Australian Government
Attorney-General's Department

February 2024

Submission

To the eSafety Commissioner's Industry Standards Public Consultation

Attorney-General's Department.

Content warning: This submission includes statistics and other information relating to child sexual exploitation and abuse. If you, or someone you know, has been impacted by child sexual abuse or is concerned about a child's safety, there are services and resources available to help. Please visit www.childsafety.gov.au for more information.

Overview

Scope of submission

The Australian Government is committed to strengthening Australia's policy, regulatory and criminal justice frameworks to prevent and respond to child sexual abuse in all settings, including online.

Australia has a comprehensive framework of offences relating to child sexual abuse committed online and overseas, including in relation to child sexual abuse material, and actively engages the Australian community, international partners and the tech industry to enhance online child protection.

The Attorney-General's Department (the department) leads the Commonwealth's policy and criminal justice response to child sexual abuse offences committed online, via postal services or by Australians overseas. The department works closely with the Australian Federal Police (AFP), and the AFP-led Australian Centre to Counter Child Exploitation, who will be making a separate submission.

Relevant to the reporting requirements in the draft industry standards for Relevant Electronic Services and Designated Internet Services, the department is responsible for Commonwealth law enforcement powers to combat online child sexual exploitation and abuse, including under the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004*.

The department is also responsible for Australia's privacy framework, including administration of the *Privacy Act 1988* (Privacy Act) which is the primary Australian law that protects the privacy of individuals, and sets out how government and industry can collect, use, and disclose individuals' personal information. Given the interactions of the draft industry standards with the Privacy Act, the department notes the importance of ongoing engagement with the eSafety Commissioner.

This submission considers how the draft industry standards for Relevant Electronic Services and Designated Internet Services will address the prevalence of child sexual abuse material on internet and electronic service platforms. It also considers the draft industry standards in relation to existing and proposed Commonwealth legislation governing privacy protections, data management, reporting requirements for telecommunications providers, and a recent legislative amendment establishing new criminal offences for the use of the internet to view and share violent extremist material.

While the submission focuses on how the draft industry standards will address online child sexual abuse material, the department notes effective safety measures for this type of material may address other forms of class 1A and 1B material[1], including pro-terror material.

Enhancing digital industry efforts to protect children online

Child sexual exploitation and abuse continues to be prevalent, commodified, organised and extreme, both globally and in Australia. In 2022, the US-based National Center for Missing and Exploited Children (NCMEC) received over 32 million reports of child sexual abuse material from countries across the world –

[1] Class 1A material consists of child sexual exploitation and abuse material, pro-terror material, and extreme crime and violence material. Class 1B material consists of crime and violence material, and drug-related material.

an 87 per cent increase on 2019. For the same period, NCMEC received 182,050 reports of child sexual abuse material attributed to Australia, a nearly three-fold rise from 65,535 reports in 2021.

While these reports are not indicative of the level of child sexual abuse in Australia, the scale of the reports indicates that a high volume of child sexual abuse material is being shared on online platforms, including on services that are covered by the existing registered industry codes and the draft industry standards.

In early 2023, the eSafety Commissioner registered industry codes dealing with class 1A and class 1B material for six industry sectors: social media services; internet carriage services (also known as internet service providers); equipment providers; app distribution services; hosting services; and internet search engine services. The department notes the registration of the industry codes for these services and welcomes regular review and reporting on the effectiveness of these codes.

As outlined in the eSafety Commissioner's November 2023 discussion paper on the draft industry standards, the draft Relevant Electronic Services industry code and Designated Internet Services industry code were found not to contain appropriate community safeguards for end-users in Australia. The draft industry standards for Relevant Electronic Services and Designated Internet Services are intended to enhance the approach to managing class 1A and 1B material on these services. This includes addressing the exemption of specific categories of online services from requirements to detect and remove known child sexual abuse material and pro-terror material, and to disrupt and deter new or unknown material of this nature.

