[redacted]

Thursday July 31, 2025

A. Overarching considerations for the Children's Online Privacy Code

Dear [redacted]

The Digital Industry Group Inc. (DIGI) thanks you for the opportunity to provide our views on the *OAIC Children's Online Privacy Code Issues paper* (the 'Issues Paper') released in June 2025.

By way of background, DIGI is a non-profit industry association that advocates for the interests of the digital industry in Australia. DIGI's founding members are Apple, Discord, eBay, Google, HelloFresh, Meta, Microsoft, Pinterest, Snap, Spotify, TikTok, Twitch and Yahoo. DIGI's vision is a thriving Australian digitally-enabled economy that fosters innovation, a growing selection of digital products and services, and where online safety and privacy are protected.

This covering letter highlights several overarching considerations for the Children's Online Privacy Code (COPC), while the remainder of the submission provides some insights in response to the questions contained in the Issues Paper.

Strong support for Privacy Act reform and the COPC

At the outset, DIGI wishes to underscore our strong, longstanding support for the need for reform of the Privacy Act. Strong privacy laws are foundational to Australians' trust and confidence in the digital economy and digital services. **Specifically, we have consistently supported the need for a Children's Online Privacy Code (COPC).** While children's privacy rights have always been included within the Privacy Act, DIGI believes there is an important opportunity in the wider reform process and the COPC to significantly advance privacy protections for Australian minors.

DIGI recognises that large technology companies are in the spotlight when it comes to questions of data privacy, and are rightly held to a high level of public scrutiny. However, there is a high level of technical experience with data governance in 'digital first' companies; this expertise may not exist to the same extent in other industries that are also using personal information in scope of the COPC. DIGI's relevant members protect young people's privacy online in a wide range of ways, including setting default privacy settings for minors, restricting unwanted contact, limiting advertising to minors, integrating privacy and safety features, offering family controls, and providing data rights for minors and others to access, download, and transfer their personal information. In an economy where arguably every company is digital, DIGI believes that Australians of all ages should have clear expectations of their privacy rights no matter what service they are using.

Consistency with international approaches

DIGI encourages consistency with international approaches in the COPC. DIGI notes that, in the Government's endorsement of the recommendation to introduce this code, it recommended that "to the extent possible, the scope of the code should align with international approaches, including the UK Age Appropriate Design Code"[1]; DIGI agrees that the UK's Age Appropriate Design Code (UK AADC) is a good model.

The UK AADC is a statutory code of practice prepared under the UK's General Data Protection Regulation (GDPR). The EU GDPR, introduced in 2018, was landmark legislation that has served as the new global model for privacy legislation. It has been implemented by many multinational companies present in Australia. Consistency between established international privacy regimes, such as the EU GDPR, will provide greater legal certainty to companies, particularly those that operate on a global basis, and consistency of experience for consumers who regularly interact with services offered outside of Australia.

Integrating the 'best interests of the child'

The UK AADC is rooted in Article 3 of the United Nations Convention on the Rights of the Child (UNCRC) on 'the best interests of the child'. **DIGI recommends that the UNCRC's 'best interests of the child' concept must be foundational to the COPC.** The 'best interests of the child' encompasses all children's rights under the UNCRC, including protection from violence, discrimination and exclusion, as well as rights to health, education, leisure, and play, and civic participation. Under the concept, there is no hierarchy of children's rights; all rights must be considered and advanced together.

While decisions relating to the best interests of a specific child by guardians or carers must take into account their individual circumstances, collective decisions must look at children in general. DIGI is of the view that we need more expert discussions on how to best translate the UNCRC 'best interests of the child; into the digital environment, and we recently convened an expert discussion in partnership with UNICEF Australia and the University of Western Sydney's Young & Resilient Centre on this subject. **As part of the development of the COPC, there is an important opportunity for the OAIC to develop technical and operational guidance for all industry practitioners that translates the UNCRC 'best interests of the child' into a digital environment**.

Flexibility with age assurance across the breadth of services

The COPC is intended to cover an expansive range of services, including providers of a Social Media Service (SMS), Relevant Electronic Service (RES) and Designated Internet Services (DIS), all within the meaning of the Online Safety Act 2021 (OSA). The SMS category is defined broadly to encompass interaction between 'two or more end users', this definition is by no means limited to large, mainstream social media services; it encompasses a wide range of services, such as local and small business community forums, educational technology, business forums, health support forums, games, news services and any blogs with comments enabled. The RES category includes services as diverse as email services, MMS and SMS services, dating services, gaming services with communications functionality, and messaging services with varying reach and risk profiles. DIS services are even more diverse, and include operating systems, cloud storage, large language models, and the full gamut of apps and

[1]Australian Government, *Government Response to the Privacy Act Review Report*, Attorney-General's Department (Canberra, 28 September 2023), https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF.

websites used by Australians – ranging from simple apps that help users find the date or time of day, sites that provide community services, and adult websites.

In developing a code for this diverse range of services, the OAIC is confronted with a critical threshold question: in order for this broad range of service providers to know when minors are accessing their services, this usually requires age assurance and/or further information collection. As the OAIC would be aware, the widespread deployment of age verification across all websites, messaging and interactive services would see a systemic increase in the collection of personal information across these services, increasing the risk and likelihood of privacy harms such as data breaches. Absent any GDPR-style consumer rights to deletion – which DIGI would strongly support – consumers may not have control in addressing the increased collection of their personal information.

DIGI notes that SMS, RES and DIS services are likely to have forthcoming related obligations under the Phase 2 Online Safety Act to prevent minors' access to age-inappropriate material; at the time of writing, these codes have been finalised by DIGI and other industry associations and are under consideration from the Office of the eSafety Commissioner, who will develop standards if the protections under the draft codes are considered unsuitable. For SMS, DIS and RES services subject to other regulatory instruments that require a form of age assurance, such as the OSA codes or standards and the Social Media Minimum Age Act (SMMA) 'Reasonable Steps', the OAIC should provide input and align with the approaches that are required of industry (noting that these are still forthcoming at time of writing).

Under the Phase 2 code for Search Engines, developed by DIGI and recently registered by the Office of the eSafety Commissioner, the codes offer flexibility that age assurance must be implemented on logged in accounts in a way that is proportionate to risk, minimises data collection, and complies with privacy laws; we encourage a similarly flexible approach in the COPC, examining how likely an APP entity's service is to be accessed by children and their likely age.

We hope these overarching considerations, as well as the specific insights below provided to the Issues Paper's questions, can be closely considered in the OAIC's advancement of the COPC. We are pleased to see progress on this important code, and we thank you for your consideration of the matters raised in this submission – should you have any questions, please do not hesitate to contact me.

Best regards,

[redacted]

Table of contents

B. Responses to Issues Paper questions

1. Scope of services covered by the code

1.1. As previously explained, the three sets of services to be covered under the code are expansive and diverse. Drawing on DIGI's experience drafting codes for these same three

industry sections, we note that the process for drafting the RES and DIS codes in particular were extremely complicated due to the range of unrelated services included in each group. It is worth noting that the scope of the UK AADC, and covers all entities regulated under the Privacy Act that are likely to be accessed by children, and we would encourage a consistent approach.

1.2. With respect to exclusions (q. 1.2), DIGI considers that a principled risk-based approach should be adopted, with exclusions clearly explained and justified with clear criteria. For example, an exemption for enterprise services may be consistent with its exemption from SMS under the OSA, on the basis that they are often governed by other internal policies and legislation.

1.3. The OAIC should also clarify the interaction between the SMMA and the COPC. For example, under the SMMA, certain SMS providers have an obligation to take reasonable steps to prevent minors from registering an account on the service. The OAIC should give due consideration as to if or how COPC should be implemented on services that are required to prohibit minors under the age of 16 under the SMMA, as the COPC would only apply to 16 and 17 year olds, until the point at which they turn 18. For example, if relevant services implement the forthcoming reasonable steps to prevent account registration from users under the age of 16, those services should be deemed unlikely to be accessible to children under 16. As the Issues Paper acknowledges, the capacity of older teenagers varies greatly from toddlers and other children.

1.4. The scope of services should adopt a risk-based and proportionate approach to differentiate between service type and risk, reflecting the approach in the UK AADC to apply a risk-based and proportionate approach. Codes should operate in harmony with overseas regulatory frameworks, such as the AADC.

