June 2024

Statutory Review of the Online Safety Act 2021

International Centre for Missing and Exploited Children Australia (ICMEC Australia)

The International Centre for Missing and Exploited Children Australia (ICMEC Australia) appreciates the ongoing efforts of the Office of the eSafety Commissioner to champion children's rights in the digital age. We welcome the opportunity to provide a submission for this Statutory Review of the Online Safety Act 2021 (the Act).

At ICMEC Australia, we're turning the use of online technology to abuse children on its head. As a not-for-profit organisation, we support those working on the frontlines of fighting child sexual abuse by using online technology and data-driven approaches to detect, report, prosecute, and prevent child sexual exploitation.

It's important to recognise that Australia has made significant progress when it comes to online safety, and ICMEC Australia applauds Australia's eSafety Commissioner in leading significant change in this space.

Importance of the Online Safety Act

As a cornerstone of Australia's commitment to protecting our children in the digital age, ICMEC Australia supports the foundations laid out by the Online Safety Act 2021. We advocate for the continual evolution and evaluation of the Act, including expanding its objectives, ensuring comprehensive coverage of the online industry, enhancing enforceability of safety standards, and refining the flexibility and inclusiveness of the code drafting process. These steps will further protect Australians from online harms. We commend the Australian Government's foresight that the online world has already evolved, and the resulting decision to bring forward the independent review of the Act.

Given the borderless nature of the internet, international collaboration is crucial to the fight against online child sexual exploitation (CSE). Leveraging emerging technologies for protective measures, and developing innovative solutions (that meet both human rights and privacy concerns and requirements) is essential if we are to outpace offenders who exploit these platforms. While ICMEC Australia recognises the importance and legitimacy of privacy concerns, we also wish to stress through this submission that adopting a stance that utilises technology to keep children safe from harm should be a priority above all else.

ICMEC Australia believes there is room to both affirm and expand the objectives of the Act to not only respond to online harms, but to proactively prevent them. It's widely known that prevention is key when it comes to keeping children safe. Ensuring that the Act can be reassessed and adapted to possibly broaden its scope is imperative to protecting our most vulnerable. It's vital that all significant areas influencing user safety are comprehensively addressed to maintain the relevance and impact of the Act.

Recommendation 1: Embed explicit reference to Artificial Intelligence (AI) into the Online Safety Act and the eSafety Commissioner's powers.

The growth of AI in the last 12 to 18 months has been significant. We know this technology will only continue to increase in capability and availability, and have a wider impact on our society.

ICMEC Australia emphasises the explicit need for:

- Reference to AI in the Act. While AI has already cultivated innovation across the globe, it also poses many challenges – including how the technology can be used to generate child sexual abuse material. Without explicit mention of AI in the Act, there is a risk that the eSafety Commissioner may be limited in ability to pursue legal recourse for AI being manipulated for insidious purposes. This inclusion will grant the eSafety Commissioner additional powers to regulate AI generated materials in Australia.

- AI models to be safe for children – including how they are designed, built, and in the outputs they provide. Embedding obligations into legislation will encourage companies to adhere to eSafety's safety-by-design approach, allowing Australia to set a global standard for child protection in the age of AI.

ICMEC Australia draws attention here to the European Union's recently adopted AI Act, the first legal framework on AI. The comprehensive nature of this legislation includes exemptions for advanced AI tools to be used in the investigation of some of society's most heinous crimes – like child abuse and exploitation – something which should be considered in Australia's legislation.

Recommendation 2: Promote a holistic approach to online safety that emphasises collaboration and initiatives that span various sectors.

At ICMEC Australia, we work closely with those on the frontlines of child protection. The continued integral role of law enforcement to investigate crimes, prosecute offenders, and remove children from harm should not be underestimated. The Act should encourage technology's application in law enforcement contexts to improve child abuse investigations.

In today's technology-driven society, child protection also has relevance across various sectors, including social media, internet service providers, and financial services. Each of these industries have a crucial role to play in supporting law enforcement's efforts to protect children.

The regulated financial sector plays this role by reporting suspicious financial transactions and collaborating closely with regulators, industry peers, and law enforcement. ICMEC Australia has helped facilitate these collaborations and detection capabilities through working groups and data products that promote the sharing of vital information and insights.

We know there is an intersection between CSE and the financial sector, as offenders both in Australia and overseas share images, videos, and livestreams of the abuse and exploitation of children for commercial purposes. These offences have a financial footprint and significantly impact children all over the world. The National Centre for Missing and Exploited Children (NCMEC) reported in 2022 that 79% of offenders of sextortion (sexual extortion)

were seeking money from the victim. With this footprint comes an obligation for the financial sector to take substantive action to prevent their systems from being used to enable CSE. It's clear, therefore, that the response to online safety must span across all sectors whose products and services are inadvertently used by bad actors to commit CSE.

The severity and growing prevalence of online child sexual exploitation makes it a high priority for financial services institutions. To ensure comprehensive knowledge about this crime type and its associated typologies, ICMEC Australia has recently begun delivering Corporate Awareness Programs to financial services and other corporate entities. This program addresses a critical gap in the corporate sector's understanding of the human aspect of CSE, and what role they can play, which is essential for navigating an effective response and raising awareness.

Another key pillar in the fight against online exploitation is the role of internet service providers (ISPs) and telecommunication companies. Like financial services, these providers' platforms are used by offenders, both overseas and within Australia to commit online child exploitation crimes. Now, more than ever, telecommunication and internet service providers must actively work towards online safety by prioritising detection efforts and information sharing. eSafety plays an important role in supporting ISPs to proactively reduce and prevent exploitation from occurring via their services.

Offenders of CSE manipulate a wide breadth of technologies, and understanding the whole threat picture helps us form a robust response. With this knowledge at the forefront of our efforts to emphasise collaboration, ICMEC Australia has been working keenly with financial institutions, payment platforms, and law enforcement agencies through our Collaboration Working Group. Expanding on the success of the APAC Financial Coalition against CSE, established by ICMEC in Australia in 2013, the Working Group has since spearheaded several innovations with a tangible impact in protecting children.

As technology changes, it is critical that public awareness increases alongside it. This includes education for parents and children around new technologies (including AI and the Metaverse) as they emerge – how they work, their benefits, and their risks. Enhanced online safety training and continuous awareness-raising efforts are vital to a comprehensive response. For instance, schools need to be equipped with the latest information to effectively discuss and implement safety measures with children. The education arm of the Office of the eSafety Commissioner is key to these efforts to prioritise prevention.

Moreover, support for non-government organisations that work towards these goals is essential to sustain and expand these efforts to achieve a safe online environment for children. Online safety requires the participation of many sectors and organisations to be truly effective. For example, ICMEC Australia has been partnering with industry, government, and not-for-profits for several years on multiple initiatives.

At ICMEC Australia, we prioritise a proactive and innovative approach to child protection, as demonstrated through our recently established SaferAI for Children Coalition. Bringing together a variety of sectors including academics, law enforcement, NGOs, and other public

sector partners, the Coalition is an example of the impactful role that collaborative initiatives can have in keeping children safe.

Similarly, our Data Products team has collaborated with world-leading data partners who are equally invested in the detection and prevention of child sexual abuse. By transposing millions of data artefacts into a localised product, ICMEC Australia's data product, *Lighthouse* allows Australian banks and payment platforms to enhance their capabilities in the fight against those who prey on children.

Recommendation 3: Provide explicit support for victim-survivors of technology facilitated abuse, noting how complex the crime type is and the severity of its impact.

Public discourse can sometimes overlook the severity of online abuse by incorrectly assuming a non-physical or 'lesser' nature of offending. However, research and experts consistently emphasise the profound psychological, emotional, and physical effects of online child sexual exploitation.[1] It is also important to note that oftentimes online technology is the mechanism used to commit in-person, contact abuse against children.

Working towards holistic online safety requires comprehensive recognition and support for victim-survivors. It's crucial to consult with victim-survivors to understand their diverse experiences and protect future victims from harm. ICMEC Australia and our NGO colleagues recognise the need to assist victim-survivors of online-facilitated abuse, and lend our support in furthering this important process.

Recommendation 4: Emphasise the obligation for all platforms to prioritise online safety and ensure this is reflected in the eSafety Commissioner's powers.

With regards to the management of online safety through service providers' terms of use, ICMEC Australia sees that while such terms are crucial, they cannot be solely relied upon to ensure a safe online environment for our children. It is vital that the Act establishes clear and enforceable safety obligations that apply universally across platforms, independent of individual terms of use.

