

CHILD PORNOGRAPHY:

Model Legislation & Global Review

8th Edition, 2016



International Centre
FOR MISSING & EXPLOITED CHILDREN

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

Child Pornography:
Model Legislation & Global Review

Copyright © 2016, International Centre for Missing & Exploited Children (ICMEC)

Eighth 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.*

We also appreciate the past support of “The Woods” Charitable Foundation (A Ware Family Foundation) for this project.

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, “The Woods” Charitable Foundation, 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 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 thinkers and opinion leaders, and collaborating with partners in the field to identify and measure threats to children and ways ICMEC can advocate for change.

Our Mission

For more than 15 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 day to make the world safer for children by eradicating child abduction, sexual abuse and exploitation. To this end, **ICMEC's mission is to advocate, train and collaborate to protect the world's children.**

- **ADVOCATE:** ICMEC proposes changes to laws, treaties and systems based on rigorous research and the latest technology to better protect children worldwide.
- **TRAIN:** ICMEC provides 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.
- **COLLABORATE:** ICMEC builds international networks of professionals across disciplines to anticipate issues, identify gaps, and develop cross-cutting solutions.

Table of Contents

Foreword	Page i
Acknowledgements	Page ii
Executive Summary	Page iii
Model Legislation	Page 1
<i>Definitions</i>	Page 1
<i>Offenses</i>	Page 2
<i>Mandatory Reporting</i>	Page 5
<i>Data Retention in the Broad Sense</i>	Page 6
<i>Sanctions and Sentencing</i>	Page 9
Regional and International Law	Page 11
<i>Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography</i>	Page 12
<i>Convention on Cybercrime</i>	Page 13
<i>Convention on the Protection of Children Against Sexual Exploitation and Abuse</i>	Page 14
<i>EU Directive on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography</i>	Page 15
Implementation	Page 17
Global Legislative Review	Page 18
<i>Afghanistan – Angola</i>	Page 18
<i>Antigua & Barbuda – Bahrain</i>	Page 19
<i>Bangladesh – Bosnia-Herzegovina</i>	Page 20
<i>Botswana – Burundi</i>	Page 21
<i>Cambodia – Chile</i>	Page 22
<i>China – Congo</i>	Page 23
<i>Costa Rica – Denmark</i>	Page 24
<i>Djibouti – Ethiopia</i>	Page 25
<i>Fiji – Greece</i>	Page 26
<i>Grenada – Honduras</i>	Page 27
<i>Hungary – Israel</i>	Page 28
<i>Italy – Laos</i>	Page 29
<i>Latvia – Liechtenstein</i>	Page 30
<i>Lithuania – Marshall Islands</i>	Page 31
<i>Mauritania – Montenegro</i>	Page 32
<i>Morocco – Nepal</i>	Page 33
<i>Netherlands – Palau</i>	Page 34
<i>Panama – Poland</i>	Page 35
<i>Portugal – Samoa</i>	Page 36
<i>San Marino – Slovenia</i>	Page 37
<i>Solomon Islands – Swaziland</i>	Page 38
<i>Sweden – Syria</i>	Page 39
<i>Tajikistan – Turkey</i>	Page 40
<i>Turkmenistan – United States</i>	Page 41
<i>Uruguay – Zimbabwe</i>	Page 42
Conclusion	Page 43

Foreword

Every year, countless numbers of children are sexually exploited or abused around the world. Modern technology, a gift in so many ways, also has been used to facilitate crimes against children, and sadly, to share repeatedly and indelibly in cyber-space evidence of a child's victimization.

More than a decade ago, ICMEC recognized the need to gain a better understanding of the global legislative landscape as it related to child pornography. After careful consideration and consultation, we developed model legislation in an effort 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 this report in 2006, 127 countries have refined or implemented new anti-child pornography legislation. While a positive trend, there is a critical need for continuing our efforts, as this report will demonstrate in subsequent pages.

It is important to note that the legislative review accompanying our model legislation is not a scorecard or a scold, but rather 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 resembles more of a menu of concepts that can be applied universally, as opposed to actual statutory language. With this latest launch, we will continue our efforts to improve the legislative landscape and strengthen child protection efforts around the world.

Data retention and/or preservation have increasingly become a point of discussion in the sphere of child online protection. Such provisions are needed for the purpose of ensuring that digital evidence is available to law enforcement when needed for the investigation and prosecution of illicit online activity. Accordingly, we have added data retention in a broad sense to our review.

ICMEC colleague Jessica Sarra conceived of this project and delivered the first several editions for publication, creating an enduring standard of excellence for our research and global outreach. Sandra Marchenko subsequently took the helm as Director of our Koons Family Institute on International Law & Policy and has ensured its continuing relevancy and impact. They each have been supported by an army of graduate-level 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. It is our conviction that the soulless horror of online child exploitation can be eradicated – if only we all work together, relentlessly, and with every tool available, to put an end to it. We hope this report spurs conversation and action and a commitment to redouble our collective efforts to protect the world's children.

We hope this report will be studied, and its data applied toward the goal of making the world a safer place for 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 pornography for the 8th 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 interns of The Koons Family Institute on International Law & Policy who have worked tirelessly to produce this report: Devin Barrett, *Legal Intern*; Kamilla Bischof, *Research Intern*; Rowena Carlton, *Legal Intern*; Genette Gaffney, *Legal Intern*; Colleen Haggerty, *Research Intern*; Didier Houttequiet, *Legal Intern*; Teri Husfloen, *Research Intern*; Annem Khan, *Legal Intern*; Kodjo Kumi, *Legal Intern*; Gina Lee, *Legal Intern*; Xiangen Li, *Legal Intern*; Laura Murchie, *Legal Intern*; Victoria Sepavich, *Research Intern*; and Alissandra Young, *Legal Intern*; 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 15 November 2015.

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 materials (child pornography). The Internet not only made this both easy and inexpensive to do, but it also made it extremely low-risk, enormously profitable, and unhindered by geographical boundaries.

There has long been a common misperception that child pornography 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. The Internet Watch Foundation (IWF) in the United Kingdom reported that, out of all reports of child pornography received by IWF in 2014, 80% of the victims appeared to be children 10 years of age or younger, and 4% were 2 years of age or younger.¹ Moreover, IWF reported that 43% of images showed sexual activity between adults and children including rape or sexual torture.²

Similar findings are also confirmed by an earlier study in Canada, which found that 82.1% of images analyzed by Cybertip.ca depicted very young, pre-pubescent children.³ It further showed that 68.5% of children abused through extreme sexual assaults (i.e., bestiality, bondage, torture) were under 8 years of age.⁴

INHOPE, the International Association of Internet Hotlines, reported that, in 2013, of the 1.2 million reports received by their 49 member hotlines, 19% were child sexual abuse images depicting pubescent children; 71% were of pre-pubescent children; and 10% were of infants.⁵

A 2012 statement by the National Center for Missing & Exploited Children (NCMEC) in the United States showed similar results: of the images most frequently submitted to NCMEC, 24% were of pubescent children; 76% were of pre-pubescent children; and 10% were of infants and toddlers.⁶ Of

¹ Internet Watch Foundation, *Annual Report 2014* 9, at https://www.iwf.org.uk/assets/media/annual-reports/IWF_Annual_Report_14_web.pdf (last visited Sep. 15, 2015) [hereafter *IWF 2014*] (on file with the International Centre for Missing & Exploited Children).

² *Id.*

³ Canadian Centre for Child Protection, *Child Sexual Abuse Images: Summary Report 1*, Nov. 2009, at https://www.cybertip.ca/pdfs/CTIP_ChildSexualAbuse_Summary_en.pdf (last visited Nov. 30, 2015) (on file with the International Centre for Missing & Exploited Children).

⁴ *Id.* at 2.

⁵ International Association of Internet Hotlines, *INHOPE Annual Report 2013-2014* 25, at http://www.inhope.org/Libraries/Annual_reports/INHOPE_Annual_Report_2013.sflb.ashx (last visited Nov. 23, 2015) [hereafter *IWF 2014*] (on file with the International Centre for Missing & Exploited Children).

⁶ Michelle Collins, *Federal Child Pornography Offenses* 4, Testimony before the U.S. Sentencing Commission (Feb. 15, 2012), at http://www.ussc.gov/sites/default/files/pdf/amendment-process/public-hearings-and-meetings/20120215-16/Testimony_15_Collins.pdf (last visited Nov. 30, 2015) (on file with the International Centre for Missing & Exploited Children).

these images, 84% depicted oral copulation; 76% depicted anal and/or vaginal penetration; 52% depicted the use of foreign objects or sexual devices; 44% contained images depicting bondage and/or sadomasochism; and 4% depicted bestiality.⁷

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. Child pornography 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.

