# Input for the UN Special Rapporteur's (on the sale and sexual exploitation of children) forthcoming report to the 79th session of the United Nations General Assembly in October 2024

**Date: May 15, 2024**

**Submitting Organization: The International Centre for Missing and Exploited Children**

## About The International Centre for Missing & Exploited Children (ICMEC)

**ICMEC** is a non-partisan, global nonprofit committed to advancing child protection and safeguarding vulnerable children around the world. We have worked for over 25 years to foster systemic change through thought leadership and research, build the capacity of government agencies, engage with the technology and financial industries and relevant regulators and work alongside partners in implementation efforts to keep children safe. ICMEC strives to influence and inspire the global community regardless of country, industry, or profession. We strongly believe the best way for ICMEC to serve children is to openly engage with policymakers, law enforcement, and industry leaders who have a genuine interest in practical solutions to achieve the common goal of building a safer world for all children.

ICMEC's mission is to advance child protection and safeguard vulnerable children by powering the global search for children who are missing, disrupting the economics and mechanics of child sexual exploitation, training partners on the front lines to prevent and respond to cases of missing children, child sexual abuse and exploitation, all in collaboration with key stakeholders.

For more than two decades, ICMEC has worked in over 120 countries empowering the global community with the tools, training, and technology to safeguard children. ICMEC is committed to building comprehensive national prevention strategies and responses to cases of missing and exploited children, including online offenses.

As an organization that trains law enforcement, prosecutors, and judges around the world, ICMEC is aware of the severe under-resourcing in the capacity to investigate Online Child Sexual Exploitation (OCSE).[1] With the overwhelming volume of reports received by the National Center for Missing and Exploited Children (NCMEC), over 90% of which have an international nexus, and the challenges for criminal justice systems to effectively manage that volume, relying solely on enforcement is not realistic or feasible to

[1] *Protecting Our Children Online*, U.S. Senate Committee on the Judiciary (2024), Testimony of John Pizzuro, CEO Raven, *at* https://www.judiciary.senate.gov/imo/media/doc/2023-02-14 - Testimony - Pizzuro.pdf.

protect children.[2] Implementing preventive measures is imperative to a comprehensive approach to child protection.

## FINANCIAL COALITIONS

Law enforcement agencies report that victims of OCSE are primarily based in South and South-East Asia, particularly the Philippines.[3] Subsequently, the Philippines has been considered by UNICEF as the global epicenter of the livestream sexual abuse trade.[4]

Recognizing the need to address the demand-side of commercial OCSE and seeing an opportunity to address it, in 2006 ICMEC established the Financial Coalition Against Child Sexual Exploitation (FCACSE), a groundbreaking alliance between private industry and the public sector in the battle against commercial child sexual exploitation. Made up of leading banks, payment gateways, electronic payment networks, the mission of the FCACSE is to follow the flow of funds and disrupt the payments facilitating this illicit enterprise. Following the success of the US FCACSE, ICMEC launched the APAC-FCACSE in 2009 to broaden the fight against OCSE and develop solutions to counter it, releasing the APAC legal framework research to prevent child exploitation in the region.

In 2017, the first APAC FCACSE Philippines Roundtable brought together representatives from the financial industry, law enforcement agencies, regulatory bodies, and other government and civil society partners. The objective was to inform stakeholders of the OCSE issue, its cross-border and cross-sector nature, and the role that financial and information and communications technology industries to combat the crime.

The collective commitment in the 2017 Roundtable launched the formation of the APFC Philippines Forum to identify the challenges that hindered cross-sector collaboration from legal and operational perspectives. The result was a Position Paper detailing the Philippines' child protection legal framework and outlined the challenges to cross-sector collaboration and operational action between law enforcement, regulatory bodies, and private industry. It laid down recommendations to effectively disrupt OCSE from both legal and operational approaches. Many of ICMEC's recommendations are now in the Philippines' 2022 Anti-Online Sexual Abuse and Exploitation of Children Act, including: Internet Service Providers required to preserve and take down CSAM; internet intermediaries are accountable to create proactive change, law enforcement agents are allowed to have access to non-content data; additional exemptions to the Bank Deposit Secrecy Law; Anti-Money Laundering Council (AMLC) information sharing

---

2 U.S. Department of Justice, *National Strategy for Child Exploitation Prevention & Interdiction – 2023 Report to Congress*, *at* https://www.justice.gov/d9/2023-06/2023_national_strategy_for_child_exploitation_prevention_interdiction_-_a_report_to_congress.pdf.

3 *Online child sexual abuse and exploitation Current forms and good practice for prevention and protection*, ECPAT International, Jun. 2017, *at* https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2018/10/Revue-OCSE_ANG-min.pdf.

4 *Safe from harm: Tackling webcam child sexual abuse in the Philippines, Challenges protecting vulnerable children and prosecuting their abusers*, UNICEF, Jun. 3, 2016, *at* https://www.unicef.org/stories/safe-from-harmtackling-webcam-child-sexual-abuse-philippines.

activities provision; and a national reporting mechanism with only one referral pathway (National Coordinating Center Against Online Sexual Exploitation and Abuse of Children).

## Technology Facilitating the Sexual Exploitation and Abuse of Children

The growing number of children and young people using technology along with rapid technological advancements and the unavoidable interconnectivity of the world have led to greater vulnerability of children to victimization and exploitation and an inevitable rise in OCSE.

Generative artificial intelligence (AI) technology, known as gen AI, is a focal point for nearly every industry and is poised to revolutionize everything as we know it. The increasing popularity of gen AI—capable of generating text and images in response to prompts—raises significant concerns regarding global child safety. With AI enabling the instant creation of sexual content, including featuring children, experts warn that this technology could exacerbate child sexual exploitation and abuse.[5] Yet, the reality is that AI child sexual abuse material (CSAM) is no longer a looming threat; it is already happening.[6]

In 2023 alone, NCMEC received 4,700 reports of content generated by artificial intelligence that depicted child sexual exploitation and abuse (CSEA), a category it only started tracking last year.[7] This number is expected to increase as technology continues to advance.

While concerted efforts are underway to develop technologies and detection methods aimed at preventing the misuse of gen AI for harmful purposes, ICMEC emphasizes the critical need to raise awareness about the ethical and legal implications of gen AI, particularly in the context of CSEA and CSAM, as a crucial step in combating its harmful effects on children globally.

## Challenges In Addressing Digital Technologies

While most countries have existing laws that offer some layer of child protection, the continuous evolution of the internet makes it increasingly difficult to anticipate and combat the corresponding rise in gen AI CSAM cases. In March 2024, the United States Federal Bureau of Investigation (FBI) issued a Public Service Announcement (PSA) cautioning against the use of gen AI to produce CSAM, warning that such actions are illegal under U.S federal law.[8] The PSA emphasized the accessibility and realism of generated content, underscoring the need for legal consequences associated with its production, distribution, and possession.

---

5 Sarah Gardner, *AI is Supercharging the Child Sex Abuse Crisis. Companies Need to Act*., Apr. 29, 2024, Tech Policy Press, at https://www.techpolicy.press/ai-is-supercharging-the-child-sex-abuse-crisis-companies-need-to-act/.

6 DeseretNews, *AI child pornography is already here and it's devastating*, May 1, 2024, *at* https://www.deseret.com/u-s-world/2024/05/01/artificial-intelligence-complicates-child-pornography-battle-csam/.

7 Katie McQue, *Child sexual abuse content growing online with AI-made images, report says*, The Guardian, Apr. 16, 2024, *at* https://www.theguardian.com/technology/2024/apr/16/child-sexual-abuse-content-online-ai

8 United States Federal Bureau of Investigation, *Alert Number: I-032924-PSA – Child Sexual Abuse Material Created by Generative AI and Similar Online Tools is Illegal*, Public Service Announcement, Mar. 29, 2024, *at* https://www.ic3.gov/Media/Y2024/PSA240329.

There is also a misconception that CSAM generated by AI poses no harm, and is not illegal, since the children pictured aren't real and the images are 'fake.' Yet AI-generated images of child sexual abuse are real and distressing,[9] and without access to the data used to train the AI generator, it is impossible to prove that there's no actual imagery of abuse. It is also possible that AI CSAM uses images of real people to create such 'fake' images. AI isn't simply 'made up,' but is rather the technological curating and repurposing of large datasets of images and text to create specific content. Therefore, the distinction between 'real' and 'fake' is difficult to decipher.[10]

There have been proposals to implement safeguards and regulations around AI models to prevent the generation of sexually explicit content, particularly CSAM. While these measures could mitigate the proliferation of AI-generated CSEA, they fail to address the problem of how technology enables a culture of sexually exploiting children.[11] Many AI models were trained on datasets containing CSAM because it is readily accessible on the internet. Therefore, it must fall upon the creators of these datasets and training models to rectify them and implement effective filters and safeguards capable of detecting and suppressing harmful content.[12]

The proliferation of AI-generated CSAM hinders the identification of real child victims,[13] prompting concerns among experts about the risk of authentic CSAM being obscured amidst this flood of "synthetic" content.[14] AI CSAM amplifies the demand on policing and law enforcement to distinguish between actual instances of child abuse and generated representations, potentially diverting resources from rescuing children in harmful situations.[15]

## MECHANISMS TO SUPPORT PARTICIPATION

### *Creation of Specialized Units for Investigation and Prosecution*

The migration of sexual offenders to virtual space, using the internet as a means of attracting potential child victims of human trafficking and child sexual exploitation has created the need for technological responses to technology-related crimes. Many countries' laws do not yet have regulations allowing police, judges, and prosecutors to criminally prosecute online sexual offenders and those who generate AI CSAM.

---

9 Angus Crawford and Tony Smith, *Illegal trade in AI child sex abuse images exposed*, BBC NEWS, Jun. 28, 2024, *at* https://www.bbc.com/news/uk-65932372.

10 DeseretNews, *supra* note 6.

11 Sarah Gardner, *supra* note 5.

12 *Id.*

13 Angus Crawford and Tony Smith, *supra* note 9.

14 Katie McQue, *supra* note 7.

15 DeseretNews, *supra* note 6.

In addition, in developing coutnries Prosecutor's Offices responsible for investigating technology-related crimes lack the needed specialized training. The increase in cases of AI-generated CSAM has diminished the capacity for an effective response on the part of those responsible for the investigation.

The creation of specialized multidisciplinary units, including technical forensic personnel specialized in computer science, prosecutors specialized in child rights and cybercrimes, and psychologists specialized in forensic interviews in the police or prosecutor's offices responsible for crimes against children or human trafficking, is one of the best practices for effective criminal prosecution. Currently, most countries do not have specialized units to investigate OCSE let alone AI-generated CSAM.

In 2020, ICMEC developed a model framework providing law enforcement and judicial officials guidance on best practices to create specialized units to investigate technology-facilitated crimes against children. The Model Framework contains sections, including key terms and definitions; preliminary assessments prior to setting up a unit; budgetary and financial considerations; personnel allocation; and workspace and equipment.

The Model provides information related to training and capacity building on investigative techniques, case management, victim identification, and other relevant procedures that are core to the effective and efficient operation of a specialized unit. As arrests alone cannot resolve the problem of technology-facilitated OCSE and AI CSAM, the Model also addresses training law enforcement, prosecutors, and other related-professionals, and educating parents, youth, and the community about the potential dangers of online activity.

In July 2022, ICMEC and CyberPeace Foundation announced a collaborative initiative to combat OCSE in India. Funded by the U.S. Department of State, this four-year endeavor sees the establishment of specialized OCSE police units in four regions and one city throughout India. It will also encompass the provision of training, specialized equipment and software, as well as technical assistance to support OCSE investigations. ICMEC will also conduct training programs for prosecutors and judges in these five locations. Furthermore, ICMEC initiated the establishment of dedicated OCSE police units in Indonesia.

## *Specialized Training for Law Enforcement, Prosecutors, and Judges*

Training on the presentation and assessment of digital evidence in cases related to technology and children is an area that should be strengthened. Law enforcement and prosecutors must receive training on managing online undercover operations, computer forensics, victim identification, and following financial trails of trafficking. Law enforcement must also be fluent in the proper handling of digital evidence and online investigative tools and how to use them to successfully bring cases to trial and conviction.

Training for judges on current technological tools to extract and review digital evidence and receive international CSAM, including AI CSAM, cases should be implemented (i.e., hotline/tipline reports, monitoring tools for the exchange of CSAM on P2P networks). The role of judges in proactive investigation processes is vital, especially when the information required by prosecutors and police must be requested from national ISPs or international technology providers require a court order. Offenders can quickly eliminate the needed digital evidence, so speed in the issuance of court orders can be decisive in locating possible victims and offenders.

## *Technology and Tools*

Technology has undoubtedly exacerbated the risks to children of abuse and exploitation but also provides avenues to build tools crucial to recovery and safeguarding. For example:

- Reporting mechanisms (i.e., a single national portal and/or clearinghouse) where the public can easily report cases of CSEA, including AI CSAM, provide information, and leads regarding where such content is hosted or is being shared/distributed enables law enforcement to initiate a case where confirmed evidence exists. ICMEC partnered with the Internet Watch Foundation (IWF) to establish a joint Reporting Portal that allows anyone, anywhere to report child sexual abuse material online. The online portal, hosted on ICMEC's website, allows concerned internet users who do not have access to their own national reporting mechanism to easily and anonymously report CSAM on the internet.

- ICMEC's GMCNgine™, an AI platform allowing users to digitally distribute missing child posters, use facial recognition to match missing child photos against data from the clear and dark webs, and create geo-targeted alerts of missing children. In assisting with the quicker recovery of children reported missing, ICMEC endeavors to lower the vulnerability of children at risk of being abused, exploited, and trafficked.

## *Collaboration and Prevention*

OCSE is an evolving digital crime that transcends borders. ICMEC's region-wide APAC-FCACSE, aimed to foster this cross-border and cross-sector collaboration is indispensable in the fight against OCSE.

With particular focus on the financial aspect, one of the largest potential sources of intelligence is banks. However, they are often prevented from legally sharing information across borders within their organization or with relevant authorities such as law enforcement and regulators. The private sector, financial institutions, and the government should forge public-private partnerships to safeguard the integrity of the financial system. Regulated financial entities such as banks and other financial institutions have invested in human resources, information technology, and in training to generate financial intelligence related to OCSE. The government has been playing its part, especially in strengthening OCSE legal frameworks; however, pooling these resources would allow the private and public sectors the

opportunity to generate quality intelligence information, develop training modules, and undertake capacity-building activities to further develop and expand their respective expertise.

Recognizing the indispensable role of the private sectors, particularly the financial and information and communication technology (ICT) actors, in working with law enforcement to combat this crime, only collaborative action across stakeholders can preempt and prevent trade in AI CSAM. Ultimately, both the public and private sectors must recognize the cross-sector nature of OCSE and the importance of promoting a genuine culture of trust, partnership, and cooperation among one another to achieve their shared objectives of combatting OCSE.

## *Strengthening Legal and Policy Frameworks – Highlighting Country Examples*

In the Philippines, its 2022 Anti-OSAEC Act already contains specific provisions on "deep fakes". Deepfakes are an emergent type of threat falling under the greater umbrella of synthetic media which creates realistic videos, pictures, audio, and text of events which never happened.[16] Deepfakes have been increasing in recent years, with an app which can virtually strip women naked receiving 38 million hits the first eight months of 2021.[17] With the emergence of deepfakes, identities of individuals can be exploited for malicious purposes, fabricated videos can damage reputations, and, for children cause re-victimization. Such deepfakes involving children may generate novel abuse of an existing victim, generate novel material whether derived from a child's likeness of a specific child or an unidentified child, or generate novel abuse where new offenders are plugged in. The Philippine's Anti-OCSAEC Act defines image-based sexual abuse (ISA) as a form of technology-facilitated sexual violence, including […] "the use of artificial intelligence to construct 'deepfake' pornographic videos". Further, the said law's mere definition of OCSE covers sharing of image-based sexual abuse, which in turn includes sharing of deep fake materials.

It is important for criminal justice system actors to acknowledge that the use of deepfake technology in the creation of child sexual abuse materials is just as harmful as livestreaming or other forms of OCSE. In Canada, a man who created synthetic, AI-generated child sexually exploitative material was sentenced to prison, with the judge calling the use of deepfake technology "chilling". Further, the judge ruled that "the children whose bodies appeared in the videos had their sexual integrity violated again" and that such AI-generated images "not only humiliate the victims, violating their dignity and privacy, but people could also seek those children out to sexually assault them."[18]

---

[16] United States Department of Homeland Security, *Increasing Threats of deepfake Identities*, *at* https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf.

[17] Shiona McCallum, *Revenge and deepfake porn laws to be toughened*, BBC, Jun. 27, 2023, *at* https://www.bbc.com/news/technology-66021643.

[18] Jacob Serebrin, *Quebec man who created synthetic, AI-generated child pornography sentenced to prison*, CBC, Apr. 26, 2023, *at* https://www.cbc.ca/news/canada/montreal/ai-child-abuse-images-1.6823808.

In 2006, ICMEC developed the first *Child Sexual Abuse Material: Model Legislation and Global Review* to examine national laws prohibiting CSAM, increase global awareness and concern, and enable governments to adopt/enact much-needed legislation to protect children. Currently in its 10th edition the report has over close to two decades encouraged nation-states to review and strengthen legislation around child protection. Similarly, ICMEC later developed an *Online Grooming of Children for Sexual Purposes: Model Legislation and Global Review* in 2018. These tools look at a core set of criteria to fully understand the national legislation on the issues and include a series of fundamental provisions essential to a comprehensive legislative strategy to combat CSAM and online grooming, including legal definitions; defining the offenses; mandatory reporting; industry responsibility; and sanctions/sentencing.

ICMEC research and tools are utilized by policymakers, law enforcement agencies, child protection experts, industry partners, and others working to improve the national response on the issues through the development of legislation and new criminal code provisions as well as driving legislative reform. We encourage relevant stakeholders in each country to make use of these tools as a means of understanding the issue broadly, assessing the sufficiency of a country's legislative measures, and comparing those measures across the region and/or globe to foster improved child protection mechanisms and greater allocation of resources.

## CONCLUSION

Evolving digital technologies have undoubtedly revolutionized various aspects of life, but have also brought about unprecedented challenges, particularly in protecting children from OCSE. The emergence of generative AI technology, capable of producing highly realistic yet fabricated, and often manipulated, content, poses a significant threat to children. Despite efforts to develop detection methods and regulations, the prevalence of AI CSAM continues to escalate, complicating the identification and protection of victims of real exploitation and abuse.

Collaborative efforts between governments, law enforcement agencies, and the public and private sectors, are crucial in addressing these challenges and enhancing online child protection measures. By strengthening legal frameworks, providing specialized training, leveraging technology for detection and prevention, and fostering proactive collaboration, we can combat OCSE and protect children online.