International Centre™
FOR MISSING & EXPLOITED CHILDREN
AUSTRALIA

Submission from the International Centre for Missing and Exploited Children (ICMEC) Australia re:

Existing and Emerging Sexually Exploitative Practices against Children in the Digital Environment

Special Rapporteur on the Sale and Sexual Exploitation of Children

May 2024

Executive Summary

ICMEC Australia is honoured to contribute to the ongoing efforts of the United Nations Special Rapporteur on the Sale and Sexual Exploitation of Children. This paper addresses the call for input regarding Existing and Emerging Sexually Exploitative Practices against Children in the Digital Environment. Our submission seeks to enhance understanding and promote a coordinated global response to counter the escalating challenge of technology-facilitated child sexual exploitation.

In this report we build upon ICMEC Australia's earlier submission provided during the Special Rapporteur's country visit in late 2023, set to be presented at the 58th session of the Human Rights Council in March 2025.

Our organisation collaborates with a range of stakeholders including law enforcement, financial services, tech companies, and child protection agencies, striving to develop innovative solutions to protect children in this rapidly evolving digital age. The growing prominence of Artificial Intelligence has presented both a threat and opportunity when it comes to child protection, and it's important for the technology to be understood globally, sooner rather than later, so that more children can be protected.

What does ICMEC Australia do?

The sexual abuse and exploitation of children is one of the fastest-growing crimes in the world and requires a strong response from a variety of sectors. In our digital age, online child sexual exploitation and abuse is rapidly growing - faster than we can respond - which challenges us to mount a formidable response. This isn't just a crime; it's a violation of innocence that knows no borders, thriving in darkness.

At ICMEC Australia, we bring together the public and private sectors to turn up the lights and fight this crime together. Artificial Intelligence (AI) has emerged as both a beacon of hope and a source of peril, especially when it comes to child sexual abuse and exploitation facilitated online. ICMEC Australia is working to navigate the nuanced role AI plays in both facilitating and fighting online child sexual exploitation. We believe understanding this new landscape isn't something that should be left solely to tech companies, regulators and government in siloes. Collaboration across sectors is key to finding solutions for the protection of children.

Technologies Facilitating Sexual Exploitation and Abuse

Offenders of child sexual exploitation manipulate any technology available to them to harm children. With the growing accessibility and capability of Generative AI, offenders have capitalised on this new technology.

These technologies are capable of creating or manipulating digital content at an unprecedented scale. Unfortunately, this includes the production of digital representations of child sexual abuse. These models, when trained on vast datasets, can inadvertently learn from inappropriate sources unless strictly monitored and controlled. For instance, recent reports from law enforcement agencies have illustrated cases where GenAI has been used to create hyper-realistic images and videos, complicating the task of distinguishing real abuses from generated content.

Generative AI platforms are increasingly being weaponised against children in several alarming ways:

● Creation of Deepfake Content

Perpetrators use AI to generate lifelike images or videos of children who have not been abused, posing significant risks to those depicted.

● Production of New Abuse Material

AI is used to create new child sexual abuse materials (CSAM) using existing images of victim-survivors of sexual abuse, revictimising children, or creating material of children who are not victims of contact offending.

● Train open-source models on CSAM

Models can be downloaded and further trained on CSAM specific datasets and be used offline, without any oversight from the corporations that build them.

These emerging threats highlight the dual use of AI technologies, necessitating urgent and informed responses to prevent their misuse. The realities of this crime are sobering:

The Internet Watch Foundation found for one dark-web forum:

- **20,254** AI-generated photos
- **12** analysts spent **87.5** hours assessing **11,108** of these images
- **2,975** were criminal
- **2,562** of these were realistic enough to be treated in the same way as CSAM
- The thousands of other material were non-criminal in nature, but contained children.

Practical recommendations for preventing the sexual exploitation and abuse of children online

For Governments

Governments play a pivotal role in combating online child sexual exploitation. We recommend the introduction of specific laws that rigorously regulate the use of generative AI technologies for insipid purposes, accompanied by severe penalties for violations. Additionally, compulsory AI ethics training within industries could substantially mitigate risks. We also emphasise the benefits of widespread public awareness campaigns that educate citizens about the risks of digital exploitation and the critical importance of reporting suspicious activities to authorities.

- Direct collaboration with the technology and AI industry is crucial to harness these technologies for prevention and detection of child exploitation while understanding their potential misuse.

- Funding innovative projects that aim to detect and disrupt the ability for technologies to be manipulated before they reach and harm children.

For Technology Industry and Online Service Providers

For the technology industry and online service providers, implementing technical safeguards is non-negotiable. This could include the integration of digital watermarking to indicate AI-generated material and advanced content filtering technologies that automatically detect and block the dissemination of exploitative content. Moreover, establishing an industry-wide standard for ethically developed AI could serve as a benchmark, similar to social/environmental or quality certifications, ensuring that all players adhere to high ethical standards.

In late 2023, LAION-5B, a dataset of 5 billion images was found to have contained over 1000 URLs containing CSAM, according to a Stanford study.

This dataset is used to train Stable Diffusion's model, a prominent image generator. Midjourney, another image generator, uses the same dataset to train its models.

- Implement AI solutions to proactively detect and remove CSAM from platforms.

- Ensure that AI models are developed using datasets free from exploitative content and incorporate protections to prevent the creation of CSAM.

Gaps in Current Frameworks

The rapid growth of new and emerging technologies poses significant challenges to coordinating a collaborative, international response to this issue. A glaring disparity exists in the technological and investigative capabilities across different regions. It's important to build the capacity of law enforcement agencies globally to ensure that they are well-equipped to respond to this changing crime type. It's our mission at ICMEC Australia to boost the capabilities of our partners, including law enforcement working on the frontlines against child sexual exploitation, and we aim for this mission to expand across borders.

Transparency issues are also key. It's important for tech companies to be forthcoming about the capabilities and limitations of their technologies in combating child sexual exploitation. Moreover, regulation and legal frameworks need continual updating to maintain pace with technological advancements. Streamlining processes and the capacity to update regulations alongside advancements in technology and threats as they emerge, is critical to protecting children.

Challenges for Law Enforcement

Law enforcement agencies face significant challenges, notably in keeping pace with rapidly evolving digital technologies. Specialised training programs in digital forensics and AI-generated materials will be crucial for modern policing. The need for enhanced international data sharing is evident, balanced with stringent respect for privacy and data protection laws.

Law enforcement agencies face numerous hurdles, including:

● Privacy vs. Safety

Balancing privacy with the need for surveillance tools to detect offenders.

● Rapid Proliferation of Material

AI facilitates the fast creation and dissemination of CSAM, making it challenging for law enforcement to investigate all reports.

● Quality of AI-Generated Material

The increasing realism of AI-generated images complicates the distinction between real and synthetic abuse material, hindering investigation efforts.

Addressing the complexities of Artificial Intelligence when it comes to protecting children from abuse

ICMEC Australia has a vision that every child can grow up free from abuse and exploitation. Our work uniquely focuses on combating technology-facilitated child sexual exploitation and abuse - a crime that affects far too many children in both Australia and beyond our borders. We believe that cross-industry collaboration is key to protecting more kids from harm - especially in the face of dramatic technological advancements, such as those we are seeing in AI. This is a global problem that requires a global solution to ensure our children are adequately protected.

ICMEC Australia has identified that there is a key gap at the intersection of child protection and Artificial Intelligence. In direct response to this, we have established Australia's first Working Group of leaders from NGOs, law enforcement, academic, and other public sector partners all dedicated to advocating for safer outcomes for children in the age of AI. The SaferAI for Children Coalition is an amalgamation of cross-industry stakeholders, dedicated to collaborating with one another to navigate AI advancements via a child protection lens - something that no other not-for-profit organisation has taken leadership on nationally.

Collaborating for a safer world for kids

Our vision is a world where international cooperation and technological innovation continuously evolve to protect children from exploitation. ICMEC Australia emphasises initiatives that promote innovation in protective technologies and legal frameworks, ensuring that they keep pace with the evolving digital landscape. By uniting global efforts and fostering an environment of continuous improvement, we can hope to achieve significant strides in the fight against child exploitation.

ICMEC Australia is open to further consultation in this space, eager to continue further discussions with our international partners to keep child protection in the digital age a foremost concern.