Little more than a decade ago, child pornography was a multi-billion dollar commercial enterprise and was among the fastest growing businesses on the Internet. Today, the commercial trade of child pornography online has been significantly reduced due to a variety of successful efforts to combat its growth.⁸ There has, however, been an increase in the trade of this illicit content between individuals and groups via peer-to-peer networks.⁹ The problem has proven to be a persistent one, and strong anti-child pornography legislation is needed in every country in order to combat it. In spite of this, laws addressing child pornography around the world are often weak or inconsistent, or there are no laws in place at all.

More than ten years ago, the International Centre for Missing & Exploited Children (ICMEC) recognized the global need to gain a better understanding of existing legislation addressing child pornography and to gauge where the issue stood on national political agendas. In response, we undertook examining 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. The first report reviewed legislation addressing the issue of child pornography in the then 184 INTERPOL member countries. The report continues to be updated regularly – now in its 8th Edition, the report includes 196 countries in the review. The review has become an internationally-utilized tool for policymakers, law enforcement agencies, child protection experts and organizations, industry partners, and others.

The 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 child pornography;
- (2) provides a definition of child pornography;
- (3) criminalizes computer-facilitated offenses;
- (4) criminalizes the knowing possession of child pornography, regardless of the intent to distribute; and
- (5) requires Internet Service Providers (ISPs)¹⁰ to report suspected child pornography to law enforcement or to some other mandated agency.

⁷ *Id.* at 5.

⁸ United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime 36 (2013), at https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (last visited Jan. 11, 2016) (on file with the International Centre for Missing & Exploited Children).

⁹ Wolak, J., 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://dx.doi.org/10.1016/j.chiabu.2013.10.018> (last visited Jan. 11, 2016) (on file with the International Centre for Missing & Exploited Children).

¹⁰ For purposes of this report, the term “Internet Service Provider” (ISP) includes electronic communication service providers and remote computing service providers.

In this 8th Edition report, we have introduced a new point of review to see if national legislation:

(6) requires ISPs to develop and implement data retention and preservation provisions.

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. Thus, we have added data retention in a broad sense to our review.

Realizing the importance of taking into consideration varying cultural, religious, socio-economic, and political norms, our model legislation resembles more of a menu of concepts that can be applied in all countries throughout the world, as opposed to actual statutory language. The model legislation consists of 11 fundamental topics/provisions that are essential to a comprehensive legislative strategy to combat child pornography.¹¹ It is divided into five parts: (1) Definitions; (2) Offenses; (3) Mandatory Reporting; (4) Data Retention and Preservation; and (5) Sanctions and Sentencing. This is followed by an overview of related regional and international law, as well as 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 child pornography does not mean that other forms of child sexual exploitation and child abuse are not criminalized.

Methodology

The review process undertaken has remained much the same each year. Open source research into national anti-child pornography legislation is conducted in-house with the help of a team of legal research interns. Primary sources of information include: LexisNexis; government submissions to 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 Chiefs 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 our research results. Upon receipt of new or corrected information, the information is reviewed and, if warranted, is inserted into the report. In some cases, the response or an excerpt may be included in the footnotes in the global review portion of the report to ensure that the information is available even when ICMEC determined that the criteria had not been met.

¹¹ The 11 fundamental topics are listed on page vii.

Results

The results of this report, along with comparative information from the 1st Edition and 7th Edition reports, are presented in the table below.

	1 st Edition (2006)*	7 th Edition (2012)	8 th Edition (2016)
Legislation sufficient to combat child pornography offenses (<i>sufficient means it meets at least criteria 1-4</i>)	<p>27 countries had sufficient legislation</p> <ul style="list-style-type: none"> ▪ 5 countries met all 5 criteria ▪ 22 countries met all but the last criteria (pertaining to ISP reporting) 	<p>69 countries had sufficient legislation</p> <ul style="list-style-type: none"> ▪ 11 countries met all 5 of the criteria ▪ 58 countries met all but the last criteria (pertaining to ISP reporting) 	<p>82 countries have sufficient legislation</p> <ul style="list-style-type: none"> ▪ 11 countries meet the first 5 criteria ▪ 71 countries meet all but the 5th criteria (pertaining to ISP reporting) <p><i>(A 6th criteria was added for this report.)</i></p>
No legislation at all specifically addressing child pornography	95 countries	53 countries	35 countries
<i>Of the remaining countries that do/did have legislation specifically addressing child pornography:</i>			
Do not define child pornography	54 countries	60 countries	60 countries
Do not provide for <u>computer-facilitated offenses</u>	27 countries	21 countries	26 countries
Do not criminalize the knowing <u>possession</u> of child pornography, regardless of intent to distribute	41 countries	47 countries	50 countries
Have <u>data retention</u> legislation (broadly) that requires ISPs to retain (i.e., keep, collect) digital user data to ensure access to the data for prosecuting online criminal activity			79 countries
*The 1 st edition of this report looked at the legislation of the 184 INTERPOL member countries. Beginning from the 6 th Edition, the report was expanded to look at the legislation of 196 countries. This difference may reduce the comparative value between the 1 st Edition and later editions of the report.			

Terminology

While the term “child pornography” implies conventional pornography with child subjects and does not aptly describe the true nature and extent of sexually exploitive images of child victims, use of this term throughout the report should not be taken to imply that children “consented” to any sexual acts depicted in any images.¹² The term is retained because it is the expression most readily recognized by the public at large, at this point in time, to describe this form of child sexual exploitation.¹³ In addition, child pornography is the term most frequently used in legislation around the world addressing the issue. It should be noted that there has been recent movement globally towards the use of other terms, including “child sexual abuse material,” “child sexual abuse content,” and “child sexual exploitative material,” which more clearly highlight the exploitation that occurs.

For purposes of this report, “child pornography” 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,”¹⁴ as well as the use of a child to create such a representation.

Topics Addressed

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

- (1) Defining “child” for the purposes of child pornography as anyone under the age of 18, regardless of the age of sexual consent;
- (2) Defining “child pornography,” and ensuring that the definition includes computer- and Internet-specific terminology;
- (3) Creating offenses specific to child pornography in the national penal code, including criminalizing the knowing possession of child pornography, 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 child pornography;
- (5) Penalizing those who make known to others where to find child pornography;
- (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) Creating data retention and/or preservation policies/provisions;
- (10) Addressing the criminal liability of children involved in pornography; and
- (11) Enhancing penalties for repeat offenders, organized crime participants, and other aggravating factors to be considered upon sentencing.

¹² 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) [hereinafter *Child-Pornography Possessors*] (on file with the International Centre for Missing & Exploited Children).

¹³ *Id.*

¹⁴ *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 [hereafter *Optional Protocol*] (on file with the International Centre for Missing & Exploited Children).

Model Legislation

A comprehensive legislative strategy that is aimed at combating child pornography 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 five parts:

- (1) Definitions;
- (2) Offenses;
- (3) Mandatory Reporting;
- (4) Data Retention and Preservation; and
- (5) Sanctions and Sentencing.

Definitions

Define “child,” for the purposes of child pornography, 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 child pornography.

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 his/her 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 child pornography legislation, should be defined as “anyone under the age of 18 years.”

Define “child pornography” and include computer- and Internet-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, child pornography should be adequately defined in national legislation. 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 pornography” 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.

Moreover, it is imperative that, with the advent of the Internet and new technology, mention be made of all the forms child pornography 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 child pornography can be distributed, including via computer networks and the Internet; and all the ways in which child pornography can be possessed, including by simply knowingly viewing an image on the Internet or knowingly downloading an image to one’s computer.

Offenses

Incorporate child pornography offenses into the penal code.

Mere labor legislation that bans the worst forms of child labor, including child pornography, 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 child pornography (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 child pornography as an evil that affects child welfare, child pornography is a crime and must be recognized as such. Child pornography 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 child pornography,” for purposes of this report, unless there is also a sentencing enhancement in the national legislation that increases penalties for those who commit pornography offenses against children. A sentencing enhancement for child victims makes the necessary distinction between adult and child pornography.

Criminalize the knowing possession of child pornography, regardless of the intent to distribute.

Every image of child pornography that is acquired encourages the further growth of this illicit industry and contributes to the development of alarming new trends such as “custom” child pornography – the sale of images of child rape created to order for the consumer and “real-time” child pornography, for which subscribers pay to watch the live-streamed rape of children as it occurs.¹⁵

A 2011 study in the United States found that 41% of arrested child pornography possessors were “dual offenders,” who sexually victimized children and possessed child pornography.¹⁶ One out of every six cases that began with an investigation of child pornography possession involved a dual offender who had also sexually abused a child or attempted to do so, which suggests that there may be a correlation between the knowing simple possession of child pornography and committing sexual abuse upon a child.¹⁷ Therefore, criminalizing the knowing possession of child pornography may not only curb industry growth, but also prevent further incidents of sexual abuse.