The industry standards will clarify and set expectations for the critical role of digital industry in detecting and reporting on harmful online material. Given the significant levels of harm this material causes to victims and survivors[2] and the broader society, all relevant online services should utilise detection technology to identify and remove child sexual exploitation and abuse material. Without the broad use of these technologies, known material will continue to circulate, impacting victim and survivors for years after the abuse took place and normalising child sexual abuse material. It is unreasonable for online services to rely on user reporting when technology is available to perform this function at scale.

Detecting and removing child sexual exploitation and abuse material online serves to protect children who are currently or are at future risk of harm. Viewing child sexual abuse material online has been linked to an increased risk of individuals seeking direct contact with children[3], including where there has been no history of previous contact offending. With new and cheaper forms of technology such as generative artificial intelligence enabling more individuals to create, use, and distribute child sexual abuse material online, it is critical that effective safety measures are built in by design, or developed where not currently in use, to reduce the availability of harmful content to current or potential future offenders.

End-to-end encryption plays an important role in protecting individuals' privacy and data. However, the right to privacy is not absolute and it is recognised that the use of this technology in some settings can have public safety risks. The detection of online child sexual exploitation and abuse provides valuable investigative leads

[2] We recognise that not all people with lived experience of child sexual abuse will identify with these terms.
[3] Nearly half (42 per cent) of respondents in a sample of over 1,546 anonymous individuals who searched for child sexual abuse material on the dark web sough direct contact with children after viewing the material through online platforms, see Risk Factors for Child Sexual Abuse Material Users Contacting Children Online | Journal of Online Trust and Safety (tsjournal.org)

for law enforcement, helping to identify victims and offenders. The implementation of end-to-end encryption greatly reduces the availability of investigative leads and evidence.

The department supports the proposed measures requiring online industry to implement systems, processes and technologies to detect and remove child sexual exploitation and abuse material where feasible, noting that services will not be required to design systemic vulnerabilities or weaknesses into end-to-end encrypted services or monitor private communications. Where this is not currently feasible, the draft standards would support the development of alternative means to detect and remove such material. This approach recognises that the concepts of privacy and safety are not mutually exclusive and must be balanced, taking into account principles of lawfulness, legitimacy, reasonableness, necessity and proportionality.

Risk Profiles

The department supports the use of pre-assessed and defined categories of services to determine whether compliance measures are mandatory or optional for services, and ensure services are subject to appropriate and targeted compliance measures. The use of these categories for services, particularly services subject to rapid technological change (for example, generative AI services), should be monitored against market changes in the online industry to ensure categories and compliance measures remain fit-for-purpose.

The department proposes regular risk reviews should be required of services to account for the evolving nature of social media services (and other services as applicable) and ensure that services are meeting minimum code requirements for the risk of child sexual exploitation and abuse material that their service carries. This should be separate to requirements in Division 1, Part 3, Section 8 (5) of the Relevant Electronic Services and Designated Internet Services, which relate to risk reviews in response to implementation of any significant feature. Social media services growth and expansion can occur as a consequence of a number of factors, not just significant feature upgrades. A sudden surge in child users due to a change in service by a competitor for example, would warrant a risk review. It is critical that services are actively considering the impact of their internal developments and the external environment in which they operate. Services should be encouraged to engage independent reviews of their services for greater transparency and accountability.

Future phases of the industry codes and standards should discourage a ‘set and forget’ approach to risk profiles and regular risk reviews, possibly annual, should take place for all online services. A regular scheduled risk review would present an opportunity for a service to review their risk rating, where other circumstances had not already triggered a review within that period.

Compliance measures

Closed communication and encrypted services

The department strongly supports privacy and security enhancing technology, including end-to-end encryption, to protect personal data, protect against cybersecurity threats and enhance protections for journalists, human rights defenders and other vulnerable cohorts.

While keeping personal data safe online, the department is concerned that the increased uptake of anonymising and encryption technologies, including end-to-end encryption, will further impact law enforcement and national security agencies’ ability to lawfully access data and investigate serious and organised crime, including online child sexual exploitation and abuse.

Encrypted communications already impact law enforcement efforts. ASIO has reported that as of 2021, end-to-end encryption damaged intelligence coverage in at least 97 per cent of its investigations, compared to 90 per cent of priority counter terrorism cases prior to 2021[4]. As more digital technology companies implement privacy enhancing technologies, the detrimental impact of encryption on law enforcement will likely increase. Anonymising and encryption technologies are used by offenders to share harmful material without fear of detection, and facilitate private communications between offenders and children online. Current law enforcement tools may become increasingly ineffective as end-to-end encryption increases, limiting law enforcement efforts to identify offenders and victims.

The eSafety Commissioner's reasons for not registering the Relevant Electronic Services industry code identified a lack of appropriate safeguards to address these issues, including a lack of requirements for closed communication Relevant Electronic Services providers to:

- deploy systems, processes or technologies to detect and remove known child sexual exploitation and abuse material and pro-terror material, where providers have those capabilities;
- implement systems, processes and technologies to deter and disrupt users from engaging with child sexual exploitation and abuse material or pro-terror material; or
- have trust and safety personnel.

To address the lack of safeguards for closed communications Relevant Electronic Services providers, which includes providers of encrypted services, the eSafety Commissioner proposes revised requirements for closed communications Relevant Electronic Services to implement systems, processes and technologies to detect and remove this harmful material where technically feasible to do so. The department views the inclusion of the technical feasibility exception for detecting and identifying known child sexual exploitation and abuse material and pro-terror material as appropriate, and a practical alternative to fully exempting closed communication Relevant Electronic Services, including encrypted services, from requirements to detect and remove known child sexual exploitation and abuse material and pro-terror material.

The department supports the position that companies are not expected to design systemic vulnerabilities or weaknesses into end-to-end encrypted services. We note that this provides consistency with the limitations imposed by section 317ZG of the *Telecommunications Act 1997* (Telco Act), which limits what can be required of industry via a technical assistance request, technical assistance notice or technical capability notice under Part 15 of the Telco Act.

The department considers it would be appropriate for the draft industry standards to clarify that companies are not expected to build systemic weaknesses. This is because it may be technically feasible, as currently included in the draft industry standards, to build a systemic vulnerability or weakness into an end-to-end encrypted service; however, it is outside the scope of relevant legislation for that to be an expectation under the draft industry standards.

The draft industry standards require closed communications Relevant Electronic Services to implement systems, processes, and technologies to deter and disrupt users from engaging with known and first-generation child sexual exploitation and abuse material or pro-terror material. The department supports

[4] Five Eyes and EU Renew Emphasis on Encryption – Michael Kans

these requirements, including the proposed use of hashing technologies, machine learning and artificial intelligence systems that scan for known child sexual exploitation and abuse material or known pro-terror material; and systems, processes, and technologies designed to detect key words, behavioural signals and patterns associated with child sexual abuse material. These approaches can supplement existing tools to detect known and unknown class 1A material, or where detection is not currently technically feasible, provide alternative mechanisms. As the use of end-to-end encrypted communications becomes commonplace, the importance of these alternative mechanisms for detecting illegal content, child sexual abuse offenders and their victims will increase.

The department supports the inclusion of closed communication Relevant Electronic Services providers under the requirements to sufficiently resource trust and safety functions, including personnel, to comply with the requirements of the Relevant Electronic Services draft industry standard. The evolving risks to public safety associated with encrypted technologies places greater responsibilities on companies to engage officers with relevant skills, experience, and expertise. Well-resourced trust and safety functions will assist companies to deliver services that support the privacy and safety of all Australians, including new and innovative products. The department recognises the establishment and maintenance of effective trust and safety functions may require a resourcing investment on online industry, while acknowledging industry is best placed to protect the safety of its users, including children.

Generative artificial intelligence (AI)

The department is concerned by the use of AI to generate child sexual exploitation and abuse material and its impacts on law enforcement, victims and survivors, and the broader community.

Under Australia's *Criminal Code Act 1995 (Cth)*, AI-generated child abuse material is included in the definition of child abuse material. The material need not depict actual children, and case law has determined that the definition of child abuse material covers drawings of fictional or imaginary characters.

The capability of AI services to create child sexual exploitation and abuse material poses unique risks.

- Generative AI programs may inadvertently expose non-offenders to material, including exposing them to age-inappropriate material such as online pornography for child users.
- The ease of use of generative AI programs lowers the barrier to entry for offenders to engage with child sexual abuse material.
- The consumption of child sexual abuse material in any form creates further demands for material and can lead some offenders to pursue material containing real children and more active forms of abuse.
- The volume of AI-generated child sexual abuse material may rapidly escalate as AI programs become faster, cheaper, easier to use and produce more realistic life-like images and videos.
- AI-generated child sexual abuse material can be difficult to distinguish from real-life content – impacting law enforcement efforts to distinguish between synthetic images or real victims. This means valuable time can be wasted looking for victims that do not exist.
- The production of AI-generated images may cause a significant increase in child sexual abuse material being circulated, impacting the ability to categorise and hash (digital fingerprint) images for future identification as known abuse images.

- As the capability of AI-powered large language models to imitate human language improves, offenders will seek to use the automated and targeted nature of these tools to groom children.

While AI-generated material is currently a small proportion of all child sexual exploitation and abuse material, based on a sample of offender files reviewed by Thorn in 2023[5], the volume has increased consistently since August 2022, and has the potential to increase further as technology advances.

The draft Designated Internet Services industry standard creates two new categories of AI-related services: a category for services that can be used to generate synthetic high impact material (high impact generative AI Designated Internet Services), and a category for machine learning model platform services. The department supports the creation of specific categories and additional compliance measures for AI-related services, including the further minimum requirements for high impact generative AI Designated Internet Services in Division 2, Part 4, Section 23 (3). The department notes these requirements, which cover preventative systems, processes and technologies, review, testing and adjustment, and warnings and links to support services, will likely require significant engagement with online industry to ensure effective implementation.

In June 2023, the Department of Industry, Science and Resources (DISR) publicised a 'Supporting responsible AI' discussion paper[6], which intended to inform a public consultation on safe and responsible AI practices held over June to August 2023. The department notes the subsequent release of the Australian Government's interim response to the public consultation, which highlighted both the positive opportunities of AI systems and applications, and a range of risks associated with generative AI. As stated in the interim response, interactions between the existing industry codes and draft online industry standards will be considered in the development of options for introducing new regulatory guardrails with a focus on testing, transparency and accountability. The department supports eSafety's ongoing engagement with DISR developing approaches to address generative AI risks, including through regulation.

End-user managed hosting services

The department notes the draft codes for Relevant Electronic Services and Designated Internet Services did not appear to capture end-user managed hosting services, including hosting services providing multi-use storage services and those primarily dedicated to image hosting. First party hosting services enable end-users to store files, photos or other media online in personal user accounts, which may be shared with other users. These high-storage sites can be used to share one image or video at a time, or one or more folders containing hundreds of images or videos under a single URL. These services are exploited by offenders to store and share illegal images and videos.

The eSafety Commissioner's Summary of Reasons for not registering these services in the draft Relevant Electronic Services codes identified a lack of appropriate safeguards for end-user managed hosting services to address these issues, including:

- no requirements to deploy systems, processes and/or technologies to detect and remove known child sexual abuse material and known pro-terror material; and

[5] Founded in the United States in 2012, Thorn employs a tech-led and partnerships-based approach to countering online child sexual exploitation abuse and child sexual trafficking – referenced in the WeProtect Global Threat Assessment 2023.

[6] Consultation hub | Supporting responsible AI: discussion paper - Consult hub (industry.gov.au)

- no requirements to act and invest in disruption and deterrence of class 1A material (including new/first generation child sexual abuse material).

The department strongly supports the inclusion of these services as a defined category in the draft Relevant Electronic Services industry standards subject to specific compliance measures, including: detection and removal requirements for known child sexual abuse material and known pro-terror material, disruption and deterrence requirements for class 1A material, and further minimum requirements to minimise accessibility of class 1A material by end-users.

In addition to reports of end-user hosted child sexual exploitation and abuse material provided to NCMEC by larger technology companies, there is significant evidence of smaller end-user managed hosting services being used by offenders to store and share illegal images, videos and other content.

Under the Canadian Centre for Child Protection's Project Arachnid, a specialised search tool scans websites to identify child sexual exploitation and abuse material. Of over 5.4 million images detected and verified over a three-year period (2018-2020), many were hosted on image and file hosting sites owned by smaller hosting services that may be covered by the draft industry standard.

The 2022 Internet Watch Foundation's Annual Report analysed over 375,000 reports of webpages confirmed as containing child sexual abuse imagery, linking to imagery, or advertising it. Their analysis identified the majority (77 per cent) of offending websites as image hosts, which provide storage for images which either appear on dedicated websites or are shared within forums.

The department supports, where feasible, the effective application of the draft industry standards to both larger mainstream technology companies and smaller service providers engaging with Australian end-users.

The department notes the private-by-default nature of these services may raise user expectations that no systems, processes or technologies will review user data. While strongly supporting the need to protect the privacy of user information, the department supports the use of privacy preserving tools to detect child sexual exploitation and abuse or pro-terror material on end-user managed hosting services.

Dating services

The department supports the inclusion of dating services as a defined category in the Relevant Electronic Services draft industry standard subject to specific compliance measures. The department notes the consolidated Industry Codes of Practice for the online industry did not appear to cover dating applications, either as a Relevant Electronic Services or Designated Internet Services.

Research by the Australian Institute of Criminology has reviewed the use of online dating platforms as a means for perpetrators to seek access to child sexual exploitation and abuse material or children, including that 'the ability of perpetrators to seek access to child sexual exploitation and abuse material or children through online dating platforms is in part facilitated by the characteristics of these platforms. In particular, most mobile dating apps and dating websites do not require individuals who set up new accounts to provide evidence that they are who they say they are—meaning that users can create any kind of avatar they want.'[7]

[7] The sexual exploitation of Australian children on dating apps and websites | Australian Institute of Criminology

The research further noted 'one in eight respondents reported that they received at least one request from someone they had met on a dating app/website to provide child sexual exploitation and abuse material or access to their children (or children they had contact with) for sexually exploitative purposes.'

Gaming services

The department notes the draft Relevant Electronic Services industry standard includes categories for:

- a gaming service with communications functionality; and
- a gaming service with limited communications functionality.

The department supports two categories for gaming services, noting gaming services with communications functionality are subject to additional compliance measures. Gaming services that include user-to-user communications (e.g. chat or file sharing) functions provide a means for offenders to target and groom children online[8] or to share child sexual exploitation and abuse material. The department suggests the compliance measures in Division 2, Part 4, Section 19 (4) (c, d, e, f and g) that provide additional protections relating to communications and privacy settings for Australian end-users of open communication and Tier 1 services, including young Australian children, be adapted to apply to gaming services with communications functionality. The relevant measures require the use of tools and settings to block messages from other end-users, prevent the display or communication of the end-user's online status, prevent end-users who are over 18 from using the service to contact a young Australian child without the consent of a child's parent or guardian, set the account of a young Australian child as private by default, and hide the location of a young Australian child from other end-users without the consent of a child's parent or guardian.

The department notes online services that provide an immersive, three-dimensional experience, also known under the umbrella terms of 'extended reality' or 'immersive technologies', provide opportunities for offenders to access, exploit and abuse children[9]. These online services may be covered by this category, or may require a separate category. The department notes the eSafety Commissioner released the report 'The Metaverse: a snapshot of experiences in virtual reality' in December 2023, which references a range of online harms that may occur in these environments.

Reporting

The reporting requirements in Division 2, Part 4, Section 15 of the Relevant Electronic Services and Designated Internet Services draft industry standards requires service providers to notify appropriate entities about child sexual exploitation and abuse material, or pro-terror material, on their services. The department notes the specific reporting requirements depend on two elements:

- Whether the material is evidence of an immediate and serious threat, which will require reporting the matter to an enforcement authority.
- Whether the material is unknown, which will require reporting the matter to an appropriate authority such as the National Center for Missing and Exploited Children.

---

[8] A Crisp study identified 45 minutes as the average time for a child to be groomed in a social gaming environment – with extreme examples as low as 19 seconds – referenced in the WeProtect Global Threat Assessment 2023.
[9] Emma Barrett, 'Extended Reality Technologies and Child Sexual Exploitation and Abuse - WeProtect Global Alliance', WeProtect Global Alliance

The department supports a reporting requirement for known material that does not require evidence of an immediate and serious threat, as this will constitute the majority of all identified material. For matters indicating an immediate and serious threat, the department suggests an indicative timeframe (e.g. within 24 hours or as soon as reasonably practicable) may be more appropriate to signal the urgency of reporting, while not prescribing a specific timeframe. An explanatory statement may be useful to accompany the reporting requirements, similar to the guidance that appears with the relevant industry codes on the intention for reporting to supplement existing laws.

Privacy

Overview

The *Privacy Act 1988* (Privacy Act) is the primary Australian Commonwealth law that protects the privacy of individuals, and restricts how government and industry can collect, use and disclose individuals' personal information. Strong privacy protections build trust and security which is necessary for economic growth, innovation and the participation of individuals in the digital economy. The department has completed a review of the Privacy Act to ensure it is fit for purpose in the digital era, and the Privacy Act Review Report (the Report) was made public on 16 February 2023. The Government's response to the Report was released on 28 September 2023, and commits the Government to progressing work to enhance the privacy protections provided to individuals and ensure Australian businesses have clarity about what information is covered by the Privacy Act and how to best protect this information.

There are a number of intersections between online safety and privacy. As identified in the eSafety Commissioner's submission to the Report[10], strong privacy protections are crucial to protect individuals, in particular children, from online harms such as data breaches, identity theft, grooming for sexual exploitation, and inappropriate targeted advertising or recommended content. The 2023 Office of the Australian Information Commissioner (OAIC) Australian Community Attitudes to Privacy Survey makes clear the high priority Australians place on the security of their personal information, with 70 per cent of those surveyed noting privacy is an extremely or very important factor when choosing a product or service. Australians want organisations to only collect the data they need, take proactive steps to protect personal information they hold, and delete it when it is no longer needed.

The draft industry standards will have interactions with proposals that the Government has agreed or agreed in-principle in the Government Response to the Report, including:

- enhancing the Privacy Act's existing security obligations in Australian Privacy Principle (APP) 11 by:
    - specifying that the requirement for entities to take reasonable steps to protect personal information they hold from misuse, interference and loss, as well as unauthorised access, modification or disclosure, includes both *technical and organisational measures* (proposal 21.1)
    - requiring entities to comply with a set of *baseline privacy outcomes* when meeting APP 11 (proposal 21.2); and
    - enhancing OAIC guidance about what reasonable steps an entity should take to keep personal information secure (proposal 21.3)

[10] eSafety Commissioner, Submission to the Privacy Act Review Report

- requiring entities to have regard to the *best interests of the child* as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances (proposal 16.4)
- developing a *Children's Online Privacy code* (proposal 16.5), and that the code apply to online services likely to be accessed by children. To the extent possible, the scope of the code should align with international approaches, including the United Kingdom's (UK) Age Appropriate Design Code; and
- codifying the principle that *valid consent must be given with capacity* (proposal 16.2). Entities should continue to rely on existing OAIC guidance on children and young people and capacity which provides sufficient flexibility by allowing entities to decide if an individual under the age of 18 has the capacity to consent on a case-by-case basis. If that is not practical, as a general rule, an entity may assume an individual over the age of 15 has capacity, unless there is something to suggest otherwise.

The department will continue to engage with eSafety on potential interactions between these proposals and the industry standards.

Security and privacy considerations

As noted, while services will not be required to design systemic vulnerabilities or weaknesses into end-to-end encrypted services or monitor private communications, the draft industry standards do not mandate a particular approach or technology. The department stresses the importance that any systems, processes and technologies used must appropriately balance privacy and security considerations. It will be crucial for eSafety to carefully consider how this can be achieved, and provide adequate guidance to regulated services to ensure they are able to meet the requirements in a privacy preserving manner. Guidance should be developed in consultation with the department and the OAIC, and reflect evolving technology.

Children's privacy

As noted in the eSafety Commissioner's submission to the Report[11], the proposed Children's Online Privacy Code will have interactions with the draft industry standards and in many cases apply to the same group of stakeholders. To ensure regulatory consistency, the department considers requirements in the Relevant Electronic Services draft industry standards should be considered against the backdrop of the Government Response to the Report.

The department notes Division 2, Part 4, Section 19 (4) of the Relevant Electronic Service draft industry standards requires open communication relevant electronic services or Tier 1 relevant electronic services to ensure the account of a young Australian child (being an Australian child under the age of 16) is private by default, and the location of a young Australian child who is an end-user of the service is not available to end-users of the service unless with the consent of the child's parent or guardian. The department considers that extending the scope of these measures to apply to all children (including those between 16 and 18 years) would provide greater alignment with the proposed approach to the Children's Online Privacy code. As noted, the Government Response to the Report states that the proposed Children's Online Privacy code should align with the UK Age Appropriate Design Code. This requires services to, for all children:

- ensure settings must be 'high privacy' by default (unless services can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child), and

[11] eSafety Commissioner, Submission to the Privacy Act Review Report

- switch geolocation options off by default (unless services can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child), and provide an obvious sign for children when location tracking is active.

The department notes these requirements appear to align with the Relevant Electronic Service draft industry standards, including the safety features and settings compliance measures in Division 2, Part 4, Section 19 (4) for Australian end-users of open communication and Tier 1 services.

Where parental or guardian consent is required, consideration should be given to whether services can undertake a case-by-case assessment of a child's capacity to consent as opposed to mandating that parental or guardian consent is required in certain circumstances for young Australian children. This approach would better reflect the recommendations of the UN Committee on the Rights of the Child's General Comment No. 25 on Children's Rights in Relation to the Digital Environment[12], which provides that states parties 'should respect the evolving capacities of the child' in the digital environment.

Violent Extremist Material

On 6 December 2023, the *Counter-Terrorism Legislation Amendment (Prohibited Hate Symbols and Other Measures) Act 2023* (the Act) passed both houses of Parliament. Relevantly to this consultation, the department draws to the eSafety Commissioner's attention the fact that the Act establishes new offences in Subdivision HA of the Criminal Code for the use of the internet to view and share violent extremist material. Examples of the types of violent extremist material intended to be captured by the offence include instructional terrorist material and terrorist organisations' recruitment materials.

Violent extremist material is harmful because it facilitates radicalisation. It may encourage and assist in planning violent acts. These acts can threaten public safety, and Australia's core values and principles, including human rights, the rule of law, democracy, equal opportunity and freedom.

To this end, the department supports consideration of whether the industry standards could be expanded so as to protect the Australian community from the harm that is inherent in violent extremist material (as defined in section 474.45A of the Criminal Code). For example, the industry standards could require providers of services to notify authorities and remove content if violent extremist material is identified or detected on their services. Such a requirement could potentially be modelled on, or incorporated within, the elements of industry standards that relate to the safeguards for pro-terror material.

The department welcomes continued engagement on options to incorporate violent extremist material into the industry standards.

Conclusion

The department welcomes the opportunity to provide this submission and remains committed to working with Industry to enhance efforts to reduce access and exposure to class 1A and 1B material. The department further welcomes the opportunity to review and provide further input to future phases of the industry codes and industry standards.

[12] United Nations Committee on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment