victimize children.

We COLLABORATE **with key stakeholders** by building international networks of professionals across disciplines to anticipate issues, identify gaps, and develop crosscutting solutions.

Table of Contents

Foreword

As global accessibility to technology platforms and the Internet has increased, so too has children's online presence. According to UNICEF, one in three Internet users worldwide is a child. And while the digital world offers countless benefits and opportunities, it also vastly multiplies the risks to children.

As ICMEC enters its 20th year, we still believe that protecting children is a global imperative. We recognize the continued need for ever stronger laws, policies, and mechanisms; increased coordination across sectors; and the value of sharing ideas, perspectives, and best practices to positively influence child protection responses. We also celebrate the progress of recent years as organizations and institutions around the world have come together in collaborative initiatives such as the WePROTECT Global Alliance, utilizing tools like the Model National Response and the World Health Organization's INSPIRE Strategies to fulfill the UN Sustainable Development Goals and enhance support for children on all fronts. We are particularly excited that adoption of our Model Legislation has been included as a key recommendation of the recent Child Dignity Alliance Technology Working Group Report.

Twelve years ago, in an effort to better understand the global legislative landscape as it related to child sexual abuse material (then referred to as "child pornography"), ICMEC launched an initiative that some have called our "Rule of Law" project. We developed model legislation, after careful consideration and consultation, to increase global understanding and concern, and enable governments around the world to adopt and enact appropriate legislation necessary to combat this crime and better protect children. Since we first published the Model Legislation report in 2006, **150** countries have refined or implemented new legislation combating child sexual abuse material. We have seen tremendous progress during the 9th Edition review period, nearly the most we have seen to date. This does not, however, mean that there is nothing left to do – rather, this is the time to be diligent, to persist and push forward to help bring the remaining countries into the fold.

As always, it is important to note that the legislative review accompanying our model legislation is not a scorecard or a scold, but an effort to assess the current state and awareness of the problem. Realizing the importance of taking into consideration varying cultural, religious, socio-economic, and political norms, our model legislation continues to resemble a menu of concepts that can be applied universally, as opposed to actual statutory language. 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 and regional legal instruments, and featuring new initiatives related to implementation.

When ICMEC colleague Jessica Sarra originally conceived of this project, she could not have anticipated the enduring influence and reach it would have. Sandra Marchenko, Director of The Koons Family Institute on International Law & Policy, has helped maintain the standard of excellence for our research and has ensured the continuing relevancy and impact of the report. They each have been supported by an army of legal interns, some of whose names we proudly feature in this report, as we have done in previous versions.

Our efforts would be futile if not for extraordinary collaborators and partners around the world. We count governments, private industry, law enforcement, and vast numbers of NGO partners as allies in the effort to make the world a safer place for children. We are confident that online child exploitation can be eradicated – if only we all work together, relentlessly, and make use of every available resource, to put an end to it. We hope this report generates continued dialogue and encourages action to protect the world's children. Thank you.

Ambassador Maura Harty, *ret.*
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 with researching national legislation relevant to child sexual abuse material for the 9th 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: Rebecca DeVerter; Clara Galiano; Nuria Villar Gonzalez; Teresa Harmon; Brennan Kartchner; Alicia Kingston; Jin Lee; Thea Philip; Matthew Reiter; Hendricks Valenzuela; and Yanie Yuan;
- Mr. John Carr, Online Adviser, ECPAT International, who provided expert input and advice; 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 15 November 2018.

Executive Summary

The Issue

The rapid growth of the Internet and 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, in many countries, these technologies are ubiquitous – permeating every aspect of our lives personal and professional, individual and social. These technologies have simultaneously created a new dimension in which the sexual exploitation of children can flourish if unchecked. Children, every day, all around the world suffer sexual abuse and sexual exploitation at the hands of individuals who seek them out in order to fulfill their own sexual needs or to profit from the child's exploitation.

Sexual offenders – and others who commit crimes against children – long ago realized that digital technology provided the ability to produce illegal images of children; trade and share images of their own sexual exploits with like-minded people; and 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.

There has long been a common misconception that CSAM is a "victimless" crime. In fact, these horrific images are photographic, video, or digital records of the sexual abuse of a child. The victims portrayed in the images are young, and the images are graphic and violent. For example, out of all CSAM reports received by the U.K.'s Internet Watch Foundation (IWF) in 2017, 55% of victims appeared to be children 0-10 years of age, and 43% of the victims appeared to be children 11-15 years of age.[1] Moreover, IWF reported that 33% of images showed sexual activity between adults and children including rape or sexual torture.[2]

Similar findings also are confirmed by a 2016 Canadian study, which found that of 152,000 reports between 2008 and 2016, 78.3% of images analyzed by Cybertip.ca depicted very young, pre-pubescent children (under the age of 12 years).[3] It further showed that 50% of all of the images reviewed showed children abused through extreme sexual assault (i.e., bestiality, bondage, torture).[4] When babies or toddlers were seen, 59.72% of the abuse acts depicted involved explicit sexual activity and extreme sexual assaults of the child.[5]

INHOPE, the International Association of Internet Hotlines, reported that, in 2017, of the 1.2 million reports received by their 48-member hotlines, 18% were child sexual abuse images depicting pubescent children (ages 14-17); 79% were of pre-pubescent children (ages 3-13); and 3% were of infants (ages 0-2).[6]

A 2015 statement by the U.S. National Center for Missing & Exploited Children (NCMEC) showed similar results: of the images most frequently reported to NCMEC, 27% were of pubescent children;

---

1 Internet Watch Foundation, *Annual Report 2017*, *at* https://annualreport.iwf.org.uk/pdf/IWF_2017_Annual_Report.pdf [hereinafter *IWF 2017*] (last visited Nov. 14, 2018) (on file with the International Centre for Missing & Exploited Children).

2 *Id.*

3 Canadian Centre for Child Protection, *Child Sexual Abuse Images on the Internet: A Cybertip.ca Analysis,* Jan. 2016, *at* https://www.protectchildren.ca/pdfs/CTIP_CSAResearchReport_2016_en.pdf (last visited Nov. 14, 2018) (on file with the International Centre for Missing & Exploited Children).

4 *Id.* at 16.

5 *Id.* at 17.

6 International Association of Internet Hotlines, *INHOPE Annual Report 2017* 13, *at* http://www.inhope.org/Libraries/Annual_reports/INHOPE_Annual_Report_2017.sflb.ashx (last visited Nov. 14, 2018) [hereinafter *INHOPE 2017*] (on file with the International Centre for Missing & Exploited Children).

64% were of pre-pubescent children; and 9% were of infants and toddlers.[7] Of these images, 44% depicted oral copulation; 52% depicted anal and/or vaginal penetration; 60% depicted manual stimulation; 11% contained images depicting bondage and/or sadomasochism; and 11% depicted urination and/or defecation.[8]

In recent years, the live-streaming of child sexual abuse has become "an established reality."[9] Live child sexual abuse is streamed over the Internet via webcam to the viewer/offender to watch while the abuse is occurring in real time.[10] In some cases, the specific sexual acts are ordered/directed by the viewer/offender.[11] When the streaming is stopped, the CSAM is gone, unless the offender intentionally records it.[12] Consequently, this type of online sexual abuse "leaves little digital imprint which makes it more challenging for police to estimate the scale of it and to take measures to combat it."[13] However, software can be used to create a permanent recording (or "capture") of the live streamed child sexual abuse; these captured child sexual abuse images are then re-distributed.[14] A 2018 IWF study on the distribution of these captured images demonstrated that of 2,082 image and video captures, 98% depicted children 13 years old or younger, while 18% of the images portrayed severe content such as penetrative sexual activity.[15]

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 and 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.[16] Today, the Dark Net[17] provides an expansive platform for offenders to easily and anonymously share CSAM. The U.S. Department of Justice has noted a "significant volume of offenders using the Tor network to advertise and distribute" CSAM and

---

7 Linda Krieg, *Child Exploitation Restitution Following the Paroline v. United States Decision*, Statement before the U.S House of Representatives Judiciary Committee on the Subcommittee on Crime, Terrorism, Homeland Security and Investigations (Mar. 19, 2015), *at* https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg93798/pdf/CHRG-114hhrg93798.pdf (last visited Nov. 14, 2018) (on file with the International Centre for Missing & Exploited Children).

8 *Id*.

9 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).

10 *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse* 47 [hereainfter *Luxembourg Guidelines*], Jan. 28, 2016, Terminology and Semantics Interagency Working Group on Sexual Exploitation of Children, ECPAT International, *at* http://luxembourgguidelines.org/ (last visited Nov. 28, 2018) (on file with the International Centre for Missing & Exploited Children).

11 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://www.state.gov/j/tip/rls/fs/2017/272010.htm (last visited Nov. 26, 2018) (on file with the International Centre for Missing & Exploited Children).

12 *Id.*

13 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).

14 "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/sites/default/files/inline-files/Distribution%20of%20Captures%20of%20Live-streamed%20Child%20Sexual%20Abuse%20FINAL.pdf (last visited Nov. 26, 2018) (on file with the International Centre for Missing & Exploited Children).

15 *Id.* at 10.

16 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 Nov. 14, 2018) (on file with the International Centre for Missing & Exploited Children).

17 The Darknet or Dark Net refers to networks that are not indexed by search engines like Google and Yahoo!. These networks are only accessible using specific software and configurations, thus are not available to the general Internet public. *See*, Darknet, *Definition – What does Darknet mean*?, *at* https://www.techopedia.com/definition/2395/darknet (last visited Nov. 20, 2018).

communicate with one another undetected by law enforcement.[18] 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."[19] An analysis of one particularly egregious Tor-based website conducted by the U.S. Federal Bureau of Investigation (FBI) "found that it hosted approximately 1.3 million images depicting children subjected to violent sexual abuse."[20] Further, an "FBI investigation of a single website hosted on Tor had approximately 200,000 registered users and 100,000 individuals had accessed the site during a 12 day period."[21] The problem has proven to be a persistent one, and strong anti-CSAM legislation is needed in every country in order to combat it. In spite of this, laws addressing CSAM around the world are often weak, inconsistent, or poorly implemented; or there are no laws in place at all.

More than ten years ago, ICMEC recognized the global need to gain a better understanding of existing legislation addressing CSAM and to gauge where the issue stood on national political agendas. In response, we undertook an examination of national laws on the issue and developed model legislation in an effort to increase global awareness and concern, and enable governments around the world to adopt and enact much-needed legislation to protect the most innocent victims.

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 then 184 INTERPOL member countries. The report has been updated regularly. Now in its 9th Edition, the report includes 196 countries and has become a globally-utilized tool for policymakers, law enforcement agencies, child protection experts and organizations, industry partners, and others.

ICMEC's research looks at a core set of criteria to gain a full understanding of national legislation on the issue. In particular, we are looking to see if national legislation:

(1) exists with specific regard to CSAM;
(2) provides a definition of CSAM;
(3) criminalizes technology-facilitated CSAM offenses;[22]
(4) criminalizes the knowing possession of CSAM, regardless of the intent to distribute; and
(5) requires Internet Service Providers (ISPs)[23] to report suspected CSAM to law enforcement or to some other mandated agency.

The model legislation consists of 13 fundamental topics/provisions that are essential to a comprehensive legislative strategy to combat child sexual abuse material.[24] 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[25] as well as related regional and

---

18 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 Nov. 20, 2018).

19 *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 Nov. 16, 2018) (on file with the International Centre for Missing & Exploited Children).

20 *Id*. at 74.

21 *Id.*

22 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.

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

24 The 13 fundamental topics are listed on page 5.

25 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

international law, and a discussion of the implementation and enforcement of national legislation. The final section contains a global legislative review with country-specific information.

It is important to note that the legislative review accompanying the model legislation is not about criticism, but rather about assessing the current state and awareness of the problem and learning from one another's experiences. Additionally, a lack of legislation specific to CSAM does not mean that other forms of child sexual exploitation and child abuse are not criminalized.

Methodology

The review process has remained much the same each year. Open source research into national anti-CSAM is conducted in-house with the help of a team of research interns. Primary sources of information include: LexisNexis; government submissions to the 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), 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 attention of 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 United Nations in New York. All letters consist of a summary of the model legislation project, as well as country-specific results, and request confirmation or correction of 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

While the term "child pornography" is often still utilized in national legislation, in line with recent global movement and international consensus, the term has been replaced with the term "child sexual abuse material" as it more aptly describes the true nature and extent of sexually exploitive images of child victims to which children can never consent.[26, 27] Consequently, with this 9th Edition we have made the conscious decision to align terminology with that now accepted by the international child protection community: "child sexual abuse material" now takes the place of "child pornography."

When the term "child pornography" is used in this report, it is to maintain the integrity of the source document (i.e., international and regional legal instruments; 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,"[28] as well as the use of a child to create such a representation.

---

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.

26 *See,* Luxembourg Guidelines, *supra* note 10, at 36-37.

27 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).

28 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 report, along with comparative information from the 1st and 8th Editions, are presented in the table below.

	1st Edition (2006)*	8th Edition (2016)	9th Edition (2018)
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	**82** countries had sufficient legislation ▪ 11 countries met all 5 of the criteria ▪ 71 countries met 4 of the 5 criteria	**118** countries have sufficient legislation ▪ 21 countries meet all 5 criteria ▪ 97 countries meet 4 of the 5 criteria
No legislation at all specifically addressing CSAM	**95** countries	**35** countries	**16** countries
Of the remaining 62 countries that have legislation specifically addressing CSAM:			
Do not define CSAM	**54** countries	**60** countries	**51** countries
Do not provide for technology-facilitated CSAM offenses	**27** countries	**26** countries	**25** countries
Do not criminalize the knowing possession of CSAM, regardless of intent to distribute	**41** countries	**50** countries	**38** 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, credit card companies, and banks;
(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.

Model Legislation

A comprehensive legislative strategy that is aimed at combating CSAM and that allows law enforcement to aggressively investigate and prosecute offenders must extend beyond 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, a challenging obstacle to the consistent and harmonized protection of children from sexual exploitation on the international level. While a person under the age of 18 may be able to freely consent to sexual relations, such an individual is not legally 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 who is 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 more accurately describe the criminal nature of such material and to avoid any confusion regarding consent.[29]

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 require explanation as well. 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.

[29] Luxembourg Guidelines, *supra* note 10.

Moreover, it is imperative that, with the advent of new technologies, mention be made of all the forms CSAM can take including, but not limited to: film, DVD, CD-ROM, diskette, CD-R, data files, data storage devices, software, information and communication technologies (ICTs), and other electronic or digital media; all the ways CSAM can be distributed, including via computer networks, smart phones, and the Internet; and all the ways in which CSAM can be possessed, including by simply knowingly viewing an image on the Internet or knowingly downloading an image to one's computer, tablet, or smart phone.

Offenses

Incorporate CSAM offenses into the penal code.

Mere labor legislation that bans the worst forms of child labor, including CSAM, without detailing specific criminal offenses, criminal sanctions, and criminal punishments is insufficient. 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 recognizing CSAM as an evil that affects child welfare, CSAM is a crime and must be recognized as such. CSAM represents nothing less than the memorialization of the sexual degradation/molestation/abuse/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 new trends such as "custom" CSAM – the sale of images of child rape created to order for the consumer and "real-time" CSAM for which subscribers pay to watch the live-streamed rape and sexual abuse of children as it occurs.[30]

A 2011 study in the United States found that 41% of arrested CSAM possessors were "dual offenders," who sexually victimized children and possessed CSAM.[31] One out of every six cases that began with a CSAM possession investigation involved a dual offender who also had sexually abused a child or attempted to do so, which suggests a correlation between the knowing simple possession of CSAM and committing sexual abuse upon a child.[32] 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, and trade CSAM on a daily basis. Therefore, as stated earlier, it is imperative that specific mention 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.

---

30 Andrew Vachss, *Let's Fight This Terrible Crime Against Our Children*, PARADE, Feb. 19, 2006, *at* http://www.vachss.com/av_dispatches/parade_021906.html (last visited Nov. 14, 2018) (on file with the International Centre for Missing & Exploited Children).

31 Janis Wolak, et al., *Child Pornography Possessors: Trends in Offender and Case Characteristics* 39, SEXUAL ABUSE: A JOURNAL OF RESEARCH AND TREATMENT 23(1) 22-42 2011 (on file with the International Centre for Missing & Exploited Children).

32 *Id.*

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 downloading/accessing illegal content should be penalized.

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.

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 and 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.[33] 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 (i.e., email, social networking sites, instant messaging, gaming systems, bulletin boards, and chat rooms) 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 and 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 or CSAM to the child to lower their inhibitions, desensitize them to sexual activity and normalize this behavior, and teach the child sexual behaviors.[34] Showing pornographic images and videos or CSAM to the child also can increase the child's sexual curiosity and lead to sexual discussions that may advance a sexual relationship and ultimately increase the likelihood of a sexual encounter, physical or virtual, with that child.[35]

Online grooming often "overlaps with incidents of online child sexual…extortion."[36] 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 offender. Once the

---

[33] 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 Nov. 14, 2018) (on file with the International Centre for Missing & Exploited Children) (emphasis added).

[34] 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).

[35] 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).

[36] 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 Nov. 14, 2018) (on file with the International Centre for Missing & Exploited Children).

offender has obtained the images/videos, they may threaten, intimidate, and 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.[37] Child victims of sextortion are typically between the ages of 10-17 years, but victims as young as nine years old have been documented.[38]

Data on the extent of online grooming is difficult to compile due to the lack of a universal understanding and use of the term. It is clear from studies, however, 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.[39] Grooming relationships can have a personal sexual intent or commercial exploitation intent and thus often precede the creation or distribution of CSAM.[40]

Recent reports show that an increasing number of grooming cases take place completely online; the offender obtains sexual gratification through non-contact offenses without the intention of meeting the child in person.[41] For example, an offender may send or receive sexually explicit photographs, perform or observe sexual acts over a webcam, and participate in sexually explicit conversations through chat, text, or email. For instance, the U.K. Child Exploitation and Online Protection Centre found that only 7% of the 1,145 online grooming cases investigated in the United Kingdom in 2012 involved the intent to meet a child offline.[42] As noted in the Explanatory Memo for Ireland's Criminal Law (Child Grooming) Bill 2014, by the time intent to meet the child has been expressed, it may be "too late" to protect the child as they likely already have been groomed and exploited online.[43]

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 and exploitation of children. It is therefore imperative that online grooming legislation criminalize all types of grooming, regardless of whether the offender intends for the relationship to progress to an offline setting.[44]

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.

---

37 Luxembourg Guidelines, *supra* note 10, at 52.

38 Josh Saul, *Online 'Sextortion' Is on the Rise*, NEWSWEEK, Dec. 1, 2016, *at* https://www.newsweek.com/2016/12/09/sextortion-social-media-hacking-blackmail-527201.html (last visited Nov. 14, 2018) (on file with the International Centre for Missing & Exploited Children).

39 Trent Toone, *Kids revealing too much online, study says*, Deseret News, Feb. 6, 2011, *at* http://www.deseretnews.com/article/705366050/Kids-revealing-too-much-online-study-says.html?pg=all (last visited Nov. 14, 2018) (on file with the International Centre for Missing & Exploited Children).

40 U.S. Department of Justice, Child Exploitation and Obscenity Section (CEOS), *Child Pornography, at* https://www.justice.gov/criminal-ceos/child-pornography (last visited Dec. 3, 2018) (on file with the International Centre for Missing & Exploited Children).

41 Dr. Mike McGuire and Samantha Dowling, *supra* note 31, at 9; *See also* Dr. Jo Bryce, *Online Sexual Exploitation of Young People* 15, CYBERSPACE RESEARCH UNIT SCHOOL OF PSYCHOLOGY UNIVERSITY OF CENTRAL LANCASHIRE (on file with the International Centre for Missing & Exploited Children).

42 *Ceop warns over 'alarming new trend' in online sex abuse*, BBC NEWS, Feb. 4, 2013, *at* https://www.bbc.com/news/uk-21314585 (last visited Oct. 25, 2018) (on file with the International Centre for Missing & Exploited Children). *See also,* Child Exploitation and Online Protection Centre, *Threat Assessment of Child Sexual Exploitation and Abuse (2013a)* 11, Jun. 2013 (on file with the International Centre for Missing & Exploited Children).

43 Explanatory Memorandum, Criminal Law (Child Grooming) Bill 2014, Ireland, *at* http://www.oireachtas.ie/documents/bills28/bills/2014/8914/b8914d-memo.pdf (last visited Nov. 14, 2018) (on file with the International Centre for Missing & Exploited Children).

44 *See,* International Centre for Missing & Exploited Children (ICMEC), *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 Nov. 16, 2018) (on file with the International Centre for Missing & Exploited Children).

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/corporate citizenship/corporate social 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.

Legislative language providing for sufficient/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. The Child Dignity Alliance Technology Working Group recommends in its 2018 report that governments should require industry to ensure that CSAM is "detected, reported and speedily removed" from its networks by providing "legislative and policy clarity about industry's obligations, penalties for non-compliance, and the development of guidance, information and resources to aid and assist industry to comply."[45]

In the United States, NCMEC reports that since 1998 ISPs have reported more than 69 million images and videos to the CyberTipline.[46] In 2017 alone NCMEC's CyberTipline received more than 10 million reports from U.S.-based ISPs.[47]

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 the payments industry also should be encouraged to report. 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 by thousands and possibly millions of individuals throughout the world. Financial companies must be vigilant and should be required to report CSAM transactions to law enforcement or another mandated agency when the transactions are discovered.

The U.S. Financial Coalition Against Child Pornography (FCACP)[48] is an example of banks, credit card companies, electronic payment networks, and third-party payment companies proactively coordinating with law enforcement, ISPs, and civil society to eradicate the commercial trade of CSAM online. The success of the U.S. FCACP led to its expansion in Europe[49] and the Asia Pacific[50] region. The FCACP 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.

---

45 Child Dignity in the Digital World, *Child Dignity Alliance Technology Working Group Report* 6, Nov. 2018 (on file with the International Centre for Missing & Exploited Children).

46 NCMEC, *Child Sexual Abuse Material: By the Numbers*, *at* http://www.missingkids.org/theissues/sexualabusematerials (last visited Nov. 15, 2018).

47 International Association of Internet Hotlines, *supra* note 6, at 14.

48 *U.S. Financial Coalition Against Child Pornography*, ICMEC & NCMEC, *at* http://www.icmec.org/fcacp/ (last visited Nov. 28, 2018).

49 European Financial Coalition against Commercial Sexual Exploitation of Children Online, *at* http://www.europeanfinancialcoalition.eu/ (last visited Nov. 28, 2018).

50 *Asia-Pacific Financial Coalition Against Child Pornography*, ICMEC, *at* https://www.icmec.org/apac-fcacp/ (last visited Nov. 28, 2018).

Require healthcare and social services professionals, teachers, and 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, and others in child-serving professions. As a first line of defense, often these child-serving professionals are the first to notice signs of physical and 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 the course of their routine work while repairing or servicing a computer or smart phone, 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 the 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 and encouraged to utilize technology tools to scan their networks/platforms to identify and eliminate CSAM.[51] ISPs also may employ filtering and/or blocking technologies to impede access to CSAM.[52] Tools like PhotoDNA[53] 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 links on websites that have previously been reported to Cybertip.ca, detect CSAM, and determine where these images/videos are available on the Internet before issuing a notice to the hosting provider requesting immediate removal of the illegal content.[54] Industry can also use the Arachnid API[55] to quickly detect CSAM on their service, rather than waiting for Project Arachnid to detect material and send a notice.[56] Project Arachnid detects 100,000 unique suspected images per month and issues approximately 700 removal notices each day to service providers.[57] ISPs can proactively utilize technology tools like these to detect illegal content on their networks and speed 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

---

51 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 Nov. 16, 2018) (on file with the International Centre for Missing & Exploited Children). *See also*, Child Dignity in the Digital World, *supra* note 45, at 7.

52 *See*, 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 Nov. 14, 2018) (on file with the International Centre for Missing & Exploited Children).

53 Microsoft, *PhotoDNA, at* https://www.microsoft.com/en-us/photodna (last visited Nov. 14, 2018) (on file with the International Centre for Missing & Exploited Children).

54 Canadian Centre for Child Protection, *Project Arachnid, at* https://protectchildren.ca/en/programs-and-initiatives/project-arachnid/ (last visited Nov. 14, 2018) (on file with the International Centre for Missing & Exploited Children).

55 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 Dec. 3, 2018).

56 Canadian Centre for Child Protection, *supra* note 54.

57 *Id.*

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.[58] Likewise, Article 25 of the 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 of or disseminating CSAM in their territory and "to block access to web pages containing or disseminating [CSAM] towards the Internet users within their territory."[59]

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

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 like IP address, date, time, size, type, duration, and source of communication[60]; location data,[61] which is data that helps identify the subscriber) or **content data** (i.e., the text of users' emails, the "message" that was delivered by a communication, or the contents of a file such as an image or film[62]). Data preservation is the obligation to preserve stored data with probative value of an identified user who is currently under investigation after a request by law 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 differing capabilities, technologies, and resources available. Legislation should indicate the purpose for 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/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

---

58 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 Oct. 25, 2018) (on file with the International Centre for Missing & Exploited Children).

59 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 Nov. 13, 2018) (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 Oct. 25, 2018) (on file with the International Centre for Missing & Exploited Children).

60 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 Nov. 27, 2018) (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).

61 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 Nov. 27, 2018) (on file with the International Centre for Missing & Exploited Children).

62 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).

practicable. The period of time that requested data must be preserved should also be outlined with the possibility 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.[63]

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, judicial authorities) responsible for the protection from and prevention of child sexual abuse and exploitation.[64] It further requires State Parties to encourage cooperation between the competent state authorities, civil society and the private sector to better prevent and fight child sexual abuse and exploitation.[65]

One example of a cross-sectoral collaboration is the WePROTECT MNR,[66] which provides countries with a roadmap for collaborative, multi-disciplinary national responses to address child sexual exploitation and abuse online. Another collaborative effort – the aforementioned FCACP – brings together key actors from law enforcement, the private sector, and civil society to disrupt the online trade of CSAM.[67]

Sanctions and Sentencing

Address the criminal liability of children involved in CSAM.
There should be no criminal liability for children involved in CSAM, and such 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 that child.

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

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.[68] Mere fines and misdemeanor classifications are not enough.

Sentencing provisions should take into account aggravating factors and enhancements.[69] 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,

---

63 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).
64 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201), *supra* note 58, at Article 10 (1).
65 *Id.* at Article 10 (3).
66 WePROTECT Global Alliance, *Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response*, *at* https://www.weprotect.org/the-model-national-response/ (last visited Oct. 26, 2018) (on file with the International Centre for Missing & Exploited Children).
67 U.S. Financial Coalition Against Child Pornography, *supra* note 48.
68 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).
69 *Id*.

distributed, and possessed; and any potential threat or risk the offender may pose to the community upon release.

In the past, media outlets from across the world have reported that criminals other than sex offenders, including terrorists, organized criminals, and gangs, have been found with CSAM. While some criminals may obtain CSAM for personal interest, accounts have suggested that these criminals may have new uses for CSAM. Terrorists have reportedly manufactured CSAM to send concealed messages and data[70] and finance their activities.[71] Likewise, organized criminals and gangs involved in human trafficking may produce pornographic/sexually exploitative images of their victims to generate additional revenue, blackmail victims into compliance, and advertise commercial sexual services.[72] The FBI reports that several sophisticated online criminal organizations using the Dark Net have written security manuals including security protocols and encryption techniques to help their members elude law enforcement and facilitate the sexual abuse of children.[73]

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

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.[74] 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.[75]

Law Enforcement Investigations & Data Retention

In the United States, for more than 10 years there has been ongoing discussion concerning the importance of computer data to investigations of online CSAM by law enforcement. The discussion has focused on the need for legal provisions requiring ISPs to retain and preserve data. In order 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 perpetrator.[76] Jason Weinstein, Deputy Assistant Attorney General of the Department of Justice, testified at a Congressional hearing in 2011 that,

> "[d]espite the diligent and efficient work by law enforcement officers at all levels, critical data has too often been deleted by providers before law enforcement can obtain that lawful process. This gap between providers' retention practices and the needs of law enforcement can be extremely harmful to investigations that are critical to protecting the public from predators and other criminals. And the problem is exacerbated by the complexity of investigating crimes committed using online means. These crimes are difficult to detect, and they may not be discovered or reported to law

---

70 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).

71 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/ (last visited Nov. 16, 2018) (on file with the International Centre for Missing & Exploited Children); *see also,* Richard Kerbaj and Dominic Kennedy, *supra* note 70.

72 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 Nov. 16, 2018) (on file with the International Centre for Missing & Exploited Children).

73 U.S. Department of Justice – CEOS, *supra* note 40.

74 Eva J. Klain, *supra* note 68, at 47.

75 *Id*.

76 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).

> enforcement until months and months have gone by. And they are even more difficult to investigate. They often involve the time-consuming process of obtaining evidence from overseas. They often require months and months of work obtaining records from a series of providers as agents attempt to follow the trail of steps used by criminals to try to cover their tracks and render themselves anonymous. Unfortunately, when providers have not retained the data that is needed for a sufficient period of time, important investigations of serious crimes may come to a dead end."[77]

The International Association of Chiefs of Police further supported this assessment stating that, "the failure of the Internet access provider industry to retain subscriber information and source or destination information for any uniform, predictable, reasonable period has resulted in the absence of data, which has become a significant hindrance and even an obstacle in certain investigations."[78]

Individual ISPs generally have the ability and technological capacity to retain and preserve users' data in order 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.[79] The suggestion, however, that data retention by ISPs should be mandatory has spurred active debate as opponents raised privacy and free speech concerns.[80]

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,[81] 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, date, time, size, type, duration, and source of communication[82]; location data[83]).[84] The objective of the Data Retention Directive was 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.[85] 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."[86] These laws significantly influenced national legislation concerning cybercrime and data processing/protection/retention. In the 8th Edition of this report, we observed that, globally, more than 75 countries had data retention and/or

---

77 Hearing before the Subcommittee on Crime, Terrorism, and Homeland Security of the Committee of the Judiciary of the U.S. House of Representatives, First Session, Serial No. 112-3, *Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes,* Jan. 25, 2011, *at* https://www.gpo.gov/fdsys/pkg/CHRG-112hhrg63873/pdf/CHRG-112hhrg63873.pdf (last visited Nov. 20, 2018) (on file with the International Centre for Missing & Exploited Children).

78 *Id.*

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

80 *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 Nov. 28, 2018) (on file with the International Centre for Missing & Exploited Children).

81 Convention on Cybercrime (CETS 185), *supra* note 60. For additional information on the *Convention on Cybercrime, see* page 25 of the Regional and International Law section of this report.

82 Convention on Cybercrime (CETS 185), *supra* note 60; 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).

83 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 Nov. 27, 2018) [hereinafter *EU Data Retention Directive*] (on file with the International Centre for Missing & Exploited Children).

84 EU Data Retention Directive, *supra* note 61.

85 *Id.*

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

preservation laws in place in 2016.[87] Many countries framed their legislation with a view to the EU Data Retention Directive and Budapest Convention.

In April 2014, the European Court of Justice (ECJ) declared the Data Retention Directive invalid, and reaffirmed its ruling in 2016.[88] 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,[89] 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 European Union.[90] 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.[91] Following the ECJ ruling, data retention/preservation laws in numerous countries were held to be void/invalid.

Since then, a paradigm shift in data privacy regulation has occurred, changing how the world thinks about personal data.[92] In 2016, the General Data Protection Regulation (GDPR) was approved by the EU Parliament following four years of preparation and debate.[93] The GDPR, which replaced the earlier EU Data Protection Directive,[94] is more heavily focused on protecting individual users' right to privacy and how their data is handled.[95] The GDPR enables people of the EU to have better control of their personal data, forces companies to think carefully about the data they hold, and makes companies accountable for how they use and store the data.[96] 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.[97]

Alongside the GDPR came the introduction of the new EU Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention,

---

87 Real-time interception of communications by technical means (i.e., wiretap) carried out by law enforcement or ISPs compelled to do so by the government was not considered for the purposes of this publication.

88 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).

89 *Id.*

90 *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 88, at 69 (on file with the International Centre for Missing & Exploited Children).

91 Judgment of the European Court of Justice (Grand Chamber), *supra* note 88, paragraphs 39-45.

92 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 Nov. 20, 2018) (on file with the International Centre for Missing & Exploited Children).

93 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 Nov. 9, 2018). *See also,* EU GDPR Portal, *GDPR Portal: Site Overview*, *at* https://www.eugdpr.org/ (last visited Nov. 9, 2018).

94 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 Nov. 19, 2018) (on file with the International Centre for Missing & Exploited Children).

95 For information regarding children's personal data protection and the GDPR, see *Children and the GDPR – What's New?*, Information Commissioner's Office, *at* https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/whats-new/ (last visited Dec. 3, 2018) (on file with the International Centre for Missing & Exploited Children).

96 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 Dec. 3, 2018). *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 Dec. 3, 2018) (on file with the International Centre for Missing & Exploited Children).

97 *Handbook on European Data Protection Law, 2018 Edition* 31, European Union Agency for Fundamental Rights and Council of Europe *at* https://www.echr.coe.int/Documents/Handbook_data_protection_02ENG.pdf (last visited Nov. 9, 2018) (on file with the International Centre for Missing & Exploited Children).

investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data (Directive 2016/680).[98] Directive 2016/680 governs the handling of data in law enforcement situations.[99] EU Member States were required to adopt and publish the laws, regulations, and administrative provisions necessary to comply with the Directive by 6 May 2018.[100] As of 15 November 2018, 16 countries had transposed the Directive into national law.[101]

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."[102] 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."[103] 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.[104]

The GDPR further dictates specific rules on its territorial scope.[105] It applies not only to businesses established in the European Union, but also to controllers and processors outside of the European Union that monitor or offer goods and services to EU residents, exponentially expanding the reach and applicability of the GDPR.[106] 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."[107]

The GDPR and Directive 2016/680 provide new limitations on how long personal data may be kept. Under the GDPR, personal data can be kept/retained for "no longer than is necessary for the purposes for which the personal data are processed."[108] Directive 2016/680 gives Member States the capability 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."[109] These limitations are in place to ensure that irrelevant, excessive, inaccurate or out of date information is no longer being stored.[110]

---

98 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 Nov. 9, 2018) (on file with the International Centre for Missing & Exploited Children).

99 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 Nov. 19, 2018) (on file with the International Centre for Missing & Exploited Children).

100 *Id.* at Article 63.

101 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).

102 EU General Data Protection Regulation (GDPR), *supra* note 93, at Article 4 – Definitions.

103 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 94, at Article 2 – Definitions.

104 EU Data Retention Directive, *supra* note 59, at Article 2 – Definitions.

105 EU General Data Protection Regulation (GDPR), *supra* note 93, at Article 3 – Territorial Scope.

106 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 Oct. 30, 2018) (on file with the International Centre for Missing & Exploited Children). See Gene

107 EU General Data Protection Regulation (GDPR), *supra* note 93, at Article 2 – Material Scope.

108 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 Nov. 28, 2018) (on file with the International Centre for Missing & Exploited Children).

109 *Id.*

110 *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 performance of a task carried out in the public interest or for legitimate interests pursued by the data controller.[111]

While the EU countries are likely the most impacted by the GDPR, the Regulation has had global impact that requires compliance from companies around the world. In response, countries have begun updating domestic legislation to align more closely with the European Union's privacy-based approach.[112] This legislative reboot has created some uncertainty as countries like Argentina, Brazil, Canada, Colombia, Japan, and South Africa have developed – or are currently developing – laws similar to the GDPR while others continue to rely on existing legislation.

The need for data in 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 Wiegman gave testimony concerning the need for law enforcement to be able access data held by U.S. communications service providers outside of the United States.[113] "The 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."[114]

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 and that related laws strike a balance between child protection and protection of privacy.

---

111 EU General Data Protection Regulation (GDPR), *supra* note 93, at Article 6 – Lawfulness of processing; Article 10 – Processing of personal data relating to criminal convictions and offences.

112 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 Nov. 19, 2018) (on file with the International Centre for Missing & Exploited Children).

113 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 Nov. 20, 2018) (on file with the International Centre for Missing & Exploited Children).

114 *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 are best able to exploit children. A holistic and uniform approach is the most effective means of combating the sexual exploitation of children because it allows for consistency in criminalization and punishment; it raises public awareness of the problem; it increases services available to assist victims; and it improves overall law enforcement efforts at the national and international levels. Complying with international legal standards is an initial step in addressing CSAM, to be followed by national implementing 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 (U.N.) Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.[115] 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.[116]

In addition to these international legal instruments, there are several regional legal instruments that are specifically relevant in the fight against CSAM. The Council of Europe's Convention on Cybercrime[117] and Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[118] 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, allowing for more effective prosecution of perpetrators.

The European Union adopted the Directive on combating the sexual abuse and sexual exploitation of children and child pornography, which came into force upon adoption.[119] 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. As of 15 November 2018, 27 EU Member States had taken steps to implement this Directive under their national law.[120]

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; it describes measures for treatment

---

115 Optional Protocol, *supra* note 28.

116 *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 Nov. 13, 2018) (on file with the International Centre for Missing & Exploited Children).

117 Convention on Cybercrime (CETS 185), *supra* note 60.

118 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201), *supra* note 58.

119 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 Nov. 13, 2018) (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 Oct. 25, 2018) (on file with the International Centre for Missing & Exploited Children).

120 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-content/EN/NIM/?uri=CELEX:32011L0093 (last visited Nov. 13, 2018) (on file with the International Centre for Missing & Exploited Children).

of offenders; and it contains provisions on supporting and protecting child victims with a focus on the best interests of the child.[121]

The African Charter on the Rights and Welfare of the Child,[122] as well as the African Union Convention on Cyber Security and Personal Data Protection,[123] 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.[124]

In conjunction with the international and regional legal instruments, several global initiatives have gained momentum in recent years that support cross-border coordination and collaboration to end the abuse, exploitation, trafficking, and all forms of violence against children. The United Nations Sustainable Development Goals (SDGs) of the 2030 Agenda for Sustainable Development[125] were adopted in September 2015 by world leaders and officially came into force 1 January 2016.[126] The 17 Sustainable Development Goals universally apply to all people and act as a call to action for all countries.[127] With specific regard to the protection of children from sexual abuse is SDG 16.2 on ending the abuse, exploitation, trafficking, and all forms of violence against and torture of children.[128]

In 2016, in support of global achievement of SDG 16.2, 10 global agencies collaborated, under the leadership of the World Health Organization (WHO), to develop INSPIRE – an evidence-based package of seven strategies aimed at assisting governments implement and monitor interventions to prevent and respond to violence against all children.[129] The INSPIRE strategies provide a comprehensive framework that presents specific approaches to implement each strategy and assess progress.

Likewise, the WePROTECT MNR, published in November 2016, supports implementation of the SDGs with a particular focus on ending abuse, exploitation, trafficking, and all forms of violence and abuse of children.[130] The MNR is intended to help "countries to establish and develop coordinated national responses to online child sexual exploitation" by detailing 21 specific capabilities needed for an effective child protection approach, highlighting existing good practices, and identifying resources for further guidance and support.[131]

---

121 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 119.

122 African Charter on the Rights and Welfare of the Child, 1990, *at* http://www.achpr.org/files/instruments/child/achpr_instr_charterchild_eng.pdf *entered into force Nov. 29, 1999* (last visited Nov. 7, 2018) (on file with the International Centre for Missing & Exploited Children).

123 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 Nov. 13, 2018) (on file with the International Centre for Missing & Exploited Children).

124 League of Arab States, Arab Convention on Combating Information Technology Offences (Arab Convention), 2010, at https://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd (last visited Nov. 30, 2018) (on file with the International Centre for Missing & Exploited Children).

125 Resolution adopted by the General Assembly on 25 September 2015 [without reference to a Main Committee (A/70/L.1)] 70/1. *Transforming our world: the 2030 Agenda for Sustainable Development,* Oct. 2015, *at* http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E (last visited Sep. 30, 2018).

126 *The Sustainable Development Agenda*, United Nations, *at* https://www.un.org/sustainabledevelopment/development-agenda/ (last visited Nov. 13, 2018).

127 *Id.*

128 UN Sustainable Development Goals, *Goal 16: Peace, Justice and Strong Institutions, at* https://www.un.org/sustainabledevelopment/peace-justice/ (last visited Sep. 30, 2018).

129 World Health Organization (WHO), *INSPIRE: Seven Strategies for Ending Violence Against Children*, 2016, *at* http://www.who.int/violence_injury_prevention/violence/inspire/en/ (last visited Oct. 26, 2018) (on file with the International Centre for Missing & Exploited Children).

130 WePROTECT Model National Response, *supra* note 66.

131 WePROTECT Global Alliance, *Our Commitments, at* https://www.weprotect.org/our-commitments/ (last visited Nov. 28, 2018).

Together, the international and regional legal instruments and targeted global initiatives demonstrate increased recognition and awareness of online child sexual abuse and exploitation and growing commitment to undertaking coordinated, comprehensive efforts in response.

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

While the Convention on the Rights of the Child[132] (CRC) aims to ensure a broad range of human rights for children – including civil, cultural, economic, political, and social rights[133] – there are Articles within the CRC and the CRC Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography[134] (Optional Protocol) that 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.

---

132 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 Nov. 13, 2018) (on file with the International Centre for Missing & Exploited Children).

133 *See,* UNICEF, Convention on the Rights of the Child, *at* http://www.unicef.org/crc/ (last visited Nov. 13, 2018) (on file with the International Centre for Missing & Exploited Children).

134 Optional Protocol, *supra* note 28.

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).[135] 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 19 November 2000. Currently, 182 ILO Member states have ratified the Convention, and 5 countries have not yet ratified.[136]

States parties are dedicated to the immediate elimination of dangerous forms of child labor.[137] 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.[138]

- 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.

---

135 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 Nov. 13, 2018) (on file with the International Centre for Missing & Exploited Children).

136 *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 Nov. 13, 2018) (on file with the International Centre for Missing & Exploited Children).

137 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 Nov. 13, 2018) (on file with the International Centre for Missing & Exploited Children).

138 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 Nov. 13, 2018) (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[139] (Budapest Convention) with the hope of implementing a cooperative and uniform approach to the prosecution of cybercrime. The Budapest Convention opened for signature 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, 61 countries (43 member States and 18 non-member States) have ratified the Budapest Convention, and 4 other countries (3 member States and 1 non-member State) have signed, but not ratified, the Budapest Convention.[140]

Pertinent to the area of child sexual exploitation is Title 3 of the Cybercrime Convention, entitled "Content-related Offences." Specifically, Article 9 of Title 3 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.

---

139 Convention on Cybercrime (CETS 185), *supra* note 60.

140 *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 Nov. 7, 2018) (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[141] (Lanzarote Convention) focuses on ensuring the best interests of children through prevention of abuse and exploitation, protection and assistance for victims, punishment of perpetrators, and promotion of 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, 44 member States have ratified the Lanzarote Convention, and 3 other member States have signed, but not ratified, the Lanzarote Convention.[142] 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.

141 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201), *supra* not 58.

142 *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 Nov. 7, 2018) (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 European Union adopted the 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, and replacing Council Framework Decision 2004/68/JHA.[143] 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 and 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.[144]

The Directive describes measures that may be taken to identify and treat those who would become offenders[145] or recidivists,[146] and prevent offenders from maintaining professions involving regular contact with children,[147] and it introduces provisions to protect the child victim during investigations and legal proceedings.[148] Furthermore, the Directive encourages enhanced cooperation between Member States and non-Member States to ensure the removal of CSAM from servers in non-Member States,[149] and to tackle child sex tourism.[150]

The Directive entered into force upon publication on 13 December 2011. In order 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. As of November 2018, 26 Member States had taken steps to implement this Directive under their national law.[151]

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 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

143 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 119.
144 *Id.* at paragraphs 3 and 12, and Articles 6 and 25.
145 *Id.* at Article 22.
146 *Id.* at Article 24.
147 *Id.* at Article 10.
148 *Id.* at Article 20.
149 *Id.* at paragraph 46.
150 *Id.* at paragraph 29.
151 National Implementing Measures, *supra* note 120. 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 119, at paragraph 52.

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.

African Charter on the Rights and Welfare of the Child

The African Charter on the Rights and Welfare of the Child[152] (African Charter) was introduced to promote and protect child rights on the African continent. The African Charter focuses on ensuring the best interests of children through prevention of abuse and exploitation, protection and assistance for victims, punishment of perpetrators, 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. Currently, 41 countries have signed and ratified the African Charter, and 9 other countries have signed, but not ratified.[153]

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.

[152] African Charter on the Rights and Welfare of the Child, 1990, *at* http://www.achpr.org/files/instruments/child/achpr_instr_charterchild_eng.pdf *entered into force Nov. 29, 1999* (last visited Nov. 7, 2018) (on file with the International Centre for Missing & Exploited Children).

[153] *See,* African Charter on the Rights and Welfare of the Child: Ratification Table, *at* http://www.achpr.org/instruments/child/ratification/ (last visited Nov. 5, 2018) (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.[154] 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.[155] The Malabo Convention aims to strengthen and harmonize existing cyber security legislation to repress cybercrime in Member States.[156]

The Malabo Convention was adopted on 27 June 2014 and has not yet entered into force.[157] The Convention is open for signature by Member States of the African Union. Currently, 3 countries have ratified the African Union Convention, and 11 other countries have signed, but not yet ratified it.[158]

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;
  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.

---

154 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 Nov. 7, 2018) (on file with the International Centre for Missing & Exploited Children).

155 *Id.*

156 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 Nov. 13, 2018) (on file with the International Centre for Missing & Exploited Children).

157 *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_0.pdf (last visited Nov. 13, 2018) (on file with the International Centre for Missing & Exploited Children).

158 *Id.*

- 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 aimed at protecting Arab society against information technology offenses.[159] 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 Member States of the League of Arab States. By 2014, 7 Arab States had ratified the Arab Convention, and 18 others had signed.[160]

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.

---

159 League of Arab States, *Arab Convention on Combating Information Technology Offences* (Arab Convention), 2010, at https://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd (last visited Nov. 30, 2018) (on file with the International Centre for Missing & Exploited Children). 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 Nov. 30, 2018) (on file with the International Centre for Missing & Exploited Children).

160 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 Nov. 13, 2018).

Implementation

There has been significant legislative change over the last 12 years as more countries have developed laws to protect children from sexual abuse and exploitation with a focus on CSAM. Even with slow but steady statutory improvement, the question remains whether countries that have laws are in fact enforcing them. To ensure that children around the world are better protected, drafting and passing legislation are only the first steps. There must be comprehensive, cross-sectoral efforts to implement and enforce those laws in order for them to become truly useful tools.

Enforcement can include not only the application of civil/criminal penalties for certain conduct articulated in the law (i.e., arrests, prosecutions, and convictions), but 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.[161]

Preventive	Protective
▪ National Strategy Plans ▪ Child online protection frameworks ▪ Training and education programs ▪ Public awareness campaigns ▪ Corporate Social Responsibility (CSR) programs ▪ Research and data collection	▪ Improved legislative tools ▪ Formalized legal processes, including arrests, prosecutions, and convictions ▪ Services for victims ▪ Services for perpetrators ▪ Monitoring and reporting mechanism

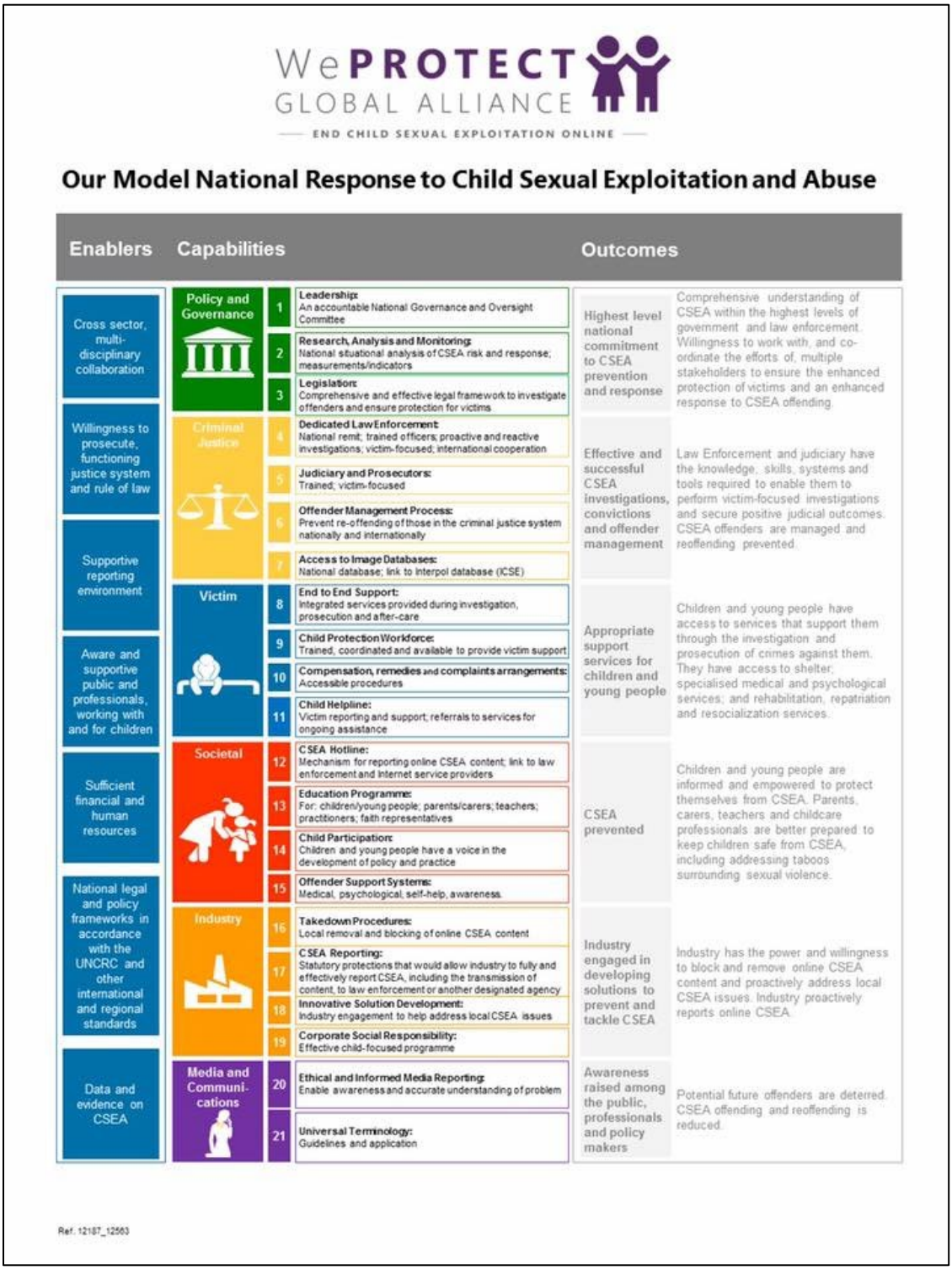
In 2017, in an effort to understand the measures countries are undertaking to support their national anti-CSAM legislation, and taking into account the aforementioned preventive and protective measures, ICMEC conducted a review process based on seven benchmarks that, if met, indicate a country's willingness to address CSAM through more than legislative action.[162] The benchmarks included: (1) investigations, arrests, prosecutions, and convictions; (2) 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. The results of the implementation report showed that of the **161** countries reviewed, **10** countries met <u>none</u> of the benchmarks, and another **35** countries met <u>fewer than 4</u> benchmarks. Only **44** met <u>all 7</u> benchmarks, making it clear that further action is needed to create a comprehensive global response to CSAM.

---

161 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201), *supra* note 58, at Chapters II and IV.

162 International Centre for Missing & Exploited Children (ICMEC), *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 Nov. 14, 2018) (on file with the International Centre for Missing & Exploited Children).

The WePROTECT MNR[163] provides a clear and comprehensive roadmap for countries that seek to fully implement existing legislation and improve or develop their response to online child sexual exploitation.



[163] WePROTECT Model National Response, *supra* note 66, at 2.

Recommendations like those made by the Child Dignity Alliance Technology Working Group also provide critical guidance for those committed to protecting children globally by highlighting the need for progressive legislative action, investigative innovation, universal cooperation frameworks, and enforcement of laws, codes of conduct/practice, and minimum standards.[164]

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 perpetrators 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 well-aligned, these can serve as important motivators for a country to frame child protection as a national priority and drive legislation towards effective and lasting implementation.

[164] Child Dignity in the Digital World, *supra* note 45.

Global Legislative Review

✗ = No
✓ = Yes

Country	Legislation Specific to CSAM[165]	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses[166]	Simple Possession[167]	ISP Reporting[168]
Afghanistan	✗	✗	✗	✗	✗
Albania	✓	✓	✓	✓	✗
Algeria	✓	✓	✓[169]	✓	✗
Andorra	✓	✓	✓	✓	✗
Angola	✓	✓	✓	✓	✗

165 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.

166 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.

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

168 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.

169 Article 333 bis 1 of the Penal Code of Algeria imposes 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	✓	✓	✓[170]	✓	✗
Armenia	✓	✗	✓	✗	✗
Aruba	✓	✓	✓	✓	✗
Australia	✓	✓	✓	✓	✓
Austria	✓	✓	✓	✓	✗[171]
Azerbaijan	✓	✓	✗	✓	✗
Bahamas	✓	✓	✓	✓	✓
Bahrain	✓	✓[172]	✓	✓	✗

[170] 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.*

[171] 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).

[172] Article 10 of Law No. 60 of 2014 on Information Technology Crimes states that in the application of the provisions of this article, "child pornography" means the definition provided in the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Bangladesh	✓	✓	✓	✓	✗
Barbados	✓	✓	✓	✓	✗
Belarus	✓	✓	✓	✗ [173]	✗
Belgium	✓	✓	✓	✓	✓ [174]
Belize	✓	✓	✓	✓	✗
Benin	✓	✓	✓ [175]	✓	✗
Bhutan	✓	✓	✓ [176]	✓	✓
Bolivia	✓	✓	✓ [177]	✓	✗

[173] In 2017, the Ministry of Internal Affairs initiated, and this year continued to develop a program of comprehensive measures in the form of a "road map" in the field of combating crimes against sexual integrity and sexual freedom of minors, trafficking in child pornography, and the sale of children. The block of legislative measures stipulated by the "roadmap" implies, among other things, the criminalization of collecting (possessing) child pornography by making appropriate amendments and additions to the Criminal Code, as well as to the Code of Administrative Offenses of the Republic of Belarus. These legislative initiatives have been submitted to the Parliament and are under consideration by interested government bodies *(translated).* Email from Pavel Shidlovsky, Charge d'Affaires, a.i., Embassy of Belarus, Washington, D.C., to the International Centre for Missing & Exploited Children (Aug. 13, 2018) (on file with the International Centre for Missing & Exploited Children).

[174] 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).

[175] 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*.

[176] 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*.

[177] 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.*

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Bosnia-Herzegovina	✓	✗	✓[178]	✓	✗
Botswana	✓	✓	✓	✓	✗
Brazil	✓	✓	✓	✓	✗[179]
Brunei Darussalam	✓	✓	✓	✓	✗[180]
Bulgaria	✓	✓	✓	✓	✗
Burkina Faso	✓	✓	✓	✓	✗
Burundi	✓	✗	✗	✗	✗

178 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.*

179 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).

180 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
Cambodia	✓	✓	✓	✓	✗
Cameroon	✓	✓	✓	✓	✗
Canada	✓	✓	✓	✓	✓
Cape Verde	✓	✓	✓	✓	✗
Central African Republic	✓	✗	✗	✗	✗
Chad	✓	✓	✓[181]	✓	✗
Chile	✓	✓	✓	✓	✗

[181] 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[182]	✓ 183	✗	✓ 184	✗	✓ 185
Colombia	✓	✓	✓	✓	✓
Comoros	✓	✗	✗	✓	✗
Congo	✓	✓	✓ 186	✓	✗

182 CSAM legislation in Hong Kong differs from that in China. Legislation in **Hong Kong**:
- defines CSAM;
- criminalizes technology-facilitated CSAE 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, but has not yet fulfilled the remaining criteria.

183 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).

184 The 2004 Interpretation by the Supreme People's Court and the Supreme People's Protectorate applies to computer-facilitated offenses. Email from Chen Feng, Police Liaison Officer, Embassy of the People's Republic of China, Washington, D.C., to the International Centre for Missing & Exploited Children (Mar. 17, 2006) (on file with the International Centre for Missing & Exploited Children).

185 China's legislation explicitly stipulates the obligation of Internet Service Providers (ISP) to report obscene pictures, child pornography and other harmful information. For example, Article 7 of the *Decision of the Standing Committee of the People's Republic of China on Preserving Computer Network Security* provides that, any unit that engages in computer network business shall conduct activities in accordance with the law and, when it discovers illegal or criminal acts or harmful information in the computer network, shall take measures to suspend transmission of harmful information and report the matter to relevant authorities without delay. Article 20 of the *Implementation Measures Relating to the Temporary Provisions for the Management of Computer Information Network in China that Take Part in International Internetworks* stipulates that, if any ISP discovers harmful pernicious information including pornographic materials, it shall promptly report to the competent authorities, and effective measures shall be taken to prevent proliferation of the information. Letter from HU Binchen, Police Counselor, 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).

186 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*.

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Costa Rica	✓	✓	✓[187]	✓	✗
Côte d'Ivoire	✓	✓	✓	✓	✓
Croatia	✓	✓	✓	✓	✗
Cuba	✓	✗	✗	✗	✗
Cyprus	✓	✓	✓	✓	✗
Czech Republic	✓	✗	✓	✓	✗
Democratic Republic of Congo	✓	✓	✓[188]	✓	✗
Denmark	✓	✓	✓	✓	✗[189]

[187] 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.*

[188] 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.*

[189] 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	✓	✗	✓[190]	✗	✗
Dominica	✓	✓	✓	✓	✗
Dominican Republic	✓	✓	✓	✓	✗
Ecuador	✓	✓	✓	✓	✗[191]
Egypt	✓	✗	✓	✓	✗
El Salvador	✓	✓	✓	✓	✗
Equatorial Guinea	✗	✗	✗	✗	✗
Eritrea	✓	✗	✗	✗	✗
Estonia	✓	✗	✓[192]	✓	✓
Ethiopia	✓	✗	✓	✓	✓

[190] 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.*

[191] 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."

[192] 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.*

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Fiji	✓	✓	✓	✓	✗
Finland	✓	✓	✓[193]	✓	✗
France	✓	✓	✓	✓	✓
Gabon	✓	✓	✓	✓	✗
Gambia, The	✓	✗	✓[194]	✓	✗
Georgia	✓	✓	✓[195]	✓	✗[196]
Germany	✓	✓	✓	✓	✗[197]
Ghana	✓	✓	✓	✓	✗
Greece	✓	✓	✓	✓	✗

193 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.*

194 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.*

195 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.*

196 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).

197 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).

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Grenada	✓	✓	✓	✓	✗
Guatemala	✓	✓	✓[198]	✓	✗
Guinea	✓	✓	✓	✓	✓
Guinea Bissau	✗	✗	✗	✗	✗
Guyana	✓	✓	✓	✓	✓
Haiti	✓	✗	✗	✗	✗
Holy See	✓	✓	✓[199]	✓	✗[200]
Honduras	✓	✓	✓	✓	✗

198 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.*

199 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*.

200 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 on line 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).

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Hungary	✓	✓	✓ [201]	✓	✗ [202]
Iceland	✓	✓	✓	✓	✗
India	✓	✓	✓	✓	✓
Indonesia	✓	✗	✓ [203]	✓	✗
Iran	✗	✗	✗	✗	✗
Iraq	✗	✗	✗	✗	✗
Ireland	✓	✓	✓	✓	✗ [204]
Israel	✓	✗	✓ [205]	✓	✗

[201] 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.*

[202] 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).

[203] 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.*

[204] 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).

[205] 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
Italy	✓	✓	✓	✓	✓
Jamaica	✓	✓	✓	✓	✗
Japan	✓	✓	✓	✓	✗
Jordan	✓	✓	✓	✗	✗
Kazakhstan	✓	✗	✗	✗	✗
Kenya	✓	✓	✓	✓	✗ [206]
Kiribati	✓	✓	✓	✓	✗
Kosovo	✓	✓	✓	✓	✗
Kuwait	✗	✗	✗	✗	✗
Kyrgyzstan	✓	✗	✗	✗	✗
Laos	✓	✗	✓	✗	✓

[206] Article 30 of Kenya's Computer and Cybercrimes Bill, 2016, 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."

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Latvia	✓	✓	✓ 207	✓	✗ 208
Lebanon	✗	✗	✗	✗	✗
Lesotho	✓	✗	✗	✗	✗
Liberia	✓	✗	✓ 209	✓	✗
Libya	✗	✗	✗	✗	✗
Liechtenstein	✓	✓	✓	✓	✗ 210
Lithuania	✓	✗	✗	✓	✗
Luxembourg	✓	✗	✓	✓	✗

207 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.*

208 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).

209 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.*

210 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
Macedonia	✓	✓	✓	✓	✗
Madagascar	✓	✓	✓[211]	✓	✗
Malawi	✓	✓	✓	✓	✓
Malaysia	✓	✓	✓[212]	✓	✗
Maldives	✓	✗	✗	✗	✗
Mali	✓	✗	✗	✗	✗
Malta	✓	✓	✓	✓	✗
Marshall Islands	✓	✗	✗	✗	✗
Mauritania	✓	✗	✓	✓	✗
Mauritius[213]	✓	✗	✓	✗	✗
Mexico	✓	✓	✓	✓	✗
Micronesia	✗	✗	✗	✗	✗

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

212 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.*

213 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
Moldova	✓	✓	✓	✓	✗
Monaco	✓	✓	✓	✓	✗
Mongolia	✓	✗	✓	✗	✗
Montenegro	✓	✗	✓	✓	✗ [214]
Morocco	✓	✓	✓ [215]	✓	✗ [216]
Mozambique	✓	✗	✓ [217]	✓	✓
Myanmar	✓	✗	✓	✗	✗

[214] 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).

[215] 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.*

[216] 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).

[217] 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.*

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Namibia	✓	✗	✗ [218]	✗	✗
Nauru	✓	✓	✓	✓	✓
Nepal	✗	✗	✗	✗	✗
Netherlands	✓	✓	✓	✓	✗ [219]
New Zealand	✓	✓	✓	✓	✗ [220]
Nicaragua	✓	✓	✓	✓	✗
Niger	✓	✓	✗	✗	✗
Nigeria	✓	✓	✓	✓	✓

[218] Namibia is in the process of finalizing the Draft Electronic Transactions and Cybercrime Bill. The current draft criminalises child pornography. The Bill will also provide for a provision for online child pornography and hence offers the opportunity to address the gap in the current legislation strengthening the legislative framework. 'section 66 of the Bill provides for child pornography, which states that a person who intentionally – (a) produces child pornography for the purpose of its distribution through an information system (b) offers or makes available child pornography through an information system or in any other manner; (c) distributes or transmits child pornography through an information system or any other manner; (d) procures or obtains child pornography through a computer system or in any other manner for himself or herself or for another person; (e) possesses child pornography in a computer system or on a computer-data storage medium or in any other form; (f) obtains access, through information and communication technologies or in any other manner to child pornography, commits an offence and is on conviction liable to a fine not exceeding N$100 000 or to imprisonment for a period not exceeding 10 years or to both such fine and such imprisonment. Letter from Mr. I.V.K. Ndjoze, Permanent Secretary, Ministry of Justice of the Republic of Namibia, Windhoek, Namibia, to the International Centre for Missing & Exploited Children (Nov. 16, 2018) (on file with the International Centre for Missing & Exploited Children).

[219] 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).

[220] 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
North Korea	✗	✗	✗	✗	✗
Norway	✓	✓	✓	✓	✗
Oman	✓	✗	✓	✗	✗
Pakistan	✓	✓	✓	✓	✗
Palau	✓	✓	✓	✓	✗
Panama	✓	✓	✓	✓	✗ [221]
Papua New Guinea	✓	✓	✓	✓	✗
Paraguay	✓	✓	✓ [222]	✓	✗ [223]
Peru	✓	✗	✓	✓	✗
Philippines	✓	✓	✓	✓	✓

[221] 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).

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

[223] 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."

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Poland	✓	✗ [224]	✓	✓	✗ [225]
Portugal	✓	✗	✓ [226]	✓	✗
Qatar	✓	✗	✓	✓	✓
Romania	✓	✓	✓	✓	✗ [227]
Russia	✓	✓	✓	✗	✗
Rwanda	✓	✗	✓	✗	✓
St. Kitts & Nevis	✓	✓	✓	✗	✗
St. Lucia	✓	✓	✓	✓	✗
St. Vincent & the Grenadines	✓	✓	✓	✓	✗
Samoa	✓	✓	✓	✓	✗

[224] 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).

[225] 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).

[226] 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.*

[227] 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).

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
San Marino	✓	✓	✓	✗	✗
Sao Tome & Principe	✓	✗	✓[228]	✓	✗
Saudi Arabia	✓	✗	✓	✗	✗[229]
Senegal	✓	✓	✓	✓	✗
Serbia	✓	✓	✓[230]	✓	✗
Seychelles	✓	✗	✓	✓	✗
Sierra Leone	✓	✓	✓[231]	✓	✗
Singapore[232]	✓	✗	✓	✗	✗

[228] 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.*

[229] 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).

[230] 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*.

[231] 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.*

[232] A major review of the Penal Code is underway. A key area under review is whether there should be dedicated laws to deal with activities related to child abuse material – from the making of such material to possession and distribution of the material. A related area under review is whether such offences should attract more severe penalties to send a stronger deterrent message. The review proposals will be tabled for public consultation in late 2018. Letter from His Excellency Ashok Kumar Mirpuri, Ambassador of the Republic of Singapore, Embassy of the Republic of Singapore, Washington, D.C., to the International Centre for Missing & Exploited Children (Aug. 31, 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
Slovak Republic	✓	✓	✓	✓	✗
Slovenia	✓	✗	✓	✓	✗
Solomon Islands	✓	✓	✗	✓	✗
Somalia	✗	✗	✗	✗	✗
South Africa	✓	✓	✓	✓	✓
South Korea	✓	✓	✓	✓	✗ [233]
South Sudan	✓	✗	✗	✗	✗
Spain	✓	✓	✓	✓	✗
Sri Lanka	✓	✗	✗	✓	✓
Sudan	✓	✓	✗	✓	✗
Suriname	✓	✓	✓	✓	✗
Swaziland	✓	✓	✓	✓	✓

[233] 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
Sweden	✓	✓ 234	✓ 235	✓	✗ 236
Switzerland	✓	✓	✓	✓	✗ 237
Syria	✗	✗	✗	✗	✗
Tajikistan	✓	✗	✓	✗	✗

234 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)*

235 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.*

236 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).

237 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).

Country	Legislation Specific to CSAM	"Child Sexual Abuse Material" Defined	Technology-Facilitated CSAM Offenses	Simple Possession	ISP Reporting
Tanzania	✓	✓	✓	✗	✓
Thailand	✓	✓	✓	✓	✗
Timor Leste	✓	✓	✓[238]	✓	✗
Togo	✓	✓	✓[239]	✗	✓
Tonga	✓	✓	✓	✓	✗
Trinidad & Tobago	✓	✓	✓	✓	✗
Tunisia	✗	✗	✗	✗	✗
Turkey	✓	✗	✗	✓	✓
Turkmenistan	✓	✗	✗	✗	✗
Tuvalu	✗	✗	✗	✗	✗
Uganda	✓	✓	✓	✓	✓
Ukraine	✓	✗	✓	✗	✗

[238] 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*.

[239] 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
United Arab Emirates	✓	✓	✓	✓	✓
United Kingdom[240]	✓	✓	✓	✓	✗ 241
United States	✓	✓	✓	✓	✓
Uruguay	✓	✓	✓ 242	✗	✗
Uzbekistan	✓	✗	✗	✗	✗
Vanuatu	✓	✓	✓	✓	✗
Venezuela	✓	✗	✓	✗	✗

240 For the purposes of this report, the United Kingdom includes England and Wales.
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.
In 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.

241 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).

242 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
Vietnam	✓	✗	✗	✗	✗
Yemen	✗	✗	✗	✗	✗
Zambia	✓	✗	✓	✓	✗
Zimbabwe	✓	✓	✗	✗	✗

Conclusion

For more than a decade, ICMEC's research regarding the status of anti-CSAM legislation around the world has demonstrated that slow and steady progress is being made. Various international and regional legal instruments are in place, which have helped raise awareness and attach new urgency to this cause. With this increased awareness has come desire and resolve by many to contribute to a lasting solution. Out of this resolve, new collaborative initiatives have emerged, bringing together child protection professionals from all sectors working toward the same goal – protecting children from sexual violence in all forms. Countless new legislative improvements are just one piece of the puzzle, albeit an important one. More countries must take action if we are to secure a safer future for the world's children. Combating CSAM at home and abroad is a daunting task, but harmonized laws, technological innovations, and continual collaborative efforts can help us make children worldwide safer.

Research.ICMEC.org | Donate.ICMEC.org

**Formerly "Child Pornography: Model Legislation & Global Review"*

International Centre
FOR MISSING & EXPLOITED CHILDREN

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