To be effectively put into practice, these obligations need to transcend all platforms – from large to small. Child sexual exploitation isn't only committed on the most popular social media platforms. Unfortunately, we know that abuse can take place across numerous technology sources.

Our frontline partners repeatedly report a shift of offending behaviour to new, smaller platforms as the most popular platforms become increasingly more restrictive and widely regulated. ICMEC Australia agrees that there is merit in the concept that regulatory obligations could be tailored based on the reach and risk profile of service providers. Such an approach could proportionately allocate responsibilities, potentially imposing stricter obligations on platforms that have extensive reach or where the risk of harm is higher.

[1]https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2023.1281996/full

Commercial platforms should be required to mitigate the carriage of illegal content on their services. The Act could create a significant impact in Australia in this regard, and encourage ISPs to share trends and insights of suspicious actors with law enforcement and other industry stakeholders. The success of sector-based collaboration and information sharing has been demonstrated by other industries' involvement, such as through our Financial Crime Collaboration Working Group. By bolstering collective knowledge, we can significantly enhance the detection and prevention of online exploitation.

The Act could also urge ISPs to regularly review the lists of 'Worst Of' online sites and platforms available from international law enforcement bodies such as Interpol.[2] There are also opportunities to encourage ISPs to work closely with law enforcement investigating child-related offences without incurring additional costs, such as those associated with subscriber checks and ISP data requests.

A duty of care requirement should be central to this comprehensive regulatory approach, ensuring that all online service providers, regardless of size, prioritise child safety. This obligation should reflect the best interests of the child above all else. The recent announcement from Twitter/X that they will allow pornography on their popular, high-traffic platform, requires guardrails and considerations for how to mitigate the impact of this on children.

It is concerning that some platforms seem to be relaxing some of their safeguarding rails, or reducing trust and safety resources, while risks to children grow. Other recent instances of non-compliance by major platforms to adhere to eSafety's requests and recommendations unfortunately highlights significant gaps in our legislation as it stands.[3] Severe non-compliance should warrant substantial penalties, including potential disruptions to an online service's ability to generate revenue in Australia. Australia could take inspiration from international legislation in this regard, including the UK's Online Safety Act 2023. This amendment would align with the eSafety Commissioner's role in enforcing strict adherence to online safety regulations. Profits and privacy should never trump safety and security.

In this same vein, ICMEC Australia supports the ongoing industry consultations and the implementation of the age verification trial that was suggested by the eSafety Commissioner's 2023 Age Verification Roadmap. The relationship between early access to explicit content and the development of harmful sexual behaviours is well-documented, necessitating stringent measures to prevent underage access to such material.[4]

Conclusion and ICMEC Australia's Priorities

ICMEC Australia is dedicated to working alongside the Office of the eSafety Commissioner towards the protection of children in digital environments.

---

[2] https://www.interpol.int/en/Crimes/Crimes-against-children/Blocking-and-categorizing-content
[3]https://www.theguardian.com/technology/article/2024/jun/05/x-elon-musk-vs-australia-esafety-commissioner-wakeley-church-stabbing-footage
[4]https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7147756/

We strongly support the work of eSafety and the Commissioner, and welcome the strengthening of the remit and enforcement mechanisms available to the Office. Australia has been a global leader in the establishment of an effective online safety regulator. As the risks and potential harm to children grows rapidly in online environments, so must our response. We need to urgently expand and extend regulation to protect children.

We are eager to lend any of our relevant expertise to the review of the Online Safety Act 2021, drawing on insights from our diverse stakeholder groups. Being a collaboration focused organisation means we have partners from across the corporate sector, law enforcement, academia, and other not-for-profits, all dedicated to child protection. We know that this work cannot be accomplished if we work in silos. Our aim is to bring people and sectors together to fill gaps and keep children safe.

ICMEC Australia looks forward to the outcomes of this independent review, and are committed to supporting the implementation of its recommendations in order to protect children from abuse and exploitation. We believe that this review will prioritise the safety and wellbeing of children, ensuring Australia continues to set global standards in online safety.

———

Anna Bowden
Chief Executive Officer
ICMEC Australia
[redacted]