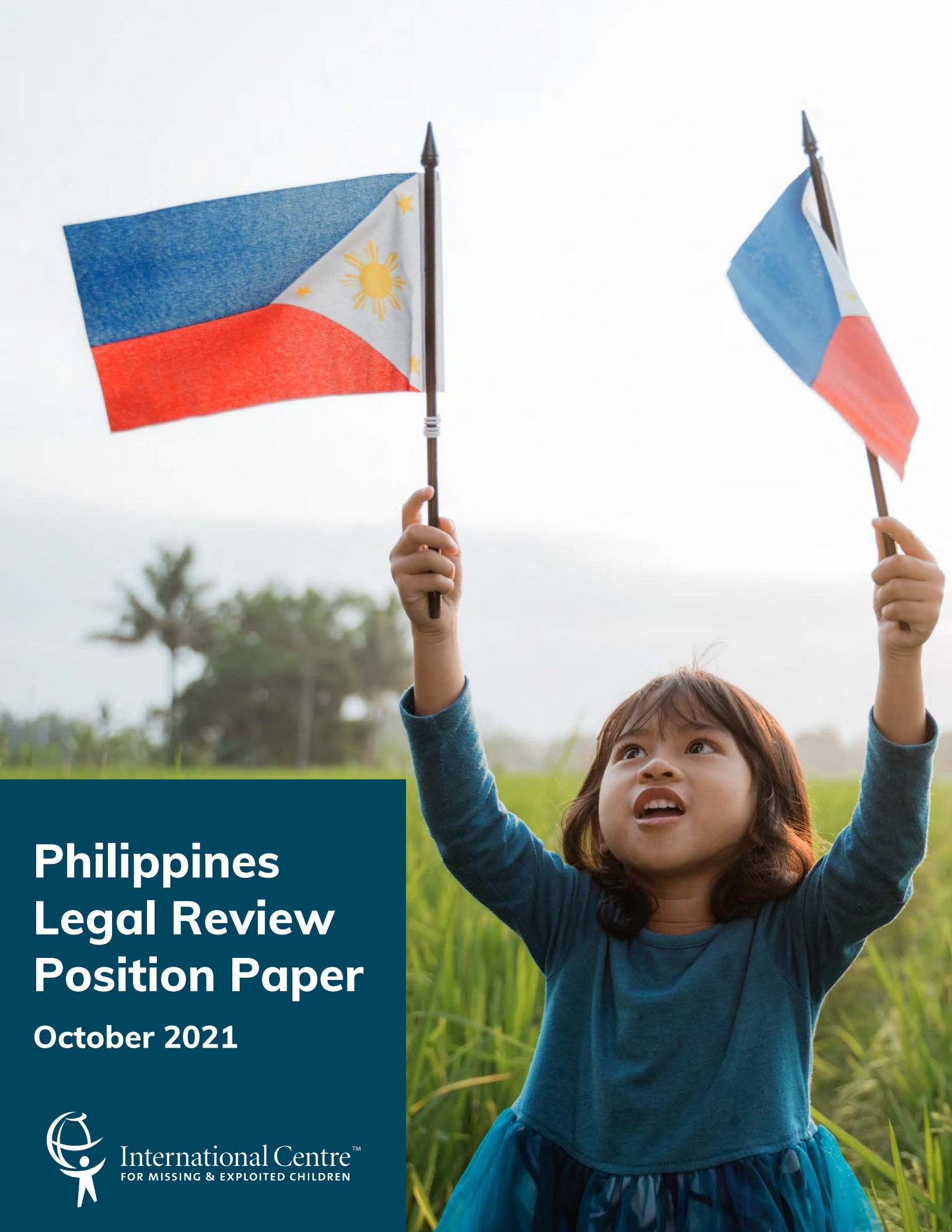


Philippines Legal Review Position Paper

October 2021

International Centre™
FOR MISSING & EXPLOITED CHILDREN

Contents

A Letter from the CEOs

Safeguarding children is a responsibility every one of us shares.

For more than two decades, the International Centre for Missing & Exploited Children (ICMEC) has focused on building a global community of caring adults and institutions all working together to bring about a world where children can grow up free from going missing, from being abducted, sexually abused or exploited.

Thanks to committed partners like Romulo Mabanta, ICMEC is able to offer support to governments, policymakers, law enforcement, prosecutors, industries, civil society, and others around the world to advance our common goal of building a safer world for children.

The following report endeavors to detail the current legal statues that hinder or collectively challenge operational action by the diverse stakeholder group. While our global community continues to make progress in improving the laws and systems to protect children, we still have work to do because one child missing, abused, or exploited is one too many. We hope that policymakers, law enforcement, and child-protection organizations will benefit from this paper that identifies challenges and gaps that still exist leaving our children vulnerable.

Bob Cunningham
The International Centre for Missing & Exploited Children

Cristina Collantes-Garcia
Romulo Mabanta Buenaventura Sayoc & Delos Angeles

Preface

The purpose of this paper is to strengthen the child protection legal framework such that it leaves no child in the Philippines vulnerable to sexual exploitation and abuse. The analysis and recommendations herein reflect the real-world challenges faced by dozens of professionals navigating the, admittedly, robust child protection legal framework in the Philippines, and recommendations from a diverse stakeholder group that supports the child protection agenda.

In 2009, the International Centre for Missing & Exploited Children (ICMEC), under the auspices of its Financial Coalitions Against Child Sexual Exploitation (FCACSE) Initiative, launched a region-wide Asia Pacific Financial Coalition Against Child Sexual Exploitation (APAC-FCACSE) to foster collaboration and develop solutions to fight the online sale and dissemination of child sexual exploitation materials, including live on-demand sexual abuse of children via video platforms.

2013 saw ICMEC pivot to a country-specific focus leveraging the Allen & Overy law firm's Asia offices and in the Philippines, Romulo Mabanta Buenaventura Sayoc & Delos Angeles law firm's legal framework research linked here to prevent child exploitation in the Asia Pacific.

In 2017, ICMEC held the Philippines Roundtable, hosted by Romulo Mabanta, bringing together 77 individuals representing banks, payment gateways, electronic payment platforms and remittance companies, law enforcement agencies, regulatory bodies, other government departments and civil society partners to discuss collaboration across sectors. The purpose of the roundtable was to inform stakeholders of the issue of online child exploitation, the cross-border and cross-sector nature of the crime, and the role industry (both financial and information and communications technology) can play in working with law enforcement to combat the crime. It was envisioned that collaborative action across stakeholders could preempt and prevent trade in child sexual abuse materials (CSAM). Namely, the misuse of legitimate corporate payment platforms in the sale, purchase, and dissemination of CSAM. All agreed that preemption and prevention of such transactions to eliminate the profits illegal merchants stand to make, was a more desirable outcome, rather than collective action after a transgression, when a child has already been victimized.

The collective commitment of the diverse stakeholders at the Philippines Roundtable in 2017 launched the formation of the APFC Philippines Working Group that thereafter met three times a year, through 2019.

Over the course of these three years, the Philippines Working Group identified numerous challenges that hindered cross-sector collaboration between law enforcement, regulatory bodies, and private industry. Discussions that followed delved deeper into the reasons why and concluded that to effectively disrupt this crime we needed to understand and review both legal and operational issues of concern. 2020 saw these meetings disrupted by the global pandemic but gave ICMEC the opportunity to step-back and reflect on the Working Group extensive discussions that resulted in this paper.

The paper enumerates several impediments faced by law enforcement, regulators, policymakers, private industry, civil society, and others to advance effective action to combat this crime. Through practical recommendations, we endeavor to detail the current legal statues that hinder or collectively challenge operational action by the diverse stakeholder group. We respectfully urge policymakers in the Philippines Congress to take up the cause and support the review, revision and/or drafting of new legislation that will address the challenges identified to close the gaps that still exist leaving our children vulnerable.

My sincere and special thanks to several committed partners who contributed to the framing and writing of this position paper.

Contributors

Cristina Collantes-Garcia, Partner, Romulo Mabanta; Atty. Mel Georgie Racela, Executive Director, Philippines Anti Money Laundering Council; Dr. Ivy Patdu, then Deputy Commissioner, Philippines National Privacy Commission; Police Brigadier General William Macavinta (now Ret.) Philippines National Police; Yvette Tamayo-Coronel, Deputy Executive Director of the Inter-Agency Council against Trafficking, Philippines Department of Justice; Atty. Marie Michelle Quezon, Child Protection Officer, UNICEF Philippines; Jordana Hiltrop, Assistant to the Police Attaché to the Philippines, The National Police of the Netherlands; Daniel Anselmo, Head - Southeast Asia Financial Intelligence Unit – Office of Law Enforcement Outreach & Investigations, Western Union and John Nicholls Senior Director & Country Site Lead, PayPal Philippines, who first join the Working Group when he was Chief Operating Officer HSBC Philippines.

Bindu Sharma
Managing Director, ICMEC Asia Pacific

Executive Summary

The dramatic rise of cases of online sexual abuse and exploitation of children (OSAEC) in the Philippines during the time of the COVID-19 pandemic proves the inadequacy of existing laws in protecting the rights of children and promoting their welfare in the digital space.

Now more than ever, there is an urgent need for Congress to revisit laws that seek to address the issues of child exploitation and trafficking.

Key areas for review recommended are:

- The Anti-Child Pornography [1] Act – there should be greater accountability on Internet Service Providers (ISPs), Internet Content Hosts, and owners and operators of other businesses who may encounter incidents of online sexual abuse and exploitation of children.
- The Bank Secrecy and Anti-Money Laundering (AML) laws – to enable law enforcement authorities to have more flexibility in investigating and prosecuting child offenders. Specific guidelines on entrapment procedures specifically crafted for OSAEC cases are also recommended via the proper government instrumentalities.
- Privacy laws – permissible data sharing between government agencies needs to be improved. Controlled data-sharing options across stakeholders could be considered, as well as providing a safe harbor for OSAEC-specific cases.

It is the objective of this position paper to inform members of the Philippine Congress on existing gaps in the policies and implementation of laws with the aim of combatting the rise of incidences of OSAEC in the Philippines, and respectfully provide recommendations on how these laws can be refined to effectively fulfill their purpose.

[1] Throughout the paper the term child pornography is used as it is the term still used in the legislation of the Philippines, and much of the world, despite the international consensus around the shift using the term child sexual abuse materials (CSAM) to convey the gravity of the crime.

Summary of Recommendations

Challenge Faced by Law Enforcement Against the Backdrop of Constitutional Provisions of the Process of Securing an Arrest Warrant

- It is recommended that the issue of enforcement and cooperation between foreign and Philippines LEA be institutionalized where LEA collectively build a case together so that the legal processes move faster, more seamlessly and can effect a warrantless arrest addressing the issue of flight of the perpetrators.

- It is recommended to establish a dedicated team of local law enforcers designated to a child protection unit which will be familiar with the processes and focused on coordination.

Anti-Child Pornography Act of 2009 (RA 9775)

- The second paragraph of Section 9 be revised such that the law does not require ISPs to look for illegal content, but they must report it when they are made aware of it. In such instances where a user reports illegal content then ISPs should be required to report the same to law enforcement.
- Create a national reporting mechanism that may be utilized by both ISPs and users, where illegal content may be reported to, and where information on such content could be collated, organized and shared on a regular basis with ISPs to ensure this content does not make its way back in the public domain.
- Incentivize ISPs to install blocking and filtering technology to remove such content from being hosted in the open Internet, failing which consider imposing stiffer penalties and fines for non-compliance.
- Amend RA 9775 to hold ISPs, Internet Content Hosts, banks, and other persons more accountable in reporting incidents of child sexual exploitation and abuse.
- Require persons and entities with reporting requirements to undergo mandatory training or education to explain the necessity of reporting these incidents, the proper method of reporting to the authorities, and the consequences should they fail to do so.
- Recommend that RA 9775 include provisions where ISPs offer specific technology tools that permit requisite oversight and control mechanisms such

that parents and schools can rightly meet their obligations in relation to a child's access to the Internet.

- Assign or establish a singular government body to which relevant entities can report incidents of OSAEC. Congress may establish a separate body or identify an existing agency tasked by law to accept and retain the records of these reports and maintain an updated list of URLs and sites, where such content is hosted that could be made available to LEAs and ISPs so they may either immediately take down or block sites that are used to facilitate the commission of OSAEC-related offenses.
- Under the implementing rules and regulations of laws such as the Anti-Child Pornography Act of 2009 (RA 9775) and the Expanded Anti-Trafficking in Persons Act of 2012 (RA 10364) provide a set of guidelines on how to conduct valid entrapment procedures in relation to the crimes these laws penalize.

Bank Deposit Secrecy Laws (RA 1405 and RA 6426 (as amended))

- Bank Deposit Secrecy Laws be amended to expand the list of exceptions to bank secrecy for both foreign currency and peso deposits and to include accounts utilized in cases of online exploitation of children, human trafficking, and other forms of child abuse to allow a greater opportunity for LEAs to trace the money trail of child offenders and ultimately identify and prosecute such offenders. Based on the risk assessments and studies made by the AMLC, OSAEC-related offenses are high-risk predicate crime and their exemption from court-issued bank inquiry can be justified as necessary.

AMLC supports the recommendation to further ease bank deposit secrecy laws.

Anti-Money Laundering Act of 2001 (RA 9160 as amended)

- AMLA be amended by Congress to provide a specific provision allowing the AMLC to share the information it collects on bank deposits relating to unlawful activities with LEAs such as the NBI or PNP for the sole purpose of prosecution of offenders alleged to have committed such activities.
- AMLA be amended to include provisions on the formation of a central database containing details of persons who were *parties* to government investigations that have been completed and who have been convicted of AMLA offenses. An AMLC maintained list specifically pertaining to the misuse of financial payments industry platforms and services would motivate industry to regularly run the list

against their customer database stemming from their obligations as a reporting entity.

- AMLA be amended to include provisions on permissible data sharing among AMLA-covered institutions from different financial groups on covered or suspicious transactions and a safe harbor for institutions participating in the data sharing.
- Amend the Anti Money Laundering Act to include all offenses related to online exploitation of children to the list of cases that would not require a court order before the AMLC may inquire into or examine any particular deposit or investment related to the same.

Data Privacy Act (RA 10175)

- Consider adding provisions to RA 10175 for less stringent requirements or an expedited process for the issuance of cybercrime warrants for traffic and content data if the case involves an incident of OSAEC. At present, LEAs are generally required to obtain a valid search warrant before being allowed to search and examine traffic and content data under RA 10175.[1] One amendment that can be introduced is to add a provision requiring a court where the application for the issuance of a search warrant relating to an OSAEC case is filed to act on the application no later than twenty-four (24) hours from its filing, similar to what is provided under Section 11 of the AMLA.
- Recommended that the Data Privacy Act be amended to provide child-specific provisions, such as more stringent qualifications before the personal information of children may be collected.

[1] Cybercrime Prevention Act of 2012 (RA 10175).

The Current Reality of Online Sexual Abuse and Exploitation of Children

The Philippine government's implementation of several lockdowns brought about by the COVID-19 pandemic has resulted in a sharp increase in incidence of cases of online sexual abuse and exploitation of children (OSAEC) and accompanying spike in related financial transactions. The table below provides information on the ***suspected***[2] incidence of OSAEC obtained from the Philippines Department of Justice - Office of Cybercrime (DOJ-OCC). The data below demonstrates a four-fold increase in the suspected incidence of OSAEC in a span of one year.

	2019	2020
March	23,465	101,560
April	24,147	80,508
May	28,947	102,331
Total	**76,559**	**284,400**

Furthermore, the Philippine Anti-Money Laundering Council (AMLC) has stated that from 15 March to 15 May 2020, online sexual exploitation of children-related transactions totaling 5,902 transactions were noted by the AMLC, compared with the 369 transactions transacted during the same period in 2019.[3]

The rise in cases of OSAEC has not gone unnoticed by President Rodrigo Duterte, and was one of the points of discussion in the most recent Cabinet meeting according to Cabinet Secretary Karlo Nograles.[4] Secretary Nograles explained that the National Telecommunications Commission (NTC) was directed to immediately sanction unnamed Internet Service Providers (ISPs) which failed to comply with their obligations under the Anti-Child Pornography Act, and urged Congress to pass pending bills seeking to amend the Anti-Trafficking in Persons Act.[5]

---

2 Please note that most of these reports are tips and leads about child sexual exploitation received by the U.S.-based National Center for Missing and Exploited Children (NCMEC) through the CyberTipline.

3 *Online Sexual Exploitation of Children: A crime with a global impact and an evolving transnational threat*, Anti-Money Laundering Council, Aug. 20, 2020, *at* http://www.amlc.gov.ph/images/PDFs/2020%20AUG%20AMLC%20OSEC%20AN%20EMERGING%20RISK%20AMID%20THE%20COVID19%20PANDEMIC.pdf.

4 *Internet providers to be penalized for enabling child porn online,* CNN, Jan. 12, 2021, *at* https://www.cnn.ph/news/2021/1/12/Online-child-porn-sexual-exploitation-internet-providers.html.

5 *Id.*

While there are laws in place to promote the welfare of children and combat the incidence of sexual exploitation of children, the steady and continuous increase in the number of cases reported, despite the presence of these laws, highlights the apparent inadequacy and ineffectiveness of said laws. In this position paper, we describe the legal framework in place and identify the significant gaps in the law which Congress may address through the passage of new or amendatory legislation.

Existing Legal Framework on Child Protection

The Philippines is a signatory to several key international conventions and declarations that aim to combat the incidence of child exploitation, such as the UN Convention on the Rights of the Child, Optional Protocol to the Convention on the Rights of the Child on the sale of children child prostitution and child pornography, and the Budapest Convention on Cybercrime. These international pieces of legislation are complemented by local laws such as the Philippine Constitution, the Child and Youth Welfare Code, and the Anti-Child Pornography Act of 2009.

International Conventions

A. The UN Convention on the Rights of the Child (CRC)[6]

Articles 12 to 17 of the CRC, ratified by the Philippines in July 1990, promote the freedom of expression and access to information, especially those aimed at the promotion of the child's well-being and health. Meanwhile, Articles 19-23 and 32-40 promote the special protection of children from abuse, exploitation, and all forms of violence.

B. The UN Convention Against Transnational Organized Crime (UNTOC)[7]

The UNTOC is intended to promote cooperation and to combat transnational organized crime, specifically those relating to trafficking in persons with particular attention to women and children. To effectively prevent and combat transnational organized crimes, such as those relating to OSAEC, the UNTOC requires ratifying parties to take a

[6] UN Convention on the Rights of the Child, entered into force Sep. 2, 1990, *at* https://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx.

[7] UN Convention against Transnational Organized Crime and the Protocols Thereto, entered into force Sep. 29, 1983, *at* https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf.

series of measures against transnational organized crime, the adoption of new frameworks for extradition, mutual legal assistance and law enforcement cooperation, and the promotion of training and technical assistance for building or upgrading the necessary capacity of national authorities.[8]

The Anti-Money Laundering Act complements the UNTOC, as it expressly includes offenses relating to trafficking-in-persons, child abuse, and violence against women and children as additional predicate crimes in the offense of money laundering. The same law also gives the Anti-Money Laundering Council the power to pursue non-conviction-based forfeiture proceedings, also known as civil forfeiture, with respect to proceeds stemming from unlawful activities as defined in the said law.

C. Budapest Convention on Cybercrime[9]

Article 9 of The Budapest Convention on Cybercrime, which was ratified by the Philippines in 2018, provides that each party thereto shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law, when committed intentionally and without right, conduct such as producing child pornography for distribution through a computer system, procuring child pornography through a computer system, and possessing child pornography in a computer system.

Philippines Law

A. The 1987 Philippine Constitution[10]

Article II, Section 13 of the Philippine Constitution is a recognition of the vital role of youth in nation building and included a State policy of promoting and protecting their physical, moral, intellectual, and social well-being. Moreover, Article XV, Section 3 states that the Government must defend "the right of children to assistance, including proper care and nutrition and special protection from all forms of neglect, abuse, cruelty, exploitation and other conditions prejudicial to their development."

8 *See* https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.

9 Budapest Convention on Cybercrime, at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

10 1987 Constitution of the Republic of the Philippines, *at* https://www.officialgazette.gov.ph/constitutions/1987-constitution/.

B. The Child and Youth Welfare Code (Presidential Decree 603)[11]

The Child and Youth Welfare Code defines the rights and responsibilities of children and the corresponding authority and obligations to them by their parents, the community, and the government and other duty bearers.

C. Special Protection of Children Against Abuse, Exploitation and Discrimination Act (Republic Act 7610)[12]

Republic Act 7610 specifically criminalizes child prostitution and other sexual abuse, child trafficking, and other acts of abuse against children. This law also criminalizes the hiring, employing, using, persuading, inducing, or coercing a child to perform in obscene exhibitions and indecent shows, whether live or in video, or model in obscene publications or pornographic materials or to sell or distribute the said materials.

Significantly, Sections 5, 7, 8, 9, 10 (c), 10 (d), 10 (e), 11, 12, and 14 of the said law are predicate crimes under the AMLA.[13]

D. Anti-Child Pornography Act of 2009 (RA 9775)[14]

Republic Act 9775 defines child pornography as "any representation, whether visual, audio, or written combination thereof, by electronic, mechanical, digital, optical, magnetic or any other means, of child engaged or involved in real or simulated explicit sexual activities."[15] It criminalizes the production, distribution, exportation, transmission, importation, intentional possession, and advertising of child pornography.[16] Significantly, the acts punishable under Section 4 of the said law, which provides the unlawful or prohibited acts in relation to child pornography, are predicate crimes under the Anti-Money Laundering Act.[17]

---

11 The Child and Youth Welfare Code, Presidential Decree 603, *at* https://www.officialgazette.gov.ph/1974/12/10/presidential-decree-no-603-s-1974/.

12 Special Protection of Children Against Abuse, Exploitation and Discrimination Act (RA 7610), Sections 5-9, *at* https://www.officialgazette.gov.ph/1992/06/17/republic-act-no-7610/.

13 Sec. 3(i)(32) of the Anti-Money Laundering Act (AMLA) of 2001 (RA 9160), as amended, at http://www.amlc.gov.ph/laws/money-laundering/2015-10-16-02-50-56/republic-act-9160, http://www.amlc.gov.ph/laws/money-laundering/2015-10-16-02-50-56/republic-act-9194, http://www.amlc.gov.ph/laws/money-laundering/2015-10-16-02-50-56/republic-act-10167, http://www.amlc.gov.ph/laws/money-laundering/2015-10-16-02-50-56/republic-act-10365, http://www.amlc.gov.ph/laws/money-laundering/2015-10-16-02-50-56/ra-10927-designating-casinos-as-covered-persons-under-ra-9160-amla-2001, and http://www.amlc.gov.ph/images/PDFs/RA%2011521.pdf.

14 Anti-Child Pornography Act of 2009 (RA 9775), *at* https://www.officialgazette.gov.ph/2009/11/17/republic-act-no-9775-s-2009/.

15 *Id.* at Sec. 3(b).

16 *Id.* at Sec. 4.

17 Sec. 3(i)(31), AMLA.

The same law imposes the following obligations and duties on ISPs and Internet Content Hosts, *viz*:

i. Mandatory notification by ISPs of the Philippine National Police (PNP) or the National Bureau of Investigation (NBI) within seven (7) days from obtaining facts and circumstances that any form of child pornography is being committed using its server or facility;
ii. Preservation of evidence for the purpose of investigation and prosecution by relevant authorities;
iii. Upon the request of proper authorities, provision of the particulars of users who gained or attempted to gain access to an Internet address, which contains any form of child pornography;[18] and
iv. Installation of available technology, program, or software to ensure that access to or transmittal of any form of child pornography will be blocked or filtered.[19]

E. Expanded Anti-Trafficking in Persons Act of 2012 (RA 10364)[20]

Republic Act 10364 defines and punishes acts of trafficking in persons, which includes the use, procuring, or offering of a child for prostitution, for the production of pornography, or for pornographic performances. Significantly, Sections 4 to 6 of the said law are predicate crimes under the AMLA.[21]

F. Data Privacy Act of 2012 (RA 10173)[22]

The Data Privacy Act of 2012 implements the State's policy of securing the right to privacy of individuals by regulating the processing and transfer of personal information. The Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that is located in the Philippines, or those who maintain an office, branch, or agency in the Philippines, subject to certain exceptions.

Notably, Section 4(e) of the said law exempts within the ambit of its application "information necessary in order to carry out the functions of public authority which

---

18 *Id.* at Sec. 11.
19 *Id.* at Sec. 9.
20 Expanded Anti-Trafficking in Persons Act of 2012 (RA 10364), *at* https://www.officialgazette.gov.ph/2013/02/06/republic-act-no-10364.
21 Sec. 3(i)(19), AMLA.
22 Data Privacy Act of 2012 (RA 10173), *at* https://www.privacy.gov.ph/data-privacy-act/.

includes the processing of personal data for the performance by the…law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions."

On a related note, the National Privacy Commission issued NPC Circular 2020-03 (Dec. 23, 2020) on Data Sharing Agreements. This Circular no longer makes Data Sharing Agreements (DSA) mandatory but requires that the sharing be based on lawful criteria under the Data Privacy Act.[23]

G. Cybercrime Prevention Act of 2012 (RA 10175)[24]

Republic Act 10175 is characterized as the first domestic and general law which comprehensively discusses and punishes cybercrime and cyber-related offenses, including content-related offenses such as cybersex. Cybersex contemplates interactive prostitution and pornography, i.e., by webcam or livestreaming.

RA 10175 also treats child pornography committed through a computer system[25] as a prohibited act, the penalty of which shall be one (1) degree higher than that provided for in RA 9775.[26]

H. Anti-Photo and Video Voyeurism Act of 2009 (RA 9995)[27]

Republic Act 9995 criminalizes the taking of photo or video coverage of a person or group of persons performing a sexual act or similar activity, or to capture an image of the private area of a person/s such as the naked or undergarment clad genitals, pubic area, buttocks, or female breast without the consent of the person/s involved and under circumstances in which the person/s has/have a reasonable expectation of privacy. The same law also punishes the act of copying or reproducing such photo or video despite consent to record or take photo or video coverage of the same was given by such person/s. Notably, acts punishable under Section 4 of the said law are predicate crimes under the AMLA.[28]

---

23 Data Sharing Agreements, NPC Circular 2020-03 on (Dec. 23, 2020), *at* https://www.privacy.gov.ph/wp-content/uploads/2021/01/Circular-Data-Sharing-Agreement-amending-16-02-21-Dec-2020-clean-copy-FINAL-LYA-and-JDN-signed-minor-edit.pdf.

24 Cybercrime Prevention Act of 2012 (RA 10175), *at* https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/.

25 *Id.* at Sec. 4(c)(2).

26 *Id.* at Sec. 8.

27 Anti-Photo and Video Voyeurism Act of 2009 (RA 9995), *at* https://dict.gov.ph/wp-content/uploads/2014/10/RA-9995-Anti-Photo-and-Video-Voyeurism-Act.pdf

28 Sec. 3(i)(30), AMLA.

I. Anti-Money Laundering Act of 2001 (RA 9160 as amended)

The Anti-Money Laundering Act (AMLA) requires covered persons to report to the AMLC all covered and suspicious transactions within five (5) working days from occurrence of such transactions, as defined therein. The AMLA also empowers the AMLC to inquire into or examine any particular deposit or investment with any banking or non-bank financial institution generally upon order of any competent court when it has been established that there is probable cause that such deposits or investments are related to an unlawful activity or money laundering offense as defined in the AMLA, notwithstanding bank secrecy laws currently in place.

Under the AMLA, covered transaction reports are filed within five (5) days from occurrence thereof, while suspicious transaction reports are required to be filed promptly filed within the next working day from occurrence thereof, in accordance with Rule 22, Section 2, of the 2018 Implementing Rules and Regulations (IRR) of the AMLA. The results of analysis of this information may be shared, under Section 8-A of the AMLA, by the AMLC, pursuant to its function as a financial intelligence unit (FIU), to relevant domestic and foreign authorities. The authority of the AMLC to conduct bank inquiry is in pursuance of its mandate as a law enforcement agency, particularly as a financial investigation body.

In addition to the foregoing, the AMLA provides other valuable tools to help fight OSAEC, namely:

a. Information exchange, sharing, and dissemination of financial intelligence, to both domestic and foreign authorities, pursuant to Section 8-A of the AMLA and Rule 6 (B) of its 2018 IRR;
b. Asset tracing through its power to investigate (including the filing of applications for bank inquiry, subpoena and search warrants), under Sections 7(5), 7(13), 7(14), and Section 11, respectively, of the AMLA;
c. Asset freezing, under Sections 7(6) and 10 of the AMLA;
d. Asset forfeiture, under Sections 7(3) and 12 of the AMLA;
e. Filing of criminal complaints for laundering of proceeds of OSAEC-related crimes, among others, under Section 7(4) of the AMLA;
f. Provision of evidence and other legal assistance (asset freezing, confiscation, etc.) to foreign States via mutual legal assistance (MLA), under Sections 7(8) and 13 of the AMLA;
g. Capacity-building of law enforcement agencies to use the AMLA as a way to fight OSAEC-related crimes, among others, under Section 7(9) of the AMLA; and
h. AML regulation and supervision (and imposition of administrative sanctions) on covered persons to ensure that appropriate measures are in place so OSAEC perpetrators will not financially benefit from the said crimes, under Sections 7(7), and 11 and 14(f) of the AMLA.

J. Law on Secrecy of Bank Deposits (RA 1405 as amended)[29] and the Foreign Currency Deposit Act (RA 6426 as amended)[30]

Republic Act 1405 (as amended) provides that all deposits of whatever nature with banks in the Philippines are absolutely confidential ***except*** upon written permission of the depositor, or in cases of impeachment, or upon order of a competent court in cases of bribery or dereliction of duty of public officials, or in cases where the money deposited or invested is the subject matter of the litigation.

Meanwhile, Republic Act 6426 (as amended) provides that all currency deposits are confidential except upon the written permission of the depositors.

Significantly, Section 24 of the AMLA has expressly repealed RA 1405 as amended and RA 6426 as amended insofar as their provisions are inconsistent with the AMLA. Consistent with the foregoing repeal, the AMLC is empowered to direct banks to produce Customer Due Diligence or Know-Your-Customer records and to submit covered and suspicious transaction reports and may also inquire into bank accounts for certain unlawful activities, as will be discussed in further detail below.

Opportunity for the Laws to Protect Our Children Better

Despite the existence of extensive legislation on OSAEC, it is believed that the effectiveness of these laws in preventing the incidence of OSAEC could be further enhanced through:

- the issuance of additional implementing guidelines on procedures specific to OSAEC cases,
- review and strengthening of specific statutes, and
- considering developments in technology impacting the nature of the crime and recognize the everchanging face of the crime.

More importantly, to address the risks posed by OSAEC in the different facets of Philippine society, including but not limited to social, security, financial, and reputational impact, we respectfully provide below our recommendations.

[29] Law on Secrecy of Bank Deposits (RA 1405), *at* http://www.pdic.gov.ph/lawonsecrecyofbankdeposits.
[30] Foreign Currency Deposit Act (RA 6426), *at* https://www.officialgazette.gov.ph/1972/04/04/republic-act-no-6426/.

A. Challenge Faced by Law Enforcement Against the Backdrop of Constitutional Provisions of the Process of Securing an Arrest Warrant

An arrest can be affected without a warrant of arrest. This is often referred to as a "citizen's arrest". Under Rule 113, Section 5 of the Revised Rules of Criminal Procedure, a peace officer, or a private person may, without a warrant, arrest a person:

(a) When, in his presence, the person to be arrested has committed, is actually committing, or is attempting to commit an offense. This is also known as an in flagrante delicto (or in the very act of wrongdoing) arrest.
(b) When an offense has just been committed and he has probable cause to believe based on personal knowledge of facts or circumstances that the person to be arrested has committed it. This is also known as a hot pursuit arrest.
(c) When the person to be arrested is a prisoner who has escaped from a penal establishment or place where he is serving final judgment or is temporarily confined while his case is pending, or has escaped while being transferred from one confinement to another.
(d) In cases falling under paragraphs (a) and (b) justifying warrantless arrests, the person arrested without a warrant shall be delivered to the nearest police station for the conduct of inquest proceedings.

Under Article III, Bill of Rights in the 1987 Philippine Constitution states:

> SECTION 1. No person shall be deprived of life, liberty, or property without due process of law, nor shall any person be denied the equal protection of the laws.
>
> SECTION 2. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.

Under current statutes a person is required to personally witness a crime before enforcing a warrantless arrest. In the instance where it is initiated by international law enforcement, the arresting private person will still need to deliver the suspect perpetrator to the Philippines law enforcement and they are then required to go through an inquest proceeding where witnesses will provide statements so that a case can be filed. In reality, the legalities of a warrantless arrest by a private citizen are quite challenging. It would be more practical if local law enforcers are involved in the

operations so that cooperation is there from the onset to avoid technical and procedural risks in the arrest of the suspect perpetrator.

Of note here, in a globally connected world today, Cybercrime is inherently transnational and global; no state can adequately address cyber threats by itself. It is emphasized that the scope of the recommendations is limited only to child exploitation and abuse cases, where the end goal is always the best interest of the exploited children, who unfortunately, as evidence supports, are getting younger and younger.

Recommendation

It is recommended that the issue of enforcement and cooperation between foreign and Philippines LEA be institutionalized where LEA collectively build a case together so that the legal processes move faster, more seamlessly and can effect a warrantless arrest addressing the issue of flight of the perpetrators.

It is recommended to establish a dedicated team of local law enforcers designated to a child protection unit which will be familiar with the processes and focused on coordination.

B. Revisiting RA 9775 – Anti Child Pornography Act of 2009

Despite the reporting requirements under RA 9775, as discussed further below, and subsequent guidance from the NTC,[31] ISPs in the Philippines currently do not report possible illegal content due to the absence of a single national entity with a mandate to receive reports of illegal content as well as apparent ambiguity on what is required of ISPs and how to comply with the requirement under RA 9775 to notify authorities of any form of child pornography being committed using their facilities.

Section 9 of the Anti-Child Pornography Act of 2009 requires ISPs to notify the PNP or the NBI within seven (7) days from obtaining facts and circumstances that any form of child pornography is being committed using its server or facility.[32]

However, the second paragraph of Section 9 appears to negate or render nugatory the requirement of an ISP to notify law enforcement authorities (LEAs) considering that under the law, it is not required to monitor the activities of any of its users, subscribers, or customers.

---

[31] National Telecommunications Commission, *NTC Memorandum Circular No. 01-01-2014, at* https://ntc.gov.ph/wp-content/uploads/2015/10/LawsRulesRegulations/MemoCirculars/MC2014/MC-01-01-2014.pdf.

[32] Sec. 9, Anti-Child Pornography Act of 2009.

Section 9. Duties of an Internet Service Provider (ISP)

All Internet service providers (ISPs) shall notify the Philippine National Police (PNP) or the National Bureau of Investigation (NBI) within seven (7) days from obtaining facts and circumstances that any form of child pornography is being committed using its server or facility. Nothing in this section may be construed to require an ISP to engage in the monitoring of any user, subscriber or customer, or the content of any communication of any such person: Provided, that no ISP shall be held civilly liable for damages on account of any notice given in good faith in compliance with this section.

Recommendation

It is thus recommended that the second paragraph of Section 9 be revised such that the law does not require ISPs to look for illegal content, but they must report it when they are made aware of it. In such instances where a user reports illegal content then ISPs should be required to report the same to law enforcement.

The dilemma the law presents is that ISPs are not required to monitor the above-mentioned activities. Moreover, there are no guidelines on how *users* of computer systems may report any illegal content they may encounter or where they may report such content. Congress is respectfully urged to create a national reporting mechanism that may be utilized by both ISPs and users, where illegal content may be reported to, and where information on such content could be collated and organized.

Congress is respectfully urged to create a national reporting mechanism that may be utilized by both ISPs and users, where illegal content may be reported to, and where information on such content could be collated and organized.

The Philippines may review reporting mechanisms established in other countries, for example:

- The United States-based **CyberTipline**[33] run by the National Center for Missing and Exploited Children (NCMEC) - is the nation's centralized reporting system for the online exploitation of children. The public and electronic service providers can make reports of suspected online enticement of children for sexual acts, child sexual molestation, child sexual abuse material, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading

[33] NCMEC's CyberTipline - https://www.missingkids.org/gethelpnow/cybertipline

domain names, and misleading words or digital images on the internet. CyberTipline is unique in that it receives and processes reports coming in from anywhere in the world.

- The UK's **Internet Watch Foundation**[34] runs a reporting hotline that minimizes the availability of online sexual abuse content. Specifically, child sexual abuse content hosted anywhere in the world and non-photographic child sexual abuse images hosted in the UK.
- Closer to home in Australia, the Office of the eSafety Commissioner's **Cyber Report**[35] team investigates complaints and assists in getting content removed.

Significantly, House Bill 7633 has been filed to amend the above-mentioned Section 9, together with a measure of preventing foreigners who have committed any sex-related offenses from entering the Philippines.[36] This bill is currently being evaluated by the House of Representatives Committee on Revision of Laws.[37]

Preserving and Disclosing Computer Data

Philippine ISPs have experienced challenges complying with their legal obligation to assist law enforcement in cybercrime investigations, such as preserving and disclosing computer data associated to a specific IP address.

The failure of the ISPs to provide the computer data has resulted in the loss of investigative leads and ultimately affects the ability to effectively prosecute illegal activities online. Undeniably, there are investigations being delayed or severely hampered by the consequent inability of LEAs to utilize IP addresses in aid of OSAEC investigations.

Until the challenges relating to ISPs' compliance with preservation and disclosure of computer data is addressed, the same difficulties in the implementation of laws promoting the welfare of children and combat against the incidence of OSAEC will be encountered by LEAs.

Installation of Blocking and Filtering Technology

It is also worth mentioning that ISPs are mandated under RA 9775 to install available technology, program, or software to ensure that access to or transmittal of any form of

[34] Internet Watch Foundation, Report Criminal Content - https://report.iwf.org.uk/en

[35] Office of the eSafety Commissioner, Australia | Report Abuse - https://www.esafety.gov.au/report

[36] *See,* Maricel Cruz, *Stricter penalties sough as child porn surges,* MANILA STANDARD, Sep. 20, 2020, *at* https://manilastandard.net/news/top-stories/334631/stricter-penalties-sought-as-child-porn-surges.html.

[37] House Bill 7633, Anti-Sexual Abuse and Exploitation of Children Act of 2020, *at* https://www.congress.gov.ph/legisdocs/basic_18/HB07633.pdf.

child pornography will be blocked or filtered. To date, ISPs have generally yet to comply with this requirement despite the issuance and guidance by the NTC as provided in NTC Memorandum Circular No. 01-01-2014[38] and Memorandum Circular No. 03-07-2015.[39]

Recommendation

We recommend Congress incentivize ISPs to act, failing which consider imposing stiffer penalties and fines for non-compliance with this requirement.

Accountability for Failure to Report

Aside from ISPs, RA 9775 also requires Internet Content Hosts, operators, and owners or lessors of other business establishments, banks, photo developers, credit card companies, and any person who has direct knowledge of any form of child pornography activities to report any suspected child pornography materials or transactions to the proper authorities within seven (7) days from knowledge of such activities.[40] Significantly, failure to report such activity would result in no liability on the part of the persons or entities who fail to comply with this requirement. The law only punishes the act of failing to report a child pornography activity if the same was "willful and intentional."[41]

Recommendation

There is therefore a need to amend RA 9775 to hold ISPs, Internet Content Hosts, banks, and other persons more accountable in reporting incidents of child sexual exploitation and abuse. RA 9775 can be amended to make these persons or entities liable for civil or administrative penalties for mere failure to report such incidents. In addition, telecommunications service providers should also be included in the list of entities required to report such activities. The penalty for this offense should be substantial enough to ensure that the reporting requirement is satisfied.

Mandatory Training

Moreover, RA 9775 can be amended to require persons and entities with reporting requirements to undergo mandatory training or education to explain the necessity of reporting these incidents, the proper method of reporting to the authorities, and the

---

38 National Telecommunications Commission, *supra* note 23.

39 National Telecommunications Commission, *Memorandum Circular 03-07-2015, at* https://region7.ntc.gov.ph/images/LawsRulesAndRegulations/MC/VAS/MC_03-07-2015.pdf.

40 Sections 9, 10, and 11, Anti-Child Pornography Act of 2009 (RA 9775).

41 *Id.* at Sec. 10.

consequences should they fail to do so. The mandatory training may also include discussions on asset freeze and asset forfeiture as key tools in fighting OSAEC, given that criminal elements are lured in these activities because they generate huge amounts of proceeds. By crippling their finances, persons, and entities with reporting requirements under RA 9775 may hit them where it hurts them the most.

Obligations of Persons/Entities Exercising Parental Authority

Of note here are institutions or individuals in positions of authority and care. For instance, schools may be required to limit Internet access by children in school premises only to the extent necessary for implementing educational related activities.

Recommendation

Additionally, it is recommended that RA 9775 include provisions where ISPs offer specific technology tools that permit requisite oversight and control mechanisms such that parents and schools can rightly meet their obligations in relation to a child's access to the Internet ensuring their safety and well-being.

Centralized Body

The current language of RA 9775, which provides that the reports should be submitted to the "PNP or NBI," could lead to confusion and lack of proper recordkeeping at the national level. Congress may establish a separate body or identify an agency tasked by law to accept and retain the records of these reports and maintain an updated list of URLs and sites, where such content is hosted that could be made available to LEAs and ISPs so they may either immediately take down or block sites that are used to facilitate the commission of OSAEC-related offenses.

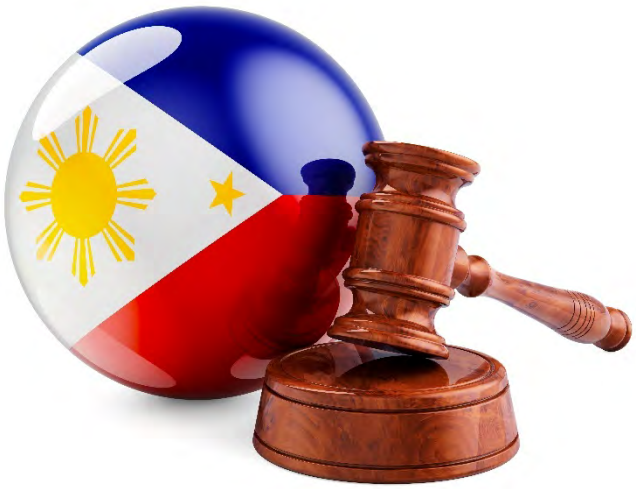
Recommendation

It is recommended as well that Congress assign or establish a singular government body to which these entities should report incidents of OSAEC.

It must be noted that there currently exists an Inter-Agency Council Against Child Pornography which was established under RA 9775 which has, among others, the function of maintaining a database of cases of child pornography.[42] Congress may thus consider identifying this council as the agency which will accept reports made by the said entities.

[42] *Id.* at Sec. 21 (n).

Another option that may be considered is for the President to set-up a national OSAEC coordinating committee (NOCC) comprised of pertinent government agencies via an Executive Order to harmonize the efforts of the entire country in fighting OSAEC. This is the track taken by the AMLC when it spearheaded the creation of the National Anti-Money Launder/Counter-Terrorism Financing Coordination Committee (NACC), which eventually paved the way to the issuance of Executive Order No. 68 on 12 November 2018.



C. Provisions on Entrapment

Entrapment procedures are legally acceptable in the Philippines and are mostly employed in dangerous drugs cases. Entrapment is the employment of ways and means in order to trap or capture a lawbreaker from whom the criminal intent or design to commit the offense charged originates.[43] In entrapment, the law enforcement officials merely facilitate the apprehension of the criminal by employing ruses and schemes.[44] Entrapment is different from "instigation", in which the accused *is lured* into the commission of the offense charged in order to prosecute him.[45] Thus, in instigation, officers of the law or their agents incite, induce, instigate, or lure an accused into committing an offense which he or she would otherwise not commit and has no intention of committing. But in entrapment, the criminal intent or design to commit the offense charged originates in the mind of the accused.[46]

The issue on whether or not a "test transaction" in relation to child exploitation is an entrapment or instigation would depend on the method by which such "test transaction" is conducted. LEAs should be guided by a set of guidelines that would ensure that the operation would be considered as an entrapment and not an instigation. These guidelines may be provided under the implementing rules and regulations of existing laws that combat child abuse and exploitation. Notably, should an operation be

[43] People v. Mendoza, G.R. No. 220759, 24 July 2017, *at* https://www.chanrobles.com/cralaw/2017julydecisions.php?id=502.
[44] *Id.*
[45] People v. Bartolome, G.R. No. 191726, 6 February 2013, *at* https://lawphil.net/judjuris/juri2013/feb2013/gr_191726_2013.html.
[46] *Id.*

deemed as an instigation by the court, the LEAs shall be deemed as *co-principals* to the crime, with the accused acquitted.[47]

It is submitted that a framework be established for entrapment procedures specific for OSAEC cases based on the same principles applied to dangerous drugs cases.

Recommendation

It is recommended that the implementing rules and regulations of laws such as the Anti-Child Pornography Act of 2009 (RA 9775) and the Expanded Anti-Trafficking in Persons Act of 2012 (RA 10364) provide a set of guidelines on how to conduct valid entrapment procedures in relation to the crimes these laws penalize.

D. Additional Exceptions to Bank Deposit Secrecy Laws

RA 1405 (as amended) and RA 6426 (as amended) provide depositors with the protection of privacy of their bank accounts, subject only to limited exceptions provided by law.

In particular, for peso deposits, some of the exceptions provided by law are the following:

a. written permission of the depositor;[48]
b. cases of impeachment;[49]
c. upon order of a competent court in cases of bribery or dereliction of duty of public officials;[50]
d. cases where the money deposited or invested is the subject matter of the litigation;[51]
e. upon order of the competent court in cases involving unexplained wealth under the Anti-Graft and Corrupt Practices Act;[52]
f. upon inquiry by the Commissioner of Internal Revenue for the purpose of determining the net estate of a deceased depositor;[53]
g. upon inquiry by the Commissioner of Internal Revenue in acceding to compromise of a taxpayer's liabilities due to financial inability to pay the tax assessed;[54]

---

47 *Id.*
48 Sec. 2, Law on Secrecy of Bank Deposits (RA 1405) (as amended).
49 *Id.*
50 *Id.*
51 *Id.*
52 Banco Filipino Savings and Mortgage Bank v. Purisima, G.R. No. L-56429, May 28, 1998 *at* https://lawphil.net/judjuris/juri1988/may1988/gr_l_56429_1988.html.
53 Sec. 6(F)(1), National Internal Revenue Code (RA 8424, as amended), *at* https://www.bir.gov.ph/index.php/tax-code.html.
54 *Id.* at Sec. 6(F)(2).

h. when the information is requested by a foreign tax authority pursuant to an international agreement entered into by the Philippines;[55]
i. upon the order of a competent court, or without one in proper cases, by the AMLC, under the AMLA;[56]
j. disclosure to the Treasurer of the Philippines for dormant deposits for at least ten (10) years under the Unclaimed Balances Act;[57]
k. Report of banks to the AMLC of covered and/or suspicious transactions;[58] and
l. Upon order of the Court of Appeals, examination by the AMLC in terrorism cases under the Anti-Terrorism Act of 2020.[59]

Significantly, for foreign currency deposits, the only exceptions to bank secrecy are the following:

a. permission of the depositor;[60]
b. upon the order of a competent court, or without one in proper cases, by the AMLC, under the AMLA; and[61]
c. Upon order of the Court of Appeals, examination by the AMLC in terrorism cases under the Anti-Terrorism Act of 2020.[62]

Expanding the list of exceptions to bank secrecy for both foreign currency and peso deposits to include accounts utilized in cases of online exploitation of children, human trafficking, and other forms of child abuse would allow a greater opportunity for LEAs to trace the money trail of child offenders and ultimately identify and prosecute such offenders.

It is noteworthy that for peso accounts, bank accounts may be examined in cases where the money deposited or invested is the subject matter of the litigation. In view of this, it is suggested that the authority examine suspicious bank accounts for the purpose of investigating cases of online exploitation of children be granted by Congress to a

55 *Id.* at Sec. 6(F)(3).
56 Sec. 11, AMLA.
57 Sec. 2, An Act Requiring Banks, Trust Companies, Savings and Mortgage Banks, Mutual Building and Loan Associations, and Banking Institutions of Every Kind to Transfer Unclaimed Balances Held by Them to the Insular Treasury, and for Other Purposes (Act No. 3936), *at* https://www.lawyerly.ph/laws/view/l3c96.
58 Sec. 9, AMLA
59 Sec. 35, The Anti-Terrorism Act of 2020 (RA 11479), *at* https://www.officialgazette.gov.ph/downloads/2020/06jun/20200703-RA-11479-RRD.pdf.
60 Sec. 28, Foreign Currency Deposit Act (RA 6426)
61 Sec. 11., AMLA.
62 Sec. 35, The Anti-Terrorism Act of 2020 (RA 11479)

specialized government committee for such purpose, and that the same exception be applicable to both peso and foreign currency bank accounts. In this manner, even in the investigation stages and before a case for child exploitation is filed with the proper court, LEAs would already have the evidence on hand to properly assess the facts and prosecute offenders if warranted by the facts and law.

On a related note, the AMLA authorizes the AMLC to examine any deposit or investment in a bank or non-bank financial institution upon order of any competent court when it has been established that there is probable cause that the subject deposits or investments, including related accounts involved, are related to an unlawful activity as defined in the same law.[63] These "unlawful activities" include the offenses under the Anti-Child Pornography Act of 2009.

Significantly, the AMLA also provides that no court order shall be required before the AMLC may inquire into or examine any particular deposit or investment in cases involving terrorism, kidnapping, certain offenses of the Comprehensive Dangerous Drugs Act of 2002, hijacking, destructive arson, and murder.[64]

It is suggested that Congress expand the coverage of the Anti-Money Laundering Act to include a broad range of offenses related to online exploitation of children, including child pornography, as part of the list of cases which would need no court order before bank accounts utilized to commit such offenses may be examined.

In view of this, it is suggested that Congress expand the coverage of the AMLA to include a broad range of offenses related to online exploitation of children, including child pornography, as part of the list of cases which would need no court order before bank accounts utilized to commit such offenses may be examined.

Recommendation

It is recommended that bank deposit secrecy laws be amended to expand the list of exceptions to bank secrecy for both foreign currency and peso deposits and to include accounts utilized in cases of online exploitation of children, human trafficking, and other forms of child abuse to allow a greater opportunity for LEAs to trace the money trail of child offenders and ultimately identify and prosecute such offenders. Based on the risk assessments and studies made by the AMLC, OSAEC-related offenses are high-risk predicate crime and their exemption from court-issued bank inquiry can be justified as necessary.

63 Sec. 11, AMLA.
64 *Id.*

Moreover, it is recommended that Congress amend the AMLA to include all offenses related to online exploitation of children to the list of cases that would not require a court order before the AMLC may inquire into or examine any deposit or investment related to the same. AMLC supports the recommendation to further ease bank deposit secrecy laws.

E. Anti-Money Laundering Act, 2001 (RA 9160 as amended) Enhanced Coordination Between AMLC and LEAs

As discussed above, the AMLC has the authority to examine and obtain information regarding bank accounts connected with predicate crimes, subject to certain exceptions. However, there is no clear basis under the AMLA to allow the AMLC to share the information it has gathered with LEAs for the purpose of investigating or prosecuting any of the predicate crimes.

To illustrate, the financial transaction related to the livestreaming of a child being sexually exploited (such as the monetary payment provided and received for the child's acts) is not an element of the offense of child pornography. Thus, the information collected by the AMLC on the said financial transaction cannot, *by itself*, be used by the NBI nor PNP to secure a subpoena or search warrant for the bank information of the accused. It may also be argued that based on the current wording of the AMLA, neither is AMLC authorized to share the information it has on the underlying transaction with the NBI or PNP.

However, while not being an essential element of an offense for child pornography or any other child exploitation case, nevertheless the information that the AMLC may gather on the underlying financial transaction may still prove useful for LEAs to build a case and properly prosecute the predicate crime.

Recommendation

Thus, it is recommended that the AMLA be amended by Congress to provide a specific provision allowing the AMLC to share the information it collects on bank deposits relating to unlawful activities with LEAs such as the NBI or PNP for the sole purpose of prosecution of offenders alleged to have committed such activities.

It is believed that online child exploitation cases would be identified more efficiently if there is a clear statutorily permissible avenue for the AMLC to share intelligence with LEAs. Perhaps Section 8-A of the AMLA, which states that the AMLC shall formulate rules governing information exchange and dissemination, could be expanded such that it would specifically allow the AMLC to share the information it has collected with LEAs

for the purpose of prosecuting individuals accused of committing predicate crimes. Such an expansion of Section 8-A of the AMLA would also do away with the necessity for the AMLC to execute memorandum of agreements with LEAs before they may share such information with LEAs.

F. Centralized Database for AMLA and AMLA-related Cases

In the United States, the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury publishes a "sanctions list" which contains a list of individuals and companies owned or controlled by, or acting for or on behalf of "targeted" countries, as well as a list of other individuals and companies who have been identified by the U.S. as to have committed illicit or undesirable activity and on whom the U.S. has imposed preventive measures.[65] The OFAC's sanctions list is publicly available online.

Meanwhile, in the Philippines, the Expanded Anti-Trafficking in Persons Act of 2012 (RA 10364) requires all government agencies tasked to undertake programs and render assistance to address trafficking in persons to develop their respective monitoring and data collection systems and databases that would gather information on all cases of trafficking in persons they encounter.[66] The information collected in these systems shall then be shared with the Inter-Agency Council Against Trafficking and included in a central database.

In the Philippines, it is recommended that a similar database as that of the OFAC's sanctions list be maintained for money laundering and related cases and be accessible to the public. Currently, while the AMLA requires banks to report and record "covered" and "suspicious" transactions as defined therein, there is no central database accessible to banks and other covered persons that would aid them in screening and evaluating their clients and other persons whom they deal with.[67] The "AMLA" central database, to be managed by the AMLC, should at least provide a list of all persons who have been convicted of AMLA offenses and their related predicate crimes, by the LEAs. Considering that the information to be included in the central database would be *public records*, there should not be any privacy concerns regarding the personal information reflected therein.

---

[65] For more information, *see* U.S. Department of the Treasury, Financial Sanctions, *Sanctions Programs and Country Information, at* https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information.

[66] Expanded Anti-Trafficking in Persons Act of 2012 (RA 10364)

[67] *See,* Anti-Money Laundering Council, *2018 Implementing Rules and Regulations of Republic Act No. 9160, as Amended, at* http://www.amlc.gov.ph/images/PDFs/FINAL%202018%20IRRv1.pdf; *See also,* Republic Act No. 9194, An Act Amending Republic Act. No. 9160, Otherwise known as the "Anti-Money Laundering Act of 2001", *at* http://www.amlc.gov.ph/laws/money-laundering/2015-10-16-02-50-56/republic-act-9194.

Recommendation

It is recommended that the AMLA be amended to include provisions on the formation of a central database containing details of persons who were parties to government investigations that have been completed and who have been convicted of AMLA offenses. Recognizing that the NBI serves as the national center for criminal records and hence there may be some overlap. However, an AMLC maintained list specifically pertaining to the misuse of financial payments industry platforms and services would motivate industry to regularly run the list against their customer database stemming from their obligations as a reporting entity.

G. Data Sharing Among AMLA-covered Institutions

In the United States, Section 314(b) of the USA Patriot Act allows financial institutions registered with the United States Department of the Treasury – Financial Crimes Enforcement Network (FinCEN) to share information with one another relating to transactions that the institution suspects may involve the proceeds of one or more specified unlawful activities, and that in sharing such information, the institution would be free from any liability by virtue of a safe harbor provision in the said law.[68]

In the Philippines, financial institutions covered by the AMLA are merely required to report suspicious or covered transactions to the AMLC. However, there is no current legal framework to allow financial institutions from different financial groups to *share* with one another information on these transactions. Establishing a permissible network of data exchange regarding suspicious or covered transactions may allow financial situations to conduct due diligence and transaction monitoring on their clients more effectively and may aid law enforcement in tracking down more efficiently perpetrators of AMLA-related crimes.

We note that Rule 15, Section 7 of the 2018 Implementing Rules and Regulations (IRR) of the AMLA requires financial and designated non-financial businesses and professions (DNFBP) groups to implement a group-wide money laundering/terrorism financing prevention program (MTTP) which allows sharing of information among

[68] For more information, *see Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act*, FinCEN, Jun. 16, 2009, *at* https://www.fincen.gov/sites/default/files/shared/fin-2009-g002.pdf; *See also, Section 314(b) Fact Sheet,* FinCEN, Dec. 2020, *at* https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

financial institutions which are members of the same financial or DNFBP group for more effective anti-money laundering risk management, customer due diligence, and reporting of covered and suspicious transactions. However, it must be noted that such framework exists only for entities within the same financial or DNFBP group. In addition, a covered party may conduct customer due diligence through third-party (also a covered person) reliance pursuant to Rule 21, Section 21(a) of the same rules. Information thus gathered can be used to improve covered and suspicious transaction reporting.

It is submitted that to allow the implementation of this proposed network, concerns on data privacy must be sufficiently addressed. Under the U.S. Patriot Act, before financial institutions intending to exchange data may avail of the safe harbor provision, the financial institutions must register with appropriate government body, notify the body of the intention to exchange the information, and that the institutions implement appropriate safeguards to ensure the protection of the confidential information shared. In the Philippines, these measures can be adopted, perhaps by the AMLC (with the support of the National Privacy Commission) serving as the body tasked with monitoring and managing the network. Moreover, a corresponding amendment to the Data Privacy Act regarding the proposed network may address any data privacy concerns on the sharing of the said information.

Recommendation

It is recommended that the AMLA be amended to include provisions on permissible data sharing among AMLA-covered institutions from different financial groups on covered or suspicious transactions and a safe harbor for institutions participating in the data sharing.

H. Comprehensive Reports for AMLA

At present, the AMLA imposes criminal liabilities on covered persons that knowingly fail to submit covered transaction or suspicious transaction reports.[69] However, there is no criminal liability under RA 9160 as amended for covered persons that submit *incomplete* transaction reports to the AMLC. This is significant because larger and more established financial institutions such as banks and remittance companies would tend to have reports accompanied by more complete data as compared with those with smaller operations. While the AMLC-prescribed template for a transaction report requires a narrative of events on the transaction and

[69] Sec. 4, AMLA.

detailed information on the known parties involved,[70] without an effective criminal sanction on *incomplete* transaction reports submitted by covered persons, certain AMLA transactions could still be undetected despite the reporting requirements.

It must be noted that Rule 22, Section 3.1 of the 2018 Implementing Rules and Regulations of the AMLA requires covered persons to ensure the completeness, accuracy and timeliness of covered transaction reports and suspicious transaction reports, whereas Rule IV, Section 2.A, Table A (D) of the Rules of Procedure in Administrative Cases (RPAC) under Republic Act No. 9160, as amended, categorizes non-compliance with the requirement on the accuracy and completeness of covered transaction reports and suspicious transaction reports as "Less Serious Violations" with administrative penalty of fine of PHP5,000 to PHP100,000 per transaction. However, it is submitted that the risk of incurring such administrative penalties may not be enough to prevent covered persons from submitting incomplete transaction reports to the AMLC.

Significantly, the AMLC recently issued Regulatory Issuance No. 5 which provides procedures for early resolution of administrative cases at the level of the Compliance and Supervising Group and prior to the filing of a Formal Charge under the ALMC's Rules of Procedure in Administrative Cases.[71]

Recommendation

It is recommended that the AMLA be revisited by Congress to include sanctions on submission of incomplete reports, particularly those which do not provide detailed information on the transaction and customer information relating to the covered or suspicious transaction.

I. Amendments to the Data Privacy Act (RA 10173)

RA 10173 provides that information necessary to carry out the functions of public authority shall be exempt from the provisions of the said law.[72] It also provides a specific exception for information necessary for banks and other financial institutions under the jurisdiction of the *Bangko Sentral ng Pilipinas* to comply with the AMLA and other applicable laws.[73]

---

70 *See, AMLC Registration and Reporting Guidelines,* Anti-Money Laundering Council, Manila, Philippines, *at* http://www.amlc.gov.ph/images/PDFs/AMLC%20Registration%20and%20Reporting%20Guidelines.pdf.

71 AMLC Regulatory Issuance No. 5 series of 2020, *at* *http://www.amlc.gov.ph/images/PDFs/ARI%205,%20Series%20of%202020%20-%20Approved%20Enforcement%20Guidelines%20(Original%20Signed).pdf*.

72 Sec. 4(d), Data Privacy Act of 2012 (RA 10173),

73 *Id.* at Sec. 4(f),

To avoid any doubt that the government bodies involved in the investigation and prosecution of OSAEC cases may lawfully share information with one another without fear of penalty, it is recommended that Congress add provisions to the Data Privacy Act that would particularly allow data sharing between government agencies for OSAEC-specific cases. Having in place such provisions in the Data Privacy Act would promote a free exchange of information between and among government agencies such as the AMLC, Department of Social Welfare and Development (DSWD), National Bureau of Investigation (NBI) and the Philippines National Police (PNP) for the purpose of tracking down and prosecuting child offenders.

It is recommended that Congress add provisions to the Data Privacy Act that would particularly allow data sharing between government agencies for OSAEC-specific cases.

Recommendation

The Philippines may also consider adopting the practices of other countries in relation to permissible data sharing between government agencies. In New Zealand, for instance, "Approved Information Sharing Agreements (AISAs) enable personal information to be shared between government organizations for the purpose of delivering public services, without intruding on individuals' rights or creating legal risk."

AISAs are approved and monitored by a centralized government body and require the contracting parties to publish the said AISA and submit regular reports to the pertinent government agencies.[74] Meanwhile, in Australia, a Data Availability and Transparency Act (DATA) is currently being discussed in parliament, which would provide government agencies with an authorization to share government data with accredited users such as other government agencies and non-government entities such as universities.[75]

The National Privacy Commission has noted in an advisory opinion that the provisions of the Anti-Child Pornography Act do not allow for access or opening of a suspected offender's email and/or social media accounts, and that LEAs cannot have access to a suspect's accounts without due process and without a lawful order from the court.[76]

---

74 For more information, *see* Privacy Commissioner, *Privacy Act 2020 – Information Sharing, at* https://privacy.org.nz/privacy-for-agencies/information-sharing/.

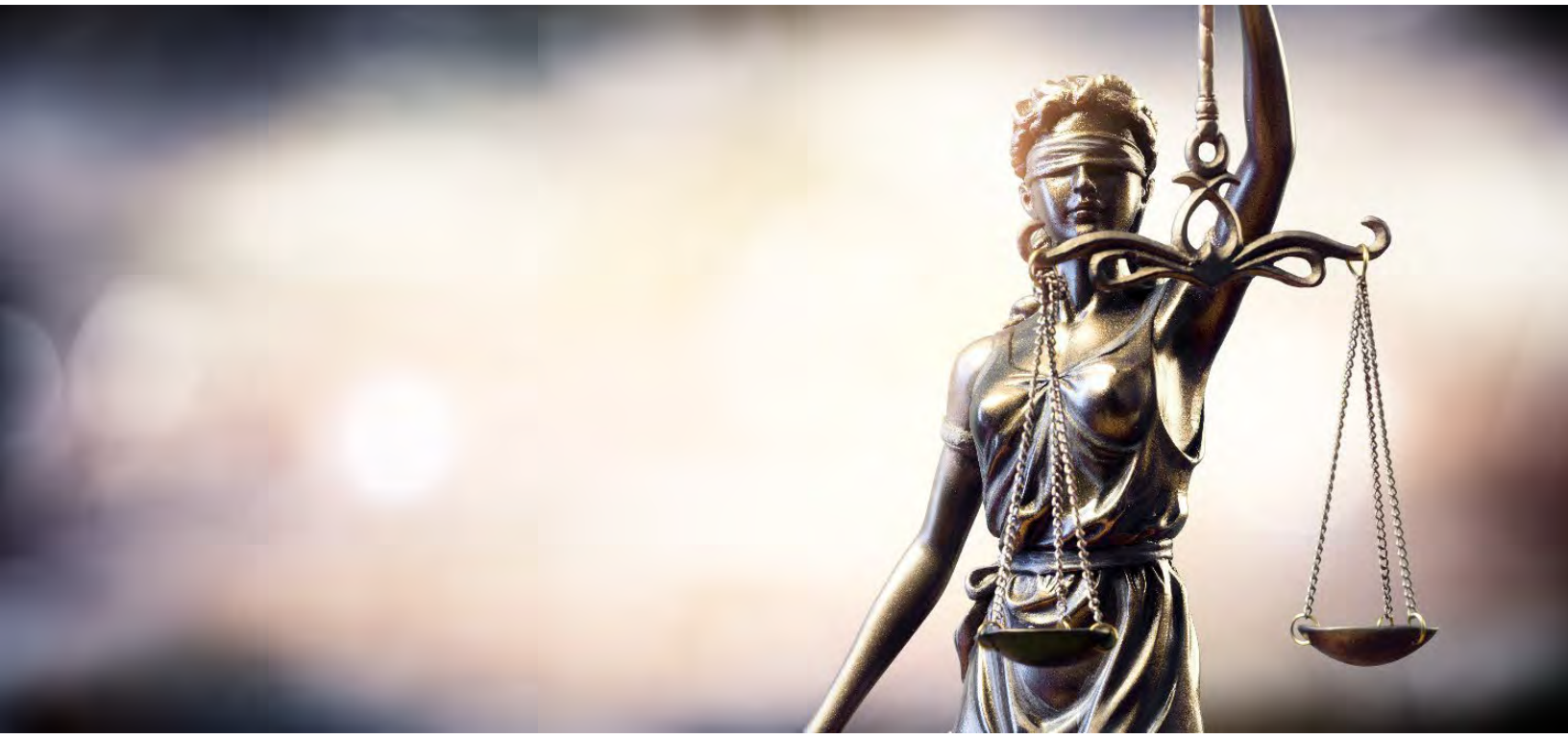
75 For more information, *see* Australian Government, Office of the National Data Commissioner, *Discussion Paper - Data Sharing and Release Legislative Reforms Discussion Paper - Accessibility.pdf,* Sep. 2019, *at* https://www.datacommissioner.gov.au/resources/discussion-paper.

76 National Privacy Commission, Privacy Policy Office, *NPC Advisory Opinion No. 2017-65, at* https://www.privacy.gov.ph/wp-content/files/attachments/advopn/NPCAONo.2017-065.pdf.

Recommendation

Thus, we respectfully recommend Congress to consider adding provisions to RA 10175 for less stringent requirements or an expedited process for the issuance of cybercrime warrants for traffic and content data if the case involves an incident of OSAEC. At present, LEAs are generally required to obtain a valid search warrant before being allowed to search and examine traffic and content data under RA 10175.[77] One amendment that can be introduced is to add a provision requiring a court where the application for the issuance of a search warrant relating to an OSAEC case is filed to act on the application no later than twenty-four (24) hours from its filing, similar to what is provided under Section 11 of the AMLA.[78]

In addition, it is recommended that the Data Privacy Act be amended to provide child-specific provisions, such as more stringent qualifications before the personal information of children may be collected. Moreover, Congress may include in the Data Privacy Act that the expression of explicit parental consent is a requirement before any personal information of a child is collected or shared.



[77] Cybercrime Prevention Act of 2012 (RA 10175).
[78] Sec. 11, AMLA.

Support Bills Currently Under Consideration

House Bill No. 5612

Significantly, House Bill No. 5612[79] authored by Rep. Victor A. Yap seeks to expand the exceptions of the coverage of the Data Privacy Act as follows:

The Act does not apply to the following:

xxx

(F) Processing of information necessary in order to carry out the functions of law enforcement or regulatory authorities, including the performance of the functions of the independent, central monetary authority and information sharing necessary for the investigation and prosecution of child pornography and other forms of child exploitation, in accordance with their constitutionally or statutorily mandated function: Provided, that protection of fundamental freedoms are guaranteed;[80]

xxx

The enactment of the above-quoted portion of House Bill No. 5612 could be used as basis for LEAs to share information with one another freely and thus facilitate enhanced coordination for the purpose of investigating and prosecuting offenders in OSAEC cases.

The same bill also requires that in case of information society providers offering services directly to a child 15 years old or below, the processing shall be lawful only if consent is given by persons exercising parental authority over the child.[81]

Significantly, on 4 February 2021, the House Committee on Information and Communications Technology approved the unnumbered substitute bill to House Bill 5612. It is thus respectfully recommended that Congress earnestly continue deliberations on the unnumbered substitute bill to House Bill No. 5612 and enact the proposed revision to the Data Privacy Act at the soonest possible time.

---

79 House Bill No. 5612 (text as filed), Nov. 25, 2019, Eighteenth Congress, Republic of the Philippines, First Regular Session, *at* https://www.congress.gov.ph/legisdocs/basic_18/HB05612.pdf.

80 *Id.* at Sec. 2.

81 *Id.* at Sec. 7.

House Bill No: 7633

Meanwhile, as previously mentioned, House Bill No. 7633 filed by Representative Fidel Nograles, which has been pending with the Committee on Revision of Laws since 15 September 2020, seeks to amend provisions of RA 9775. In particular, the proposed bill seeks to remove the ambiguous phrase – "Nothing in this section may be construed to require an ISP to engage in the monitoring of any user, subscriber or customer, or the content of any communication of any such person xxx" found on Section 9 of the said law,[82] and to explicitly provide that ISPs have the obligation to install a program or software that ensures that access to or transmittal of any form of child pornography will be blocked.[83] The proposed bill also seeks to add a provision on the exclusion of foreign nationals who have committed any offense of a sexual nature involving children from any form of travel to the Philippines.[84] Congress is respectfully urged to expedite the passage of House Bill No. 7633.

Senate Bill No. 2209

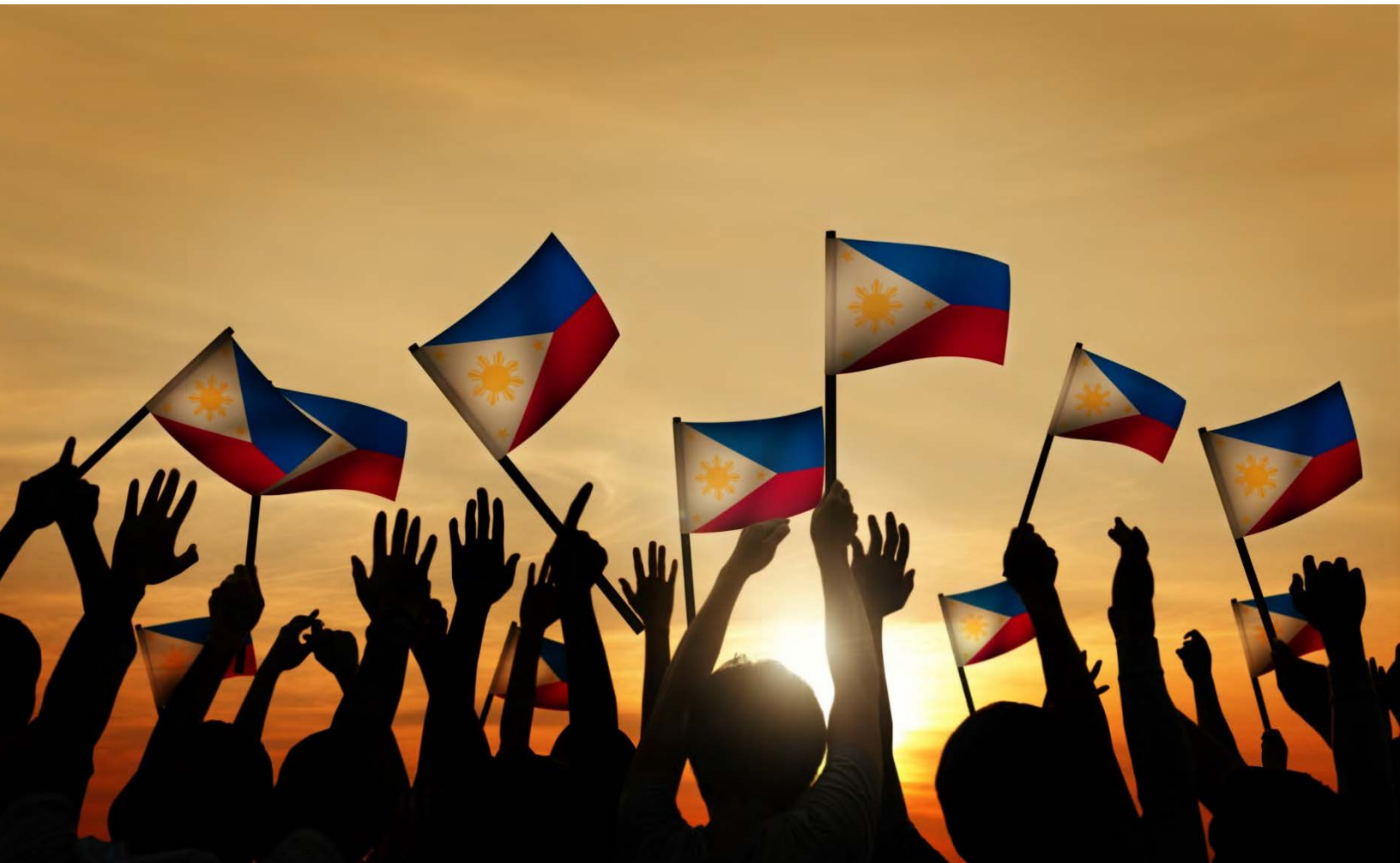
Additionally, Senator Risa Hontiveros introduced Senate Bill No. 2209 which seeks to provide amendments to the Republic Act No. 9775 and Republic Act 9995 by strengthening current protection of children against online sexual abuse and exploitation and providing penalties for their violation. On May 27, 2021, the Senate unanimously passed Senate Bill (SB) No. 2209 otherwise known as the proposed "Special Protections against Online Sexual Abuse and Exploitation of Children Act", previously introduced as Senate Bill 2068. This bill provides additional tools for law enforcement agencies to pursue Filipino and foreign sexual abusers of children, stating that any sex offender convicted overseas would be barred from entering the Philippines. This bill would also require social media networks, internet service providers, web hosting providers, and online payment system providers to create mechanisms to detect, block, and report cases of sexual abuse of children.

82 Sec. 5, House Bill 7633, Anti-Sexual Abuse and Exploitation of Children Act of 2020.
83 *Id.*
84 *Id.* at Section 6.

Conclusion

Despite the presence of laws specifically dealing with the safety and welfare of children, OSAEC cases continue to be on the rise in the Philippines. Based on an analysis of the current legal framework in place, it is believed that the primary solution is **not** to pass additional laws, but to continue to refine those already in place. There is an urgent need for Congress to realign laws like the AMLA, Data Privacy Act, and the Anti-Child Pornography Act, where needed, to allow for improved coordination among government agencies, require a higher standard of accountability on interested and involved stakeholders, and ultimately, lessen the incidence of online exploitation of Filipino children, especially during this time when quarantine measures are in effect.

Despite the presence of laws specifically dealing with the safety and welfare of children, OSAEC cases continue to be on the rise in the Philippines. Based on an analysis of the current legal framework in place, it is believed that the primary solution is not to pass additional laws, but to continue to refine those already in place.



Acknowledgements

Thank you to the members of the APAC Financial Coalition Philippines Working Group for being generous in sharing their time, knowledge, expertise, and experience on the subject of child sexual abuse material.

Australian Federal Police
BDO Bank
Bank of Commerce
Disini & Disini Law Office
Delegation of the European Union to the Philippines
The National Police of the Netherlands
Global Payments
HSBC
International Justice Mission
National Crime Agency, UK
Mastercard
Maybank
Metrobank
MoneyGram
MLhuillier
PayMaya
PayPal
Philippines Anti-Money Laundering Council
Philippines National Police
Philippines National Privacy Commission
Philippines National Bureau of Investigation
Philippines Department of Justice - Office of Cyber Crime and the Inter Agency Council against Trafficking
Philippines Department of Information Communication and Technology
Plan International
Romulo Mabanta
Smart Telecoms
Trend Micro
UNICEF Philippines
U.S. Homeland Security Investigations
U.S. Federal Bureau of Investigation
Visa
Western Union
United Coconut Planters Bank

International Centre™
FOR MISSING & EXPLOITED CHILDREN