Criminalize knowingly downloading or knowingly viewing child pornography images on the Internet and using the Internet to distribute child pornography.

Offenders use the Internet to view, download, distribute, acquire, and trade child pornography on a daily basis. Therefore, as stated earlier, it is imperative that specific mention be made, in some way, of computer or Internet technology being used to make, view, possess, distribute, or in some other way commit a child pornography-related offense.

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

¹⁵ 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. 30, 2015) (on file with the International Centre for Missing & Exploited Children).

¹⁶ 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).

¹⁷ *Id.*

Penalize those who make known to others where to find child pornography.

Offering information on where to find child pornography 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 child pornography) through offering advice or taking actions that facilitate knowingly possessing or knowingly downloading illegal content should be penalized.

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

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

There can be no transfer of consent from the parent or guardian to the child to participate in child pornography. 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 child pornography.

Turning a child over to the pornography 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 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 18.¹⁸ The process of grooming represents the initial actions taken by an individual to sexually abuse a child by developing a relationship of trust with a child victim. Sex offenders use a variety of means such as 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 pornography (adult or child) to the victim to lower the child's inhibitions, desensitize the child to sexual activity and normalize this behavior, and teach the child sexual behaviors.¹⁹ Showing pornographic images and videos to the child can also 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.²⁰

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 and regions communicate with strangers online and unwittingly share personal information, which

¹⁸ 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 Oct. 27, 2015) (on file with the International Centre for Missing & Exploited Children) (emphasis added).

¹⁹ C. Emmanuel Ahia et al., *Protecting Children from Online Sexual Predators: Technological, Psychoeducational, and Legal Considerations*, 35 PROFESSIONAL PSYCHOLOGY: RESEARCH AND PRACTICE 67 [hereinafter *Protecting Children from Online Sexual Predators*] (on file with the International Centre for Missing & Exploited Children).

²⁰ 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).

can be one of the first steps in a grooming relationship.²¹ Grooming relationships can have a personal sexual intent or commercial exploitation intent and thus often precede the creation or distribution of child pornography.

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.²² 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. In the United Kingdom, for instance, the Child Exploitation and Online Protection Centre found that only 7% of the 1,145 online grooming cases investigated in the UK in 2012 involved the intent to meet a child offline.²³ 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 have already been groomed and exploited online.²⁴

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.

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 his/her first misstep that even incomplete crimes against children will not be tolerated.

²¹ 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 Feb. 26, 2013) (on file with the International Centre for Missing & Exploited Children).

²² Dr. Mike McGuire and Samantha Dowling, *supra* note 18, 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).

²³ *Alarming New Trend in Online Sexual Abuse*, CEOP Command, Feb. 4, 2013, at <http://ceop.police.uk/Media-Centre/Press-releases/2013/ALARMING-NEW-TREND-IN-ONLINE-SEXUAL-ABUSE/> (last visited Nov. 30, 2015) (on file with the International Centre for Missing & Exploited Children).

²⁴ 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. 30, 2015) (on file with the International Centre for Missing & Exploited Children).

Mandatory Reporting

Require healthcare and social services professionals, teachers, law enforcement officers, photo developers, IT professionals, ISPs, credit card companies, and banks to report suspected child pornography to law enforcement or another agency.

There are three classes of individuals and organizations that should be required to report suspected child pornography activities and offenses to law enforcement or another mandated agency:

- (1) individuals who, in their everyday, professional capacity, come into contact with children and owe a certain duty of care to those children;
- (2) individuals who, in their everyday, professional capacity, do not come into contact with children, but may potentially be exposed to child pornography as a result of their job responsibilities; and
- (3) organizations or corporations the services of which are being used to proliferate child pornography activities and which, as a result, should exercise a certain amount of industry responsibility / corporate citizenship / corporate social responsibility in their day-to-day business operations.

The first group is rather self-explanatory. Members include, but are not necessarily limited to, healthcare and social services professionals, law enforcement officers, and teachers, school counselors, and others in child serving professions. Based on daily interactions with children, these individuals may develop well-founded suspicions about potential child victims.

The second group is consisted primarily of IT professionals who may accidentally discover child pornography images during the course of their routine work. Not long ago, this group was comprised of photo developers who may have come across these images while processing film, but with the increased use of technology, these images are now more likely to be found in digital form. IT professionals may find child pornography while repairing or servicing a computer, 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.

Finally, the last group consists mostly of ISPs, credit card companies, banks, and the payments industry. In many circumstances, law enforcement would be unaware of many child pornography offenses if ISPs did not report them (either voluntarily or under legal obligation). Given the heavy traffic in child pornography over the Internet, ISPs are in an almost ideal position to report suspected child pornography offenses to law enforcement through content management and 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 child pornography, including the transmission of images, to law enforcement or another designated agency.

With regard to members of the financial industry, the ability to use credit cards, money transfers, digital currency, and other payment methods to purchase child pornography has made it easier than ever to obtain child pornography; moreover, distribution over the Internet 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 child pornography transactions to law enforcement or another mandated agency when the transactions are discovered.

Data Retention in the Broad Sense

Since the last edition of this report was published, discussion regarding data retention and data preservation has increased as law enforcement has turned much of its efforts towards targeting and identifying those who distribute, purchase, possess, and view child pornography online. In order to effectively conduct investigations in these cases, law enforcement regularly requires access to computer data, but may discover that it has been deleted, making it more difficult or even impossible to find and prosecute the perpetrator.²⁵ Individual ISPs generally have the ability and technological capacity to retain and preserve their users' data in order to make it available for the purposes of criminal prosecution.

In this context, there are two types of computer data: content-based and non-content based. **Content-based data** includes information such as 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.²⁶ **Non-content based data**, on the other hand, includes **subscriber information** (data that helps identify the subscriber), **traffic data** on the route, time, size, type, date, duration, destination, and source of a communication,²⁷ as well as **location data**.²⁸

In light of the recent attention to this issue, we expanded our research for this edition with a sixth criterion on data retention. Data retention broadly means the obligation for ISPs to retain computer data for a specific period of time. This could be a legal obligation to retain non-content data (i.e., IP address, date, time, and time zone for emails sent; full email address) for all users from the moment of collection (**data retention**) and/or an obligation to preserve stored data with probative value of an identified user who is currently under investigation after a request by law enforcement (**data preservation**). Guidelines for data retention and data preservation vary widely by country, industry, and type of data. However, as a global trend, we observed that countries with data collection regulations opt for one of these two systems, or implement both.²⁹

It is imperative that law enforcement have the proper tools to fight online crimes and protect children from abuse, molestation, and exploitation. Data retention in the broad sense is essential to law enforcement in order to be able to identify and prosecute offenders. The primary purpose for adopting data preservation legislation 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.³⁰ However, a strict data preservation system has limitations. If ISPs are not obliged to retain data for a set period of time and immediately or shortly after its collection the data is deleted, investigators may be faced with the consequence of requesting the data too late.³¹ The procedures for law enforcement to

²⁵ 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).

²⁶ 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).

²⁷ *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 Oct. 27, 2015) (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).

²⁸ *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 Oct. 27, 2015) [hereafter EU Data Retention Directive] (on file with the International Centre for Missing & Exploited Children).

²⁹ 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.

³⁰ Department of Justice of Canada, *Lawful Access FAQ* 4 (2005) (on file with the International Centre for Missing & Exploited Children).

³¹ Jason Weinstein, *supra* note 25, at 3.

obtain the proper authorization or warrant, as well as the internal procedures ISPs must follow to grant access to stored data vary greatly and can be slow. According to the International Association of Chiefs of Police, “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.”³² Accordingly, the main purpose of data retention is to secure the availability of sufficient data to law enforcement for a standard period of time.

There is growing international awareness of the importance of developing effective data retention and preservation policies. These policies must be consistent across providers in terms of the type of data retained and preserved, the period of time for which it must be retained and preserved, and for what purpose it must be supplied to law enforcement. The Council of Europe Convention on Cybercrime, adopted in 2001, incorporates recommendations for data preservation measures.³³ In 2006, the European Parliament and Council of the European Union issued a Directive focused on the retention of non-content based data.³⁴ The objective of the Directive was to harmonize the obligations on providers to retain certain data (traffic and location or “non-content” data), by requiring all Member States to adopt a standard set of data retention policies.³⁵ 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.”³⁶ However, the Directive was declared invalid by the European Court of Justice (ECJ) in April 2014. 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,³⁷ 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.³⁸ Far from abandoning the concept of data retention, the ECJ suggests that EU Member States that choose to alter existing national legislation or introduce new laws on data retention should do so in contemplation of its ruling and recommendations.³⁹

An equally robust conversation about data retention has been occurring in the United States. The U.S. Department of Justice sought mandatory data retention noting that, “[d]ata retention is fundamental to the Department’s work in investigating and prosecuting almost every type of crime.”⁴⁰ During a hearing of the House of Representatives Committee on Judiciary Subcommittee on Crime, Terrorism, and Homeland Security, the need for Congress to strike an appropriate balance between privacy and police concerns was highlighted.⁴¹ Canada has reconciled these concerns by taking an innovative approach. Rather than requiring ISPs to retain or preserve user data for all users, Canadian legislation ties the requirement to preserve all computer data to the ISPs obligation to notify law enforcement of child pornography offenses on their network. ISPs are then obliged to

³² *Id.*

³³ *Convention on Cybercrime*, *supra* note 27. For additional information on the *Convention on Cybercrime*, see page 13 of the Regional and International Law section of this report.

³⁴ EU Data Retention Directive, *supra* note 28.

³⁵ *Id.*

³⁶ *Id.* at recitals (7) and (9).

³⁷ Judgment of the European Court of Justice (Grand Chamber), 8 April 2014, in joined Cases C-293/12 and C-594/12, at 43-44, 49 and 51 (on file with the International Centre for Missing & Exploited Children).

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

³⁹ Judgment of the European Court of Justice (Grand Chamber), *supra* note 37, paragraphs 39-45.

⁴⁰ Declan McCullagh, *Justice Department seeks mandatory data retention*, Jan. 24, 2011, at <http://www.cnet.com/news/justice-department-seeks-mandatory-data-retention> (last visited Oct. 28, 2015) (on file with the International Centre for Missing & Exploited Children).

⁴¹ Jason Weinstein, *supra* note 25, at 5.

“preserve all computer data related to the notification that is in their possession or control for 21 days after the day on which the notification is made.”⁴² Following the 21-day period, the data must be destroyed, unless there is a judicial order compelling the ISP to keep the data for an additional period of time.⁴³

Based on our research, the following good practices have come to the forefront:⁴⁴

Data Retention

- Promoting the retention of subscriber information, traffic data, and location data for a minimum of 6 months;
- Supporting the implementation of a legal framework that limits the scope and application of data retention;
- Encouraging differentiation as to the data that must be collected; and
- Requiring sufficient guarantees for the protection of the data against unlawful access and abuse.

Data Preservation

- Ensuring that ISPs have a process in place for the prompt response to subpoenas or law enforcement requests for data;
- Obliging ISPs to respond to preservation orders for data as soon as practicable; and
- Requiring that requested data be preserved for no less than 90 days with the possibility to request an extension.

Effective data retention and preservation frameworks will include legal provisions that harmonize the obligations of ISPs, while recognizing that ISPs have differing capabilities, technologies, and resources available. Increased communication and cooperation between law enforcement organizations and ISPs should also be encouraged and supported.⁴⁵

We acknowledge that data retention and data preservation are not yet settled matters, but we strive to call attention to this important issue. We aim to provide a balanced approach, considering both the need for such provisions in the realm of child online protection, as well as the need to ensure privacy protections for Internet users.

⁴² Bill C-22 respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service, Sections 2 and 3 (Mar. 23, 2011), at <http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=5075713&File=35#2> (last visited on Nov. 19, 2015) (on file with the International Centre for Missing & Exploited Children).

⁴³ *Id.* at Section 4.

⁴⁴ Additional information about the good practices represented in this diagram can be found in the following sources: *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; EU Data Retention Directive, *supra* note 28, at Article 1; Judgment of the European Court of Justice (Grand Chamber), *supra* note 37.

⁴⁵ 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).

Sanctions and Sentencing

Address the criminal liability of children involved in pornography.

There should be no criminal liability for children involved in pornography, 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 he/she is a **child victim**.

Criminal liability must focus on the adult offender, who is responsible for the exploitation of the child, and on the crimes he/she committed against that child.

Legal provisions should be enacted that would 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-child pornography legislation should carry strict sentences that will be enforced, thereby guaranteeing a true deterrent effect.⁴⁶ Mere fines and misdemeanor classifications are not enough.

Sentencing provisions should take into account aggravating factors and enhancements.⁴⁷ Aggravating factors may include the number of images manufactured, produced, distributed, and possessed; the severity of the offender's existing criminal record; the sexual violence toward the children (including rape, torture, and bondage) being depicted in the images that were manufactured, produced, distributed, and possessed; and any potential threat or risk the offender may pose to the community upon release.

Media outlets from across the world have reported that criminals other than sex offenders, including terrorists, organized criminals, and gangs, have been found with child pornography. While some criminals may obtain child pornography for personal interest, accounts have suggested that these criminals may have new uses for child pornography. Terrorists have reportedly manufactured child pornography to send concealed messages and data⁴⁸ and finance their activities.⁴⁹ Likewise, organized criminals and gangs involved in human trafficking may produce pornographic images of their victims to generate additional revenue, blackmail victims into compliance, and advertise commercial sexual services.⁵⁰ These examples suggest that child pornography 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.

⁴⁶ 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) [hereinafter *Prostitution of Children and Child-Sex Tourism*] (on file with the International Centre for Missing & Exploited Children).

⁴⁷ *Id.*

⁴⁸ Richard Kerbaj and Dominic Kennedy, *Link Between Child Porn and Muslim Terrorists Discovered in Police Raids*, TIMES ONLINE, Oct. 7, 2008 [hereinafter *Child Porn and Terrorists*] (on file with the International Centre for Missing & Exploited Children).

⁴⁹ 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 Oct. 1, 2015) (on file with the International Centre for Missing & Exploited Children); see also *Child Porn and Terrorists*, *supra* note 48.

⁵⁰ 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 Oct. 7, 2015) (on file with the International Centre for Missing & Exploited Children).

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 child pornography activities.⁵¹ 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.⁵²

⁵¹ *Prostitution of Children and Child-Sex Tourism*, *supra* note 46, at 47.

⁵² *Id.*

Regional and International Law

Child pornography is a multi-jurisdictional problem that demands a global response. Successfully combating child pornography and child exploitation on a global scale requires uniform legislation; laws that vary from country to country serve to 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 child pornography, to be followed by national implementing legislation and the creation of a national legislative scheme to combat child pornography.

There are three main international legal instruments that address child pornography: the Optional Protocol to the (U.N.) Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography;⁵³ the Council of Europe's Convention on Cybercrime;⁵⁴ and the Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.⁵⁵ All three 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 Optional Protocol and the Convention on the Protection of Children also serve as comprehensive examples of legal mechanisms that require governments to implement and provide for services to assist child victims and their families.

In addition to these three international legal instruments, 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. 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. At the time of publication, 26 Member States had taken steps to implement this Directive under their national law.⁵⁶

In comparison with 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 regarding sexual abuse and exploitation of children. In particular, the Directive provides recommendations for terms of imprisonment for certain offenses; it describes measures for treatment of offenders; and it contains provisions on supporting and protecting child victims with a focus on the best interests of the child.⁵⁷

⁵³ *Optional Protocol*, *supra* note 14.

⁵⁴ *Convention on Cybercrime (CETS 185)*, *supra* note 27.

⁵⁵ *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. 27, 2015) (on file with the International Centre for Missing & Exploited Children).

⁵⁶ 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, <http://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32011L0093> (last visited Jan. 1, 2016) (on file with the International Centre for Missing & Exploited Children).

⁵⁷ 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. 30, 2015) (on file with the International Centre for Missing & Exploited Children). (Corrigendum to Directive 2011/92/EU, '2011/92/EU' to be read as

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

While the Convention on the Rights of the Child⁵⁸ (CRC) aims to ensure a broad range of human rights for children – including civil, cultural, economic, political, and social rights⁵⁹ – there are Articles within the CRC and the Optional Protocol to the CRC 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 CRC Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography (Optional Protocol) entered into force on 18 January 2002. Specific to child pornography:

- 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 child pornography, whether committed domestically or transnationally, on an individual or organized basis.
- Article 3 (1) (c) requires States Parties to criminalize simple possession regardless of the intent to distribute.
- Article 3 (4) addresses the liability of legal persons and encourages each State Party to establish such liability for offenses specific to child pornography. This article reflects the notion that a comprehensive approach requires industry involvement.
- Article 10 (1) addresses the need for international cooperation. As mentioned above, child pornography is readily distributed across borders; without international cooperation, many offenders may evade apprehension.

'2011/93/EU', <http://db.eurocrim.org/db/en/doc/1715.pdf> (last visited Oct. 27, 2015) (on file with the International Centre for Missing & Exploited Children).

⁵⁸ *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 (on file with the International Centre for Missing & Exploited Children).

⁵⁹ See UNICEF, *Convention on the Rights of the Child*, at <http://www.unicef.org/crc/> (last visited Feb. 26, 2013) (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 (Cybercrime Convention) with the hope of implementing a cooperative and uniform approach to the prosecution of cybercrime. The Cybercrime Convention 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, 47 countries (39 member States and 8 non-member States) have ratified the Cybercrime Convention, and 7 other countries (6 member States and 1 non-member State) have signed, but not ratified, the Cybercrime Convention.⁶⁰

Pertinent to the area of child sexual exploitation is Title 3 of the Cybercrime Convention, entitled “Content-Related Offenses.” Specifically, Article 9 of Title 3 deals with offenses 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 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 12 (1) addresses corporate liability.
- Article 23 addresses the issue of international cooperation.

⁶⁰ 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 Jan. 20, 2016) (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 (Child Protection 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 Child Protection Convention was opened for signature on 25 October 2007, and entered into force on 1 July 2010. The Child Protection 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, 39 member States have ratified the Child Protection Convention, and 8 other member States have signed, but not ratified, the Child Protection Convention.⁶¹ With regard to child pornography:

- 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 child pornography or knowingly attend performances involving child pornography.
- Article 24 addresses attempt crimes as well as aiding and abetting.
- Article 26 (1) addresses the issue of corporate responsibility.
- Article 38 (1) addresses the issue of international cooperation.

⁶¹ 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 Jan. 20, 2016) (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.⁶² 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.⁶³

The Directive describes measures that may be taken to identify and treat those who would become offenders⁶⁴ or recidivists,⁶⁵ and prevent offenders from maintaining professions involving regular contact with children,⁶⁶ and it introduces provisions to protect the child victim during investigations and legal proceedings.⁶⁷ Furthermore, the Directive encourages enhanced cooperation between Member States and non-Member States to ensure the removal of child sexual abuse images (child pornography) from servers in non-Member States,⁶⁸ and to tackle child sex tourism.⁶⁹

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 2015, 26 Member States had taken steps to implement this Directive under their national law.⁷⁰

With regard to the text of the Directive itself, child pornography 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.”

⁶² 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 57.

⁶³ *Id.* at paragraphs 3 and 12, and Articles 6 and 25.

⁶⁴ *Id.* at Article 22.

⁶⁵ *Id.* at Article 24.

⁶⁶ *Id.* at Article 10.

⁶⁷ *Id.* at Article 20.

⁶⁸ *Id.* at paragraph 46.

⁶⁹ *Id.* at paragraph 29.

⁷⁰ National Implementing Measures, *supra* note 56. 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 57, at paragraph 52.

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

Implementation

There has been significant legislative change over the last 10 years as more countries have developed laws to protect children from sexual abuse and exploitation with a focus on child pornography. Even with slow but steady statutory improvement, the question remains whether countries that have legislation are in fact enforcing those laws. 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 for fighting child victimization.

Enforcement is a straightforward concept wherein the civil and criminal penalties for certain actions articulated in the law are upheld in/through action (i.e., arrests, prosecutions, sentencing, etc.). However, implementation – viewed broadly – goes well beyond simply ensuring that each component of the law is integrated into the legal system of a country. 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.⁷¹ Examples of best practices that encompass protective and preventive approaches are:

Preventive	Protective
<ul style="list-style-type: none">▪ National Strategy Plans*▪ Child online protection frameworks▪ Training and education programs▪ Public awareness campaigns▪ Corporate Social Responsibility (CSR) programs▪ Research and data collection	<ul style="list-style-type: none">▪ Improved legislative tools▪ Formalized legal processes, including arrests, prosecutions, and convictions▪ Services for victims▪ Services for perpetrators▪ Monitoring and reporting mechanisms

* A National Strategy Plan provides a comprehensive, long-term blueprint for a country that seeks to prioritize a particular issue, such as child protection or sexual exploitation, on its political, social and legislative agendas. It can be a very valuable tool for helping relevant stakeholders to understand the scope of the issue and to establish cohesive policies, procedures, standards, mechanisms, technologies, and other resources to address it.

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.

⁷¹ Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, *supra* note 55, at Chapters II and IV.

Global Legislative Review

✘ = No
✔ = Yes

Country	Legislation Specific to Child Pornography ⁷²	“Child Pornography” Defined	Computer-Facilitated Offenses ⁷³	Simple Possession ⁷⁴	ISP Reporting ⁷⁵	Data Retention Broadly ⁷⁶
Afghanistan	✘	✘	✘	✘	✘	✔
Albania	✔	✔	✔	✔	✘	✔
Algeria	✔	✔	✔ ⁷⁷	✔	✘	✔
Andorra	✔	✘	✔ ⁷⁸	✘	✘	✘
Angola	✔	✔	✔	✔	✘	✘

⁷² For the purposes of this report, we were looking for specific laws that proscribe and/or penalize child pornography offenses. Mere labor legislation that simply bans the “worst forms of child labor,” among which is child pornography, is not considered “legislation specific to child pornography.”

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 pornography,” unless there is a sentencing enhancement provided for offenses committed against a child victim.

⁷³ In order to qualify as a computer-facilitated offense, we were looking for specific mention of a computer, computer system, Internet, or similar language (even if such mention is of a “computer image” or something similar in the definition of “child pornography”). In cases where other language is used in national legislation, an explanatory footnote is provided.

⁷⁴ “Simple possession,” for the purposes of this report, refers to knowing possession regardless of the intent to distribute.

⁷⁵ 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 child pornography 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.

⁷⁶ For the purposes of this report, data retention broadly means the obligation for ISPs to retain computer data for a specific period of time. This could be an obligation provided by law to retain non-content data (i.e., IP address, date, time and time zone for emails sent, full email address) for all users from its collection (data retention) and/or an obligation to preserve stored data with probative value of an identified user who is currently under investigation from the moment of its request by law enforcement (data preservation). 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 is not considered.

⁷⁷ Article 333 bis 1 of the Penal Code of Algeria imposes criminal penalty for anyone who represents, **by any means**, a person under eighteen (18) years participating 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.*

⁷⁸ Article 155 of the Nouveau Code Penal of Andorra criminalizes “produc[ing], sell[ing], distribut[ing], disseminat[ing], exhibit[ing], **by any means**, pornographic material where images of minors...appear.” *Emphasis added.*

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Antigua & Barbuda	✓	✓	✓	✓	✗	✓
Argentina	✓	✓	✓ ⁷⁹	✗	✗	✓
Armenia	✓	✗	✓	✓ ⁸⁰	✗	✓
Aruba	✓	✓	✓	✓	✗	✗
Australia	✓	✓	✓	✓	✓	✓
Austria	✓	✓	✓ ⁸¹	✓	✗ ⁸²	✗
Azerbaijan	✓	✓	✗	✓	✗	✗
Bahamas	✓	✓	✓	✓	✗	✗
Bahrain	✓	✗	✓	✗	✗	✗

⁷⁹ 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.*

⁸⁰ Article 263 of the Armenia Penal Code criminalizes possession of child pornography only when “keeping/saving them into computer system or in any computer data storage system”.

⁸¹ Section 207a(1)(3) of the Austrian Penal Code criminalizes “mak[ing] available in **any other manner**...a pornographic depiction of a minor.” *Emphasis added.*

⁸² 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).

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Bangladesh	✓	✓	✓	✓	✗	✗
Barbados	✓	✓	✓	✓	✗	✓
Belarus	✓	✓	✓	✗	✗	✗
Belgium	✓	✓	✓ ⁸³	✓	✓ ⁸⁴	✗
Belize	✓	✗	✗	✗	✗	✗
Benin	✗	✗	✗	✗	✗	✗
Bhutan	✓	✓	✓ ⁸⁵	✗	✓	✗
Bolivia	✓	✓	✓ ⁸⁶	✓	✗	✗
Bosnia-Herzegovina	✓	✗	✓ ⁸⁷	✓	✗	✗

⁸³ Article 383bis of the Belgian Penal Code, as amended on 1 April 2001, criminalizes, *inter alia*, the dissemination of child pornography, thereby including dissemination via computers. Letter from Jan Luykx, Deputy Chief of Mission, Embassy of Belgium, Washington, D.C., to the International Centre for Missing & Exploited Children (Feb. 24, 2006) (on file with the International Centre for Missing & Exploited Children).

⁸⁴ 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).

⁸⁵ 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.*

⁸⁶ Article 281(a) of Law 3325 Trata y Trafico de Personas y Otros Delitos Relacionados of Bolivia states that “whoever by himself or through a third person, **by any means**, promotes, produces, displays, markets or distributes pornographic materials, or promotes obscene performances that involve children or adolescents will be punished with imprisonment of three (3) to six (6) years.” *Emphasis added.*

⁸⁷ Articles 189 and 211 of the Penal Code of Bosnia-Herzegovina reference “**other pornographic materials**” in addition to photographs and audio-visual tapes. *Emphasis added.*

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Botswana	✓	✓	✓	✓	✗	✓
Brazil	✓	✓	✓	✓	✗ ⁸⁸	✓
Brunei Darussalam	✓	✓	✓	✓	✗ ⁸⁹	✗
Bulgaria	✓	✓	✓	✓	✗	✓
Burkina Faso	✗	✗	✗	✗	✗	✓
Burundi	✓	✗	✗	✗	✗	✗

⁸⁸ 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).

⁸⁹ 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 Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Cambodia	✓	✓	✓	✗	✗	✗
Cameroon	✓	✓	✓	✓	✗	✗
Canada	✓	✓	✓	✓	✓	✓ ⁹⁰
Cape Verde	✓	✗	✗	✗	✗	✗
Central African Republic	✓	✗	✗	✗	✗	✗
Chad	✗	✗	✗	✗	✗	✗
Chile	✓	✓	✓	✓	✗	✗

⁹⁰ Bill C-22 respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service, *supra* notes 42-43. The law mandates reporting by ISPs to law enforcement of child pornography offenses committed via an Internet service and obliges ISPs to “preserve all computer data related to the notification that is in their possession or control for 21 days after the day on which the notification is made”.

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
China ⁹¹	✓ ⁹²	✗	✓ ⁹³	✗	✓ ⁹⁴	✓
Colombia	✓	✓	✓	✓	✓	✓
Comoros	✓	✗	✗	✗	✗	✗
Congo	✓	✓	✗	✓	✗	✗

⁹¹ Child pornography legislation in Hong Kong differs from that in China. Legislation in Hong Kong:

- defines child pornography;
- criminalizes computer-facilitated offenses; and
- criminalizes simple possession of child pornography.

Taiwan has legislation specific to child pornography that:

- criminalizes simple possession of child pornography; and
- mandates ISPs to report child pornography.

Macau has legislation specific to child pornography, but has not yet fulfilled the remaining five criteria.

⁹² 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).

⁹³ 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).

⁹⁴ 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).

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Costa Rica	✓	✓	✓ ⁹⁵	✓	✗	✗
Côte d’Ivoire	✓	✓	✗	✗	✗	✗
Croatia	✓	✓	✓	✓	✗	✓
Cuba	✓	✗	✗	✗	✗	✗
Cyprus	✓	✓	✓	✓	✗	✗
Czech Republic	✓	✗	✓	✓	✗	✓
Democratic Republic of Congo	✓	✓	✓ ⁹⁶	✗	✗	✗
Denmark	✓	✓	✓ ⁹⁷	✓	✗ ⁹⁸	✓

⁹⁵ Article 173 of the Costa Rican Penal Code imposes a penalty on those who “display, disseminate, distribute, finance or market **by any means**...pornographic material in which minors appear, or possess for this purpose.” *Emphasis added.*

⁹⁶ Section 174M of the Penal Code of the Democratic Republic of Congo criminalizes “representations **by any means whatsoever**” of child pornography. *Emphasis added.*

⁹⁷ Section 235 of the Danish Criminal Code criminalizes, *inter alia*, dissemination and possession of “**other**...visual reproductions” of pornographic materials concerning children under the age of 18. *Emphasis added.*

⁹⁸ 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 Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Djibouti	✓	✗	✓ ⁹⁹	✗	✗	✗
Dominica	✗	✗	✗	✗	✗	✗
Dominican Republic	✓	✓	✓	✓	✗	✓
Ecuador	✓	✓	✓	✓	✗ ¹⁰⁰	✗
Egypt	✓	✗	✓	✓	✗	✗
El Salvador	✓	✓	✓	✓	✗	✓
Equatorial Guinea	✗	✗	✗	✗	✗	✗
Eritrea	✗	✗	✗	✗	✗	✗
Estonia	✓	✓	✓ ¹⁰¹	✓	✓	✓
Ethiopia	✗	✗	✗	✗	✗	✗

⁹⁹ 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.*

¹⁰⁰ 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.”

¹⁰¹ Articles 177 and 178 of the Estonian Penal Code criminalize using a minor in “**other works**” or using “**any other manner**” to manufacture, store, hand over, display, or make available child pornography. *Emphasis added.*

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Fiji	✓	✓	✓	✓	✗	✗
Finland	✓	✓	✓ ¹⁰²	✓	✗	✓
France	✓	✓	✓	✓	✓	✓
Gabon	✗	✗	✗	✗	✗	✗
Gambia, The	✓	✗	✗	✗	✗	✓
Georgia	✓	✓	✓ ¹⁰³	✓	✗ ¹⁰⁴	✗ ¹⁰⁵
Germany	✓	✓	✓	✓	✗ ¹⁰⁶	✗
Ghana	✓	✓	✓	✓	✗	✓
Greece	✓	✓	✓ ¹⁰⁷	✓	✗	✓

¹⁰² Chapter 17, Section 18 of the Finnish Criminal Act criminalizes “any person who...**otherwise** distributes obscene pictures or visual recordings depicting children.” *Emphasis added.*

¹⁰³ The Note in Article 255 of the Criminal Code of Georgia specifies that “video or audio material produced **in any manner**, involving a minor or a person appearing to be a minor involved in sexually explicit, simulated or computer generated sexual scenes,...shall be considered as pornographic material.” *Emphasis added.*

¹⁰⁴ 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).

¹⁰⁵ *Id.*

¹⁰⁶ 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).

¹⁰⁷ Article 348a of the Greek Penal Code criminalizes various child pornography offenses, including possession, purchase, transfer, and sale of child pornography “**in any way.**” *Emphasis added.*

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Grenada	✓	✓	✓	✓	✗	✓
Guatemala	✓	✗	✓ ¹⁰⁸	✓	✗	✗
Guinea	✓	✓	✓	✓	✗	✗
Guinea Bissau	✗	✗	✗	✗	✗	✗
Guyana	✗	✗	✗	✗	✗	✓
Haiti	✓	✗	✗	✗	✗	✗
Holy See	✓	✓	✓ ¹⁰⁹	✓	✗ ¹¹⁰	✓ ¹¹¹
Honduras	✓	✗	✓	✓	✗	✗

¹⁰⁸ Article 194 of the Penal Code of Guatemala criminalizes “Any person who, **by whatever form or through whatever mechanism**, produces, makes or enhances pornographic material that contains the image or voice (actual or simulated) of one or of various minors....” *Emphasis added.*

¹⁰⁹ Canon Law of the Holy See criminalizes “the acquisition, possession, or distribution by a cleric of pornographic images of minors under the age of fourteen, for purposes of sexual gratification, **by whatever means or using whatever technology.**” *Emphasis added.*

¹¹⁰ 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).

¹¹¹ Article 12 of the Legge sulle fonti del diritto, Law No. LXXI states that the law in force in Italy, including regulations and treaties covering telecommunications and relevant services both of landline and mobile networks, is applicable except when otherwise provided by specific Vatican Legislation.

See also “If a specific regulation related to child pornography is lacking, the case may also be delegated to the Italian judiciary system at the request of the Holy See.” 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 Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Hungary	✓	✓	✓ ¹¹²	✓	✗ ¹¹³	✓
Iceland	✓	✓	✓ ¹¹⁴	✓	✗	✗
India	✓	✓	✓	✓	✓	✓
Indonesia	✓	✗	✓ ¹¹⁵	✓	✗	✗
Iran	✗	✗	✗	✗	✗	✓
Iraq	✗	✗	✗	✗	✗	✗
Ireland	✓	✓	✓	✓	✗ ¹¹⁶	✓
Israel	✓	✓	✓	✓	✗	✗

¹¹² Under Section 195/A(3) of the Hungarian Criminal Code, a person making, distributing, or trading pornographic pictures of a minor by video, film, photograph, or “by any other means,” or making such pictures available to the public, commits a felony. Further, according to a recent decision of the Hungarian Appellate Court (Nr. BH 133/2005), the reference to “any other means” and “making available to the public” includes distribution through the Internet. Letter from Viktor Szederkényi, Deputy Chief of Mission, Embassy of the Republic of Hungary, Washington, D.C., to the International Centre for Missing & Exploited Children (Feb. 6, 2006) (on file with the International Centre for Missing & Exploited Children).

¹¹³ 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).

¹¹⁴ Article 210 of the Penal Code of Iceland criminalizes the “possession of photographs, films, or **comparable items** depicting children in a sexual or obscene manner.” *Emphasis added.*

¹¹⁵ Article 1 of the Indonesian Anti-Pornography Law criminalizes pornography created “through **any media or mode of communication.**” *Emphasis added.*

¹¹⁶ 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).

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Italy	✓	✓	✓	✓	✓	✓
Jamaica	✓	✓	✓	✓	✗	✗
Japan	✓	✓	✓	✓	✗	✓
Jordan	✓	✓	✓	✗	✗	✗
Kazakhstan	✓	✗	✓ ¹¹⁷	✗	✗	✓
Kenya	✓	✗	✓ ¹¹⁸	✗	✗	✗
Kiribati	✗	✗	✗	✗	✗	✗
Kosovo	✓	✓	✓	✓	✗	✗
Kuwait	✗	✗	✗	✗	✗	✗
Kyrgyzstan	✓	✓	✗	✗	✗	✗
Laos	✓	✗	✓	✗	✓	✗

¹¹⁷ Article 273 of the Penal Code of Kazakhstan criminalizes the manufacture, distribution, advertisement of and trade in “pornographic materials or objects, as well as ... printed publications, films or videos, pictures or **other items of a pornographic nature.**” Article 273-1 specifically addresses “pornographic images of minors.” *Emphasis added.*

¹¹⁸ Section 16(1)(aa) of the Kenyan Sexual Offenses Act imposes sanctions on anyone who “sells, lets to hire, distributes, publicly exhibits, or **in any manner**” child pornography. *Emphasis added.*

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Latvia	✓	✓	✓ ¹¹⁹	✓	✗ ¹²⁰	✓
Lebanon	✗	✗	✗	✗	✗	✓
Lesotho	✓	✗	✗	✗	✗	✗
Liberia	✓	✗	✓ ¹²¹	✓	✗	✗
Libya	✗	✗	✗	✗	✗	✗
Liechtenstein	✓	✓	✓	✓	✗ ¹²²	✗

¹¹⁹ Article 166(2) of the Criminal Law of Latvia criminalizes “the importation, production, public demonstration, advertising, or **other distribution** of such pornographic...materials as relate or portray the sexual abuse of children.” *Emphasis added.*

¹²⁰ Regarding to the responsibility of Internet Service Providers to report suspected child pornography to law enforcement or to some other mandated agency the Ministry of Justice informs that the Article 369 of the Criminal Procedure Law provides that non-governmental organisations or any natural person or legal person which has not directly suffered may submit information indicating the committing of a possible criminal offence to an investigating institution, Prosecutor’s Office, or court. Additionally the Ministry of Justice would like to inform that the Article 315 of the Criminal Law provides criminal liability for failing to inform, where it is known with certainty that preparation for or commission of a serious or especially serious crime is taking place...Involvement of underaged persons in the production of pornographic or erotic materials is an especially serious crime. Letter from L. Medin, Deputy Secretary State, Ministry of Justice of the Republic of Latvia, Washington, D.C. to the International Centre for Missing & Exploited Children (Nov. 21, 2012) (on file with the International Centre for Missing & Exploited Children).

¹²¹ Article 18.16 of the Penal Code of Liberia (Children’s Law 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.*

¹²² 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).

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Lithuania	✓	✗	✗	✓	✗	✓
Luxembourg	✓	✗	✓ ¹²³	✓	✗	✓
Macedonia	✓	✓	✓ ¹²⁴	✓	✗	✓
Madagascar	✓	✓	✓ ¹²⁵	✓	✗	✗
Malawi	✓	✓	✓	✓	✗	✗
Malaysia	✓	✗	✗	✗	✗	✗
Maldives	✗	✗	✗	✗	✗	✗
Mali	✓	✗	✗	✗	✗	✗
Malta	✓	✓	✓	✓	✗	✓
Marshall Islands	✗	✗	✗	✗	✗	✗

¹²³ Article 383 of the Penal Code of Luxembourg criminalizes not only the manufacture and possession (for trade, distribution, or public display) of “writings, printings, images, photographs, films, or **other objects** of a pornographic nature,” but also the commission of a variety of other child pornography offenses in “**any way.**” *Emphasis added.*

¹²⁴ Article 193(3) of the Macedonian Penal Code criminalizes the abuse of a “juvenile” in the “production of audio-visual, pictures or **other objects** with a pornographic content.” *Emphasis added.*

¹²⁵ Article 346 of the Penal Code of Madagascar criminalizes the use of “**any means**” to disseminate child pornography. *Emphasis added.*

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Mauritania	✓	✗	✓	✓	✗	✗
Mauritius	✓	✗	✓	✗	✗	✓
Mexico	✓	✓	✓	✓	✗	✓
Micronesia	✗	✗	✗	✗	✗	✗
Moldova	✓	✓	✓	✓	✗	✓
Monaco	✓	✓	✓	✓	✗	✗
Mongolia	✓	✗	✗	✗	✗	✗
Montenegro	✓	✗	✓ ¹²⁶	✓	✗ ¹²⁷	✓

¹²⁶ Article 211(2) of the Penal Code of Montenegro criminalizes “exploit[ing] a child for the production of pictures, audio-visual, **or other objects** of pornographic content.” Article 211(3) criminalizes procuring, selling, showing ... **in electronic or some other manner** mak[ing] available pictures, audio-visual or other objects of pornographic content portraying a minor. *Emphasis added.*

¹²⁷ 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).

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Morocco	✓	✓	✓ ¹²⁸	✓	✗ ¹²⁹	✗
Mozambique	✗	✗	✗	✗	✗	✗
Myanmar	✓	✗	✓	✗	✗	✗
Namibia	✓	✗	✗	✗	✗	✗
Nauru	✗	✗	✗	✗	✗	✗
Nepal	✗	✗	✗	✗	✗	✗

¹²⁸ Article 503.2 of the Penal Code of Morocco (Amended in 2003 by Law No. 24-03) criminalizes “caus[ing], incit[ing] or facilitat[ing] the exploitation of children under the age of eighteen in pornography of any kind, **by whatever means**, of a real, simulated or perceived sexual act or of any representation of the sexual organ of a child for sexual purposes.” *Emphasis added.*

¹²⁹ While in Morocco there is no explicit provision on the legal responsibility of Internet Service Providers to report child pornography sites to the police, or of web hosts or telephone operators to share details of abusers, Morocco has taken some very strong steps to combat child pornography. I would like to turn your attention to the following:

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

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

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Netherlands	✓	✓	✓	✓	✗ ¹³⁰	✓
New Zealand	✓	✓	✓	✓	✗ ¹³¹	✓
Nicaragua	✓	✓	✓	✓	✗	✓
Niger	✓	✗	✗	✗	✗	✗
Nigeria	✓	✓	✓	✗	✗	✓
North Korea	✗	✗	✗	✗	✗	✗
Norway	✓	✓	✓	✓	✗	✗
Oman	✓	✗	✓	✓	✗	✓
Pakistan	✗	✗	✗	✗	✗	✓
Palau	✗	✗	✗	✗	✗	✗

¹³⁰ 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).

¹³¹ 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 Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Panama	✓	✓	✓	✓	✗ ¹³²	✓
Papua New Guinea	✓	✓	✓ ¹³³	✓	✗	✗
Paraguay	✓	✓	✓ ¹³⁴	✗	✗ ¹³⁵	✗
Peru	✓	✗	✓	✓	✗	✓
Philippines	✓	✓	✓	✓	✓	✓
Poland	✓	✗ ¹³⁶	✓	✓	✗ ¹³⁷	✓

¹³² While there is no mandatory reporting requirement specific to ISPs, Article 231-I of the Panamanian Penal Code establishes that if anyone who has knowledge of the use of minors in pornography or sexual activities, whether the person obtained such information by means of his/her duties, job, business, profession, or by any other means, fails to report it to the authorities, he/she will be sent to prison for this omission. If the commission of the crime (child pornography or sexual activity) cannot be proved after the report, the person who reported it will be exempted of any liability with regards to his/her report to the authorities. Email from Isabel Fernández, Embassy of Panama, Washington, D.C., to the International Centre for Missing & Exploited Children (Apr. 12, 2006) (on file with the International Centre for Missing & Exploited Children).

¹³³ Section 299 of the Criminal Code Act 1974 of Papua New Guinea defines child pornography as “any photographic, film, video or **other visual representation**” and criminalizes “a person who uses a child for the production of child pornography.” *Emphasis added.*

¹³⁴ Article 1 of Paraguayan Law Number 2.861/06 imposes sanctions on “whoever, **by any means**, produces, or reproduces” child pornography. *Emphasis added.*

¹³⁵ 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.”

¹³⁶ 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. Budyń-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).

¹³⁷ 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).

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Portugal	✓	✗	✓ ¹³⁸	✓	✗	✓
Qatar	✓	✗	✓	✓	✓	✓
Romania	✓	✓	✓	✓	✗ ¹³⁹	✓
Russia	✓	✗	✓	✗	✗	✓
Rwanda	✓	✗	✓ ¹⁴⁰	✗	✗	✗
St. Kitts & Nevis	✓	✓	✓ ¹⁴¹	✗	✗	✗
St. Lucia	✗	✗	✗	✗	✗	✓
St. Vincent & the Grenadines	✓	✓	✓	✓	✗	✓
Samoa	✗	✗	✗	✗	✗	✓

¹³⁸ It can be inferred from Article 172 of the Portuguese Penal Law that the expression “by any means” allows a Prosecutor to view information and communication technologies as a means to commit the crime of circulating images, sounds, or movies clearly showing minors younger than 14 years old engaged in sexual acts. Letter from Pedro Catarino, Ambassador, Embassy of Portugal, Washington, D.C., to the International Centre for Missing & Exploited Children (Feb. 22, 2006) (on file with the International Centre for Missing & Exploited Children).

¹³⁹ 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).

¹⁴⁰ Article 229 of N° 01/2012/OL of 02/05/2012 Organic Law instituting the Penal Code of Rwanda criminalizes “Any person who records a picture or the voice of a child or disseminates it **in any way for** pornographic purposes.” *Emphasis added.*

¹⁴¹ Article 2 of the Trafficking in Persons Prevention Act of St. Kitts and Nevis criminalizes “the audio or visual depiction of sexually explicit conduct involving a child whether made or produced by electronic, mechanical **or other means....**” *Emphasis added.*

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
San Marino	✓	✓	✓	✗	✗	✗
Sao Tome & Principe	✓	✗	✓ ¹⁴²	✓	✗	✗
Saudi Arabia	✓	✗	✓	✗	✗	✗
Senegal	✓	✓	✓	✓	✗	✓
Serbia	✓	✗	✓ ¹⁴³	✓	✗	✓
Seychelles	✓	✗	✓	✓	✗	✗
Sierra Leone	✓	✓	✓ ¹⁴⁴	✓	✗	✗
Singapore	✓	✗	✓	✗	✗	✗
Slovak Republic	✓	✓	✓ ¹⁴⁵	✓	✗	✗
Slovenia	✓	✗	✓ ¹⁴⁶	✓	✗	✗

¹⁴² 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....**"

¹⁴³ Article 111a of the Serbian Penal Code criminalizes making a “photograph, film, or **some other picture**” of a minor for the purpose of making an item of pornographic content. Additionally, Article 185 criminalizes using a minor for producing “pictures, audio-visual, or **other items** of pornography content.” *Emphasis added.*

¹⁴⁴ 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.*

¹⁴⁵ Section 369 of Act No. 300/2005 Coll. Criminal Code of the Slovak Republic criminalizes “disseminat[ing], transport[ing], procur[ing], mak[ing] accessible **or otherwise put[ting] into distribution** child pornography.” *Emphasis added.*

¹⁴⁶ Article 187(2) of the Penal Code of Slovenia criminalizes the abuse of a minor “to produce pictures, audio-visual, or **other items** of a pornographic nature”; Article 187(3) criminalizes the actions of anyone who “produces, distributes, sells, imports, exports, ... or supplies [pornographic material depicting minors] **in any other way**, or who possesses such material with the intention of producing, distributing, selling, importing, exporting, or supplying it **in any other way.**” *Emphasis added.*

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Solomon Islands	✗	✗	✗	✗	✗	✗
Somalia	✗	✗	✗	✗	✗	✗
South Africa	✓	✓	✓	✓	✓	✓
South Korea	✓	✓	✓	✓	✗ ¹⁴⁷	✓
South Sudan	✓	✗	✗	✗	✗	✗
Spain	✓	✗	✓ ¹⁴⁸	✓	✗	✓
Sri Lanka	✓	✗	✗	✓	✓	✓
Sudan	✓	✓	✗	✓	✗	✗
Suriname	✓	✓	✓	✓	✗	✗
Swaziland	✓	✗	✗	✗	✗	✗

¹⁴⁷ 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).

¹⁴⁸ Article 189(1)(a) of the Spanish Penal Code criminalizes using a minor "to prepare **any type** of pornography material"; Article 189(1)(b) criminalizes producing, selling, distributing, displaying, or facilitating the production, sale, dissemination, or exhibition, of "**any type**" of child pornography by "**any means**"; and Article 189(7) repeats the "**any type**" and "**any means**" language previously used. *Emphasis added.*

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Sweden	✓	✓ ¹⁴⁹	✓ ¹⁵⁰	✓	✗ ¹⁵¹	✓
Switzerland	✓	✓	✓	✓	✗ ¹⁵²	✓
Syria	✗	✗	✗	✗	✗	✗

¹⁴⁹ 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)

¹⁵⁰ Swedish criminal legislation is, in principle, formulated so that it will apply regardless of technical prerequisites. The criminalization of child pornography is no exception and, accordingly, Chapter 16, Section 10a, of the Swedish Penal Code extends to computer-facilitated offenses. Letter from Anette Nilsson, First Secretary, Embassy of Sweden, Washington, D.C., to the International Centre for Missing & Exploited Children (Feb. 23, 2006) (on file with the International Centre for Missing & Exploited Children).

¹⁵¹ In 1998, Sweden enacted the Bulletin Board System (BBS) Liability Act (1998:112), which aims to prevent the spread of child pornography by obligating BBS providers to supervise BBS content. BBS providers are also obligated to remove or in some other way prevent the dissemination of messages with a criminal content, including those with child pornography. Letter from Anette Nilsson, First Secretary, Embassy of Sweden, Washington, D.C., to the International Centre for Missing & Exploited Children (Feb. 23, 2006) (on file with the International Centre for Missing & Exploited Children).

¹⁵² 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 Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Tajikistan	✓	✗	✓	✗	✗	✗
Tanzania	✓	✓	✓	✗	✓	✓
Thailand	✓	✗	✓	✓	✗	✓
Timor Leste	✓	✓	✓ ¹⁵³	✓	✗	✗
Togo	✓	✓	✓ ¹⁵⁴	✗	✗	✗
Tonga	✓	✓	✓	✓	✗	✓
Trinidad & Tobago	✓	✓	✓	✓	✗	✗
Tunisia	✗	✗	✗	✗	✗	✓
Turkey	✓	✗	✓	✓	✓	✓

¹⁵³ 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.*”

¹⁵⁴ 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 Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Turkmenistan	✓	✗	✗	✗	✗	✗
Tuvalu	✗	✗	✗	✗	✗	✗
Uganda	✓	✓	✓	✓	✗	✓
Ukraine	✓	✓	✓	✗	✗	✗
United Arab Emirates	✓	✓	✓	✓	✗	✗
United Kingdom ¹⁵⁵	✓	✓	✓	✓	✗ ¹⁵⁶	✓
United States	✓	✓	✓	✓	✓	✓

¹⁵⁵ For the purposes of this report, the United Kingdom includes England and Wales. Northern Ireland and Scotland each have legislation specific to child pornography, but do not meet the remaining criteria. In regards to data retention, the law of the United Kingdom applies also to Northern Ireland and Scotland.

¹⁵⁶ 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 server 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).

Country	Legislation Specific to Child Pornography	“Child Pornography” Defined	Computer-Facilitated Offenses	Simple Possession	ISP Reporting	Data Retention Broadly
Uruguay	✓	✓	✓ ¹⁵⁷	✗	✗	✗
Uzbekistan	✓	✗	✗	✗	✗	✗
Vanuatu	✓	✓	✓	✓	✗	✗
Venezuela	✓	✗	✓	✗	✗	✗
Vietnam	✓	✗	✗	✗	✗	✗
Yemen	✗	✗	✗	✗	✗	✗
Zambia	✓	✗	✓	✓	✗	✗
Zimbabwe	✗	✗	✗	✗	✗	✗

¹⁵⁷ Law 17.815 of the Oriental Republic of Uruguay criminalizes certain child pornography offenses regardless of how they are committed (i.e., Article 1: “in any way makes or produces child pornography”; Article 2: “**in any way** facilitates the commercialization, diffusion, exhibition, storage, or acquisition of child pornography”). *Emphasis added.*

Conclusion

Over the past ten years, ICMEC's research regarding the status of child pornography legislation around the world has demonstrated that slow and steady progress is being made. Various international legal instruments are in place, which have helped raise awareness and attach new urgency to this cause. It remains clear, however, that more countries need to take action now if we are to secure a safer future for the world's children. While combating child pornography at home and abroad is a daunting task, the harmonization of laws is essential in order to effectively address this growing, international phenomenon.



1700 Diagonal Road, Suite 625 ♦ Alexandria, Virginia 22314-2844 ♦ USA
Tel +1 703 837 6313 ♦ Fax +1 703 549 4504 ♦ www.icmec.org