American Chamber of Commerce in Australia
Level 3, 15 Castlereagh Street | Sydney NSW 2000

(02) 8031 9000
www.amcham.com.au

AmCham

CONFIDENTIAL

Friday, 8 August 2025

Office of the Australian Information Commissioner
Via email: copc@oaic.gov.au

Dear Sir/Madam,

Children's Online Privacy Code

The American Chamber of Commerce in Australia (AmCham) writes in response to the Office of the Australian Information Commissioner's (OAIC) Issues Paper on the *Children's Online Privacy Code* (Code).

We support the objective of the Code to protect the personal information of children in relation to online services likely accessed by them and appreciate the opportunity to share our insights with the OAIC.

We are aware that some of our members have or will be making submissions to the Issues Paper, many of whom have invested in substantial resources and innovations to protect the privacy of children online. Our intention is to limit the submission to key areas of concern and themes related to our joint position.

General Comments

We recommend that regulations, in general, should be harmonised and interoperable, which helps provide certainty to both users and service providers, enabling better and more consistent experiences by users and achievable compliance by Australian Privacy Principles (APP) entities. The Code should set out guidelines where there is conflict, if any, with the APP requirements as well as with other overlapping regulatory frameworks including, in particular, phase 2 codes under the Online Safety Act and the implementation of the social media age restrictions.

We also support aligning the Code with the *United Kingdom's Age-Appropriate Design Code* (AADC), which provides a proportionate, flexible, risk-based approach to the privacy of children and teens that has proven to be effective and enforceable.[1]

Specific Comments

1. Scope of Services Covered by the Code

Adopt an expressly proportionate and risk-based approach to applying the Code to APP entities. We encourage the OAIC to refer to the AADC's assignment of proportionate regulatory obligations to services based on risk as informed by a Data Protection Impact Assessment (DPIA). This approach would consider risk to children based on factors such as:

- The target audience for the service, and whether it is directed at adults or children;
- Whether the service is offered for free, or requires a paid account;
- The methods that exist to 'age gate' certain content, such as the need for credit cards to sign up, or the ability to set up child profiles;
- The extent and extent of user interaction; and
- The way content is controlled, for example if it is a user generated content service, or if it offers professionally produced and curated content.

This approach recognises that risk profiles vary greatly, depending on the nature of online services, which differ substantially in respect to the functionality, features, the reach of their content, and risk profiles. We encourage the OAIC to take a similar approach, with practices considered low, medium, and high risk clearly articulated. The guidance of the United Kingdom's Information Commissioner's Office (ICO) on 'high risk' and 'likely to result in high risk'[2] practices could be adopted, as was considered in the 2022 *Privacy Act Review Report* by the Attorney-General's Department, Australian Government.

This risk-based approach enables APP entities to adjust their obligations according to what is necessary and proportionate. For instance, a streaming service may be assessed as 'low risk' if it is designed for adults or mainly accessed by children under adult supervision, and provides professionally produced content with minimal opportunity for interaction among subscribers, as opposed to user-generated content platforms. Regulatory requirements applicable to high-risk services, such as implementing default 'high privacy' settings for children or developing privacy policies and consent notices suited to different age groups, would therefore not apply to low-risk services such as streaming services.

---

[1] In March 2025, the ICO announced investigations into the child's data collection and processing practices of Tik Tok, Reddit, Imgur. See here.

[2] ICO, Age-Appropriate Design Code - When do we need to do a DPIA? 'What does high risk mean?', here.

Using this risk-based approach, we further encourage the OAIC to exercise its discretion to state which classes of APP entities are inside and outside of the Code to provide additional clarity to industry by specifying that certain clearly low-risk services, such as enterprise services, cloud storage services, and online professional services, are outside the scope of the code.

Apply Code requirements flexibly, as appropriate, relevant, and proportionate. The scope of services to be covered by the Code should apply a risk-based approach that differentiates between service type and risk. The AADC allows services to choose how to meet standards based on their specific context. They can apply protections either to features likely accessed by children or to all users. We recommend the OAIC adopt a similar policy. It is important that services are only required to apply Code compliance requirements to the elements of the service 'likely to be accessed by children'.

In addition, we recommend the OAIC establish a Code Exemption for data collected exclusively for service provision and internal operations, with clear definitions of 'internal operations'. Data collected mainly for internal purposes should be classified as low risk and subject to proportionate regulation, given the minimal risk to individuals. As such, enterprise services and services offering professional development networking should also be excluded from the scope of the Code.

2. When and How the Code Should Apply to APP Entities

Guidance around the 'likely to be accessed by children' standard. We endorse the adoption of the AADC's 'likely to be accessed by children' standard and recommend that the OAIC issue guidance interpreting this definition, consistent with the AADC's existing guidance[3]. The guidance should define what is 'of particular appeal' to children, helping services assess whether their activities fall under the Code. Services that do not initially meet the 'likely to be accessed by children' threshold should be explicitly excluded, such as those primarily designed for enterprise or business-to-business (B2B) purposes. This distinction ensures that irrelevant services are not compelled to prove their non-compliance with this threshold, thus minimizing unnecessary regulatory uncertainty and burden.

3. Age Range-Specific Guidance

The protection approach must consider different development stages and varying maturity levels. Any legislation requiring protections for children users should reflect the differences in maturity, capacity, and risks of harm between children, and enable services to provide age-appropriate experiences. Doing so would also meet children's need for access to digital tools that help them learn and develop social skills, connect with friends and family, and compete in the global economy.

[3] ICO, Age Appropriate Design Code - Services Covered By This Code, here.

We support aligning the Code with the AADC's threshold. We encourage the OAIC to consider broader age bands for children's privacy protections that align with existing industry standards, with stricter protections and parental oversight of young children under thirteen and more autonomy and control for teens 13-17 (e.g., film and video game classification age bands). Differentiating requirements based on very granular ranges would impact ease of compliance and require the collection of more personal data.

The Code should also provide for parental involvement but be reflective of evolving capacities (e.g., age and maturity), recognising that children and teens have the right to privacy from their parents as they mature. This aligns with United Nations Convention on the Rights of the Child (UNCRC) principles regarding the evolving capacities of the child (Article 5) and their rights to have their views given due weight in accordance with their age and maturity (Article 12)[4].

We recommend that the obligations of the Code should only apply when an entity has actual knowledge that a user is a child, for example when the user is logged in to a child account. Requirements to infer a user's age can conversely lead to privacy-invasive practices such as collecting more personal data on all users for the purposes of profiling that user's likely age.

It is essential that age-specific requirements remain flexible, enabling entities to design their services to suit the needs of the user groups most likely to access them. While the AADC provides developmental age ranges, the ICO advises to apply a risk-based approach to recognising the age of individual users and to ensure effective application of standards to child users. The ICO states that it is not necessary to design services for developmental stages unlikely to use those services, and exact age ranges do not have to be used if different groupings are more suitable for a specific service.[5] Moreover, online services allow parents to adjust parental controls based on content and functionality classifications. While we support the provision of age-based guidance, it is important to recognise that different services will apply to different age-based categories, and the guidance should therefore be voluntary and flexible. For example, services that comply with the National Classification Scheme must rate content as G, PG, M, MA15+ and R18+. Adopting a different set of age ranges for the Code would place over-burdensome and unnecessary obligations on these services.

In general, we consider that it may be appropriate for services with logged-in users to distinguish between two broader categories of age ranges: young children under 13 who should have strong parental controls in place; and older children between 13-17 who may be able to exercise greater autonomy over their privacy settings.

---

[4] United Nations. (1989). Convention on the Rights of the Child. Retrieved from OHCHR website: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

[5] ICO, Age Appropriate Design Code - Age Appropriate Application, here.

4. Open and Transparent Management of Personal Information

Where transparency and notification requirements (e.g., under APP 1 and APP 5) are necessary and proportionate based on a service's level of risk, these should be offered at different points in time, as appropriate. For example, the Philippines National Privacy Commission (NPC) recommends the use of just-in-time notices and layered notices. Transparency notices should be coupled with age-appropriate controls and features that provide users with a range of privacy-preserving settings, depending on the child's needs and circumstances. For example, for children under the age of parental consent, these settings and tools should provide parents with a meaningful ability to understand and control their child's experience on the service.

5. Anonymity and Pseudonymity

We support specific obligations on high-risk online services to protect the personal data of known child users, including data minimisation requirements, prohibition on targeting ads, prohibition on collecting precise geolocation data, and comprehensive parental oversight, and control over personal data of children under thirteen. We further note that protections to minimise harm to children online should also consider other fundamental rights including freedom of expression, security, digital safety, and the benefits of online participation.

We generally agree that the Code should apply the principles of data minimisation, high privacy settings, and geolocation data by default, similar to the requirement by the Singapore's Personal Data Protection Commission (PDPC) and the Philippines NPC. The Code should allow companies to provide services in 'signed out and unregistered mode,' and not require any age-gating in those situations.

The Code should allow online services to offer a range of privacy-preserving settings and tools that help parents address the unique needs and preferences of their family as well as give families the flexibility to manage their relationships with technology and make meaningful choices for accessing and controlling their data.

As practiced in most countries in the Asia Pacific, the Code should not prescribe mandatory age assurance methods for a number of reasons.

In accordance with the AADC, the Code should acknowledge that services ought to retain the flexibility to implement age assurance methods that are appropriate for the unique requirements of each service. For instance, payment methods such as credit and debit cards have been effective in enabling streaming services to verify that subscribers are at least 18 years of age. This approach to age assurance is recognised and endorsed by Australia's Restricted Access System. [6]

[6] Restricted Access System - Explanatory Statement, 2021, here.

Even in some cases where there is child-specific guidance, age assurance need not always be required. For example, the Philippines NPC guidance provides that controllers may implement age assurance mechanisms to determine a user's age range to facilitate age-appropriate practices. Similarly, while Singapore's PDPC supports the use of age assurance methods, it does not mandate these mechanisms in the implementation of relevant safeguards. The Code should allow organisations to have flexibility over whether and when to implement age assurance. Singapore's PDPC further recognises that age assurance need not be at the account registration stage and could be at another appropriate juncture (e.g., when there is a higher risk to users). Because age assurance technologies are novel, imperfect, and evolving, requirements should also provide reasonable protection from liability for good-faith efforts to develop and implement improved solutions in this space.

Further, age assurance requirements may not be suitable or required for services classified as 'low risk'. As outlined in the AADC, it is incumbent upon services to assess *"whether the level of certainty they have about the age of their individual users is appropriate to the risks that arise from data processing."* [7] Therefore, we support accountability requirements such as undertaking risk or impact assessments (e.g., DPIAs) for processing children's personal data where there are greater risks of harm.

This is aligned with the AADC, the European Union's General Data Protection Regulation, guidance from Singapore's PDPC, and the Philippines NPC. The DPIA should also be principles-based, provide companies the flexibility to determine their DPIA templates and how to demonstrate accountability in their privacy practices.

Finally, mandating age assurance methods may conflict with ongoing reforms like the Age Assurance Trail or with existing frameworks such as the Restricted Access System.

Although age assurance can play an important role in helping to identify child users, there are privacy and free expression concerns with over-reliance on age assurance technologies. Any method to determine the age of users across services comes with trade-offs, such as intruding on privacy interests, requiring more data collection and use, or restricting adult users' access to important information and services.

It is important that age assurance programs protect privacy, including rules around data minimisation and building systems under the principles of privacy by design so that they operate with a minimum amount of data sharing. The Code should apply a risk-based approach to age assurance, preserving users' access to information and services and respecting their privacy. In light of eSafety's ongoing work on age assurance, it is also critical for Australian regulators to provide coordinated guidance for industry on their expectations in this area.

---

[7] ICO, Age Appropriate Design Code - Age Appropriate Application, here.

Where required, age assurance should be through a workable, interoperable standard that preserves the potential for anonymous or pseudonymous experiences. It should avoid requiring the collection or processing of additional personal information, treating all users like children, or impinging on the ability of adults to access information. Collection of data which would generally be considered sensitive (such as verification with 'hard identifiers' like government IDs) should be limited to high-risk services (e.g., alcohol, gambling, or pornography) or age correction.

6. Collection of Solicited Personal Information

In relation to APP 3 and when information is reasonably required, the Code should enable a principles-based approach of what is reasonable, similar to the guidance of Singapore's PDPC. The Code should explain the circumstances under which the OAIC considers it necessary and justifiable to collect and process sensitive personal information, biometric, and location data of children on a limited basis.

7. Notification of the Collection of Personal Information

While we recognise the importance of age-appropriate communication, the Code should not be overly prescriptive and should retain flexibility for online service providers to determine what is the most appropriate way to communicate with its users. Guidance from the Singapore's PDPC recognises that there is 'no one-size-fits-all approach' and organisations should consider the nature of their content and adopt age-appropriate language and format (e.g., infographics, video clips). It also recommends using language that is 'readily understandable by children' but does not provide prescriptive requirements. In addition, the Philippines NPC recommends that controllers take a risk-based and child-oriented approach when informing children and teens about data processing, considering their age and the risks involved in the specific processing activity.

Controllers should also consider the readability (e.g., vocabulary, tone, style), comprehension, and granularity of privacy notices while considering the best interests and evolving capacities of children. This could include using different formats (e.g., videos, infographics, audio, animations).

8. Cross-Border Disclosure of Personal Information

While children's data may be treated as a category of sensitive personal data that affords a high level of protection (e.g., applying enhanced security measures as recommended by Singapore's PDPC), there should not be specific different requirements for children's data in respect of cross-border transfers, or specific prescribed technical and organisational measures with respect to children's data only.

With regard to cross-border transfers specifically, we are not aware of any country that imposes different requirements for children's data as this would not work in practice.

9. Access to Personal Information

Base the Code on the UN Convention on the Rights of the Child (UNCRC) 'best interests of the child' principle. We recommend that the OAIC incorporate the UNCRC's 'best interests of the child' principle into the Code, consistent with the AADC. This approach establishes a robust framework for services to evaluate what best serves the child's overall well-being, development, and protection in comparison to other relevant interests. When determining the best interests of the child, privacy protection should be considered alongside other interests such as safety, physical and mental health, access to information, and freedom of participation in society. According to the UNCRC General Comment 25, the best interests of the child require an assessment tailored to the specific context. It recommends that parties *"ensure that, in all actions regarding the provision, regulation, design, management and use of the digital environment, the best interests of every child is a primary consideration."* [8]

A huge body of international jurisprudence about the online privacy of children and teens already exists. We recommend that the Code also draws on similar principles, e.g., what 'likely to be accessed by children' or 'best interests of the child' means. The Code should adopt a risk-based approach, considering the best interests of the children, addressing different risks with proportional responses, and giving space for product and business improvements.

Implementing the 'best interests of the child' principle corresponds with recommendation 16.4 from the 2022 *Privacy Act Review Report*, which advises that *"entities 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."* Recommendation 16.5 further notes that *"the substantive requirements of the Online Children's Privacy Code could address how the best interests of child users should be supported in the design of an online service."*[9]

The Code should provide guidance on what the OAIC considers to be the best interests of the child or provide a framework to help service providers assess and determine the best interests and avoid misapplication and inconsistencies in practice. The Code should enumerate examples to facilitate a clear and consistent understanding and implementation of requirements specific to this area.

Responsibilities of parents and guardians. We respectfully urge the OAIC to acknowledge the significant role and responsibility that parents hold in guiding their children's development, including their involvement in managing access to various services throughout the developmental stages.

---

[8] General comment No. 25, para. 12, UN Committee on the Rights of the Child (2021).

[9] Attorney General's Department, 2022, 'Privacy Act Review Report', p. 124, here.

Conclusion

Thank you for your consideration and for this opportunity to submit AmCham's views. We welcome any queries you may have regarding our submission and any opportunities to engage in further consultation.

Kind regards,

[redacted]

About AmCham

AmCham was founded in 1961 by Australian and American businesses to encourage the two-way flow of trade and investment between Australia and the United States, and to assist its members in furthering business contacts with other nations. AmCham is Australia's largest and most active international chamber of commerce, representing some of America's most significant companies operating in the Indo-Pacific region, as well as start-ups and SMEs. In pursuing its purpose, the Chamber has found itself not only representing the United States' business view but also speaking increasingly for a broad range of members involved in the Australian business community.

US-Australia Alliance

The US-Australia alliance is underpinned by core common values including the rule of law, transparency, hard work, and fair play. The relationship has provided an immense benefit to Australia – including new jobs, higher wages, elevated productivity, market access, capabilities, intelligence, interoperability, research and development, trade and investment, cultural ideas, and exchanges of people. The current two-way trade and investment relationship between our countries is valued at almost $1.6 trillion. US trade and investment in Australia accounts for approximately $131 billion or 7% of Australia's GDP. Over a quarter of all foreign investment in Australia comes from the United States, making it the biggest investor in our country.