2. When and how the code should apply to APP entities

2.1. With the risk-based and proportionate approach suggested above, rather than prescribing age gating or access control, obligations under the COPC should apply depending on how likely an APP entity's service is to be accessed by children and their likely age.

2.2. The Issues Paper asks what threshold should determine when a service is considered ‘likely to be accessed by children’ (q. 2.1). We note that the US Children's Online Privacy Protection Rule (COPPA) uses language of ‘targeted or directed towards’ which would exclude general audience type sites, such as news and many of the general purpose websites captured by the DIS category.

2.3. That said, one of the challenges of the COPPA approach in this context is that COPPA only applies to young people under the age of 13, where it is much easier to distinguish between material targeted to a child of that age vs an adult. In the case of the COPC, there will be challenges distinguishing between the age range of 13-18.

2.4. While we recommend aligning the scope with the UK AADC, there have been challenges in operationalising a similar threshold in the UK (q. 2.2). In this regard, the UK has provided guidance under the AADC asking regulated entities to consider the content and design of a service and whether this is likely to appeal to children, as well as any

measures in place to restrict or discourage their access to the service; for example, an enterprise service may be accessible to a child, but is unlikely to be designed to appeal. We recommend a similar approach.

2.5. In relation to the steps that APP entities should reasonably be expected to take to assess whether children are likely to access their services (q. 2.3, q. 2.7), DIGI suggests that a risk-based approach should inform the approach to age assurance under the COPC. When drafting the OSA codes, the drafters' goal was to require online platforms accessible to minors to restrict Class 2 materials, by implementing appropriate and proportionate measures that ensure a high level of privacy, safety, and security. Class 2 materials that include pornography, content related to crime and violence, self-harm materials (advocating or instructing in self-harm, suicide, or eating disorders), and games simulating gambling. The risk assessment requirements throughout the Codes ensure that measures are only applicable where there is a risk that minors will encounter Class 2 materials, taking into consideration factors such as the number of minors accessing the service. This approach to risk assessment allows for a situation where the functionality of a service rapidly changes, such as through adding a new feature.

2.6. In relation to the potential role of age gating or other access control mechanisms in the COPC (q. 2.4), as previously noted, we recommend that the OAIC give due consideration as to if or how COPC should be implemented on services that are required to prohibit minors under the age of 16 under the SMMA.

2.7. The successful implementation of the SMMA is contingent on two interlinked bodies of work: the 'Legislative Rules' that determine the scope of services captured, and the forthcoming 'Reasonable Steps Guidance' that determine how companies can satisfy the SMMA Act's requirement. The Reasonable Steps Guidance is also to be informed by the findings of the Age Assurance Technology Trial.

2.8. The current uncertainty in timing of the 'Reasonable Steps Guidance' means that it is not clear at time of writing what companies in scope of the SMMA Act must do to comply before the SMMA comes into effect on December 10, 2025. Companies that are currently advancing their implementation run the risk that their plans will not align with the yet-to-be-finalised guidance; conversely, companies waiting for the finalisation of the guidance may not have sufficient time to build compliant technology. To implement a technology project of this magnitude, industry participants require time to develop or procure compliant technology, thoroughly evaluate it in diverse operating environments, and establish supporting systems to ensure safe and secure deployment, including appropriate management of user personal information. Therefore, DIGI recommends that the COPC works appropriately with the SMMA Rules and Reasonable steps. Further, the OAIC might consider issuing joint guidance with eSafety to industry to ensure a co-ordinated approach.

2.9. Regarding alternative approaches that APP entities could take to meet their obligations without age gating or age verification (q. 2.5), the least privacy intrusive way will be through self-identification of age, or verifiable parental consent. This may be appropriate for certain services of low likelihood of access from minors. Consistent with the UK AADC's risk-based and proportionate approach, rather than prescribing age gating or access control, obligations under the COPC should apply depending on how likely an APP entity's service is to be accessed by children and their likely age. For services with strong safety measures and higher likelihood of minor access, the OAIC may consider providing

an option for services where there is no need for age assurance or verification, and the service may choose to apply the COPC to all of its users indiscriminately (i.e., minors and adults alike) as a privacy preserving approach.

3. Age range-specific guidance

3.1. DIGI supports the suggestion of age-based guidance to assist APP entities (q. 3.1), and we suggest that this guidance be based on age brackets of minors, noting the vast differences between toddlers and teenagers. For services with an age limit, such as 13+ or 16+, they should only have to apply the guidance that is relevant to the age range they service.

3.2. While DIGI's members have a range of strict restrictions of advertising to minors, as detailed in Section C of this submission), to the extent that the OAIC is considering restrictions on targeted advertising, it is worth considering how these restrictions align with other areas such as broadcasting advertising restrictions.

4. APP 1 – Open and transparent management

4.1. In relation to the communication methods APP entities should use to ensure privacy policies are meaningfully understood by children of different ages, abilities and backgrounds (q. 4.1), APP entities will be presented with challenges in accurately describing their data processing without oversimplification, and not presenting misleading representations of their full privacy policy. To the extent that child-friendly summaries of privacy policies are a requirement under the COPC, there should be legal protections for APP entities in the COPC that any summaries or graphics do not provide a comprehensive picture of data processing.

4.2. Further, we suggest the OAIC produce guidance on the meaning of 'understood' in this context for relevant age groups, perhaps with examples of language, tools, methods etc.

4.3. In relation to reasonable steps (q. 4.3), the Privacy Act is principles-based and many APPs are already premised on what is 'reasonable', including the measures in relation to children. Reasonable steps should remain risk-proportionate and flexible, allowing APP entities to calibrate their internal privacy practices based on the nature, scale, and context of their services.

5. APP 2 – Anonymity and pseudonymity

5.1. Questions of anonymity and pseudonymity are critical challenges that the OAIC will confront in reconciling rights under APP2 with likely requirements for great age assurance, such as those under the Online Safety Act. On the one hand, anonymity is used to perpetuate harmful content. There are arguments that real names help create a safer environment by making it easier for users to identify who they are connecting with and reducing the likelihood of abusive behavior. On the other hand, many users – including minors – have valid and important reasons for anonymity. For example, as the

Office of the eSafety Commissioner acknowledges[2], a valid reason for anonymity and identity shielding is to protect users from unwanted contact. eSafety encourages children only to use their given name, a nickname or an avatar online instead of a full real name which makes it more difficult for sexual predators and scammers to interact with them. As acknowledged by the former UN Special Rapporteur for Human Rights David Kaye, the ability for users to remain anonymous online can also be an important means for keeping them safe and promoting human rights[3]. These challenges underscore the need for flexibility in the deployment of age gating or age verification in the COPC, given the breadth of its service application to all websites, messaging and interaction services accessible in Australia.

5.2. One of the key questions that the OAIC will need to navigate in relation to anonymity and pseudonymity are the common user choices people will make around whether they wish to be logged-in to a service, or logged out. The state of being logged-in will provide minors with due protections in relation to privacy and safety (some of which are detailed in Section C of this submission), whereas the state of being logged out will provide anonymity or pseudonymity. While the latter may be more appropriate for certain functions young people may seek on digital services, such as help-seeking behaviour, it will also serve to restrict their access to privacy and safety protections.

5.3. Therefore, in considering anonymity and pseudonymity, we encourage the OAIC to adopt a considered approach to imposing default privacy or safety requirements on users who are not logged in; mandating extensive requirements for anonymous users may undermine the value of anonymity for legitimate purposes for children and adults, such as help-seeking and privacy protection.

5.4. Rather than placing broad restrictions on anonymous users, DIGI recommends a more targeted and risk-based approach. For example, this might focus on restricting specific features or content types (e.g. purchasing age-restricted products) to authenticated adults. This approach allows services to maintain the benefits of anonymity and pseudonymity for minors engaging in sensitive or exploratory behaviors, while still ensuring strong protections where the risks are greatest. It also supports a clearer regulatory distinction between the responsibilities owed to logged-in and not logged-in users.

6. APP 3 – Collection of solicited personal information

6.1. In relation to the criteria that defines 'reasonably necessary' when collecting children's personal information for an APP entity's functions or activities (q. 6.1), flexibility will be needed to cater to a wide range of applications. Examples of what may be 'reasonably necessary' could include information that:

6.1.1. is integral to the core functionality of the service (e.g. age or username for account creation, or IP address to display websites in correct language);

[2] Office of the eSafety Commissioner, *Anonymity and identity shielding*, accessed at https://www.esafety.gov.au/about-us/tech-trends-and-challenges/anonymity

[3] Kaye, David (2015), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Human Rights Council,* accessed at https://www.undocs.org/A/HRC/29/32

6.1.2. supports security features;

6.1.3. enables safety features, or age-appropriate experiences;

6.1.4. enables user experience features actively requested by the child, with their consent.

6.2. With respect to the meaning of 'lawful' and 'fair' (q. 6.2), care must be taken to not precede the 'fair and reasonable' test that has been endorsed by the Government in the wider reform of the Privacy Act.

6.3. With respect to questions of parental consent from parents or guardians (q. 6.4), parental consent measures are commonly used by DIGI's members (as detailed in Section C) and are highly recommended in certain situations. However, any universal application of these measures poses implementation and other challenges because different services operate differently.

6.4. Verifiable parental consent will be a highly effective and privacy-preserving method of applying appropriate controls for users for some services. For others, guardian consent requires personal information and, depending on the veracity of verification, may require the collection of secondary documents to verify parental status or guardianship. There are many parents or guardians who do not have the same last name as their children, e.g. because children have the last name of their spouse, due to adoption, or for legal guardians who are not biological parents.

6.5. In contemplating the circumstances where parental consent is appropriate, consideration must be given to situations where teenagers may require access to digital services outside of the purview of their legal guardian, such as to access to assistance or health information. This is particularly relevant in situations where the minor's relationship with their guardian may be constrained.

6.6. This is one of several concerns identified in a UNICEF Discussion Paper, *titled Digital Age Assurance, Age Verification Tools, and Children's Rights Online*[4]. In relation to the UNCRC's Article 2 concerning non-discrimination, the paper states:

"It is important that age assurance processes do not inadvertently discriminate against children who do not have access to official documents, children with developmental delays, children whose ethnicity is not recognized by algorithms used to assess age, or children who do not have parents or caregivers who are able to engage with verification processes that require parental input."

7. APP 4 – Dealing with unsolicited personal information

7.1. DIGI is extremely supportive of offering consumers strengthened consumer rights, such as the right to erasure, the right to access and the right to object, which mirror similar laws under the EU GDPR. When applied economy-wide, affording Australians with these

[4] UNICEF, (2021), *Digital Age Assurance, Age Verification Tools, and Children's Rights Online across the Globe: A Discussion Paper*, https://c-fam.org/wp-content/uploads/Digital-Age-Assurance-Tools-and-Childrens-Rights-Online-across-the-Globe.pd

consumer rights will empower people with a consistent level of choice, control and transparency over their personal information. These same rights may also provide strengthened recourse in circumstances where minors or their guardians become aware of unsolicited personal information.

8. APP 5 – Notification of collection

8.1. With respect to the methods can be employed by APP entities to effectively notify or ensure children are aware of data collection practices in an age-appropriate way (q. 8.1), while user-friendly privacy notices outside of their privacy policies are commonly used by DIGI's members' services, we reiterate that APP entities will be presented with challenges in accurately describing their data processing without oversimplification, and not presenting misleading representations of their full privacy policy. To the extent that child-friendly notices are a requirement under the COPC, there should be legal protections that any summaries or graphics cannot provide a comprehensive picture of data processing.

8.2. With respect to how APP entities ensure that notifications are accessible to children with diverse needs (q. 8.2), the challenge for industry practitioners will be how to determine that a child has diverse needs without collecting more personal or sensitive information. This may require specific OAIC guidance.

8.3. With respect to whether there are circumstances in which an APP entity would be justified in not notifying children about data collection practices (q. 8.3), there may be a range of such circumstances, such as when the data collection is obvious or self-evident, or if it is in the child's best interests to provide minimal information, such as in certain content moderation situations.

8.4. We caution that an over-reliance on notice mechanisms could contribute to 'notice fatigue', much like 'consent fatigue', where users do not pay adequate attention. We also note that there can be a tension between the desire to create notices that are 'understandable' and also legally comprehensive.

9. APP 6 – Use or disclosure

9.1. With respect to the question about how APP entities obtain genuine consent from children or their guardians for use or disclosure of personal information, (q. 9.1), DIGI reiterates the points made above in paragraph 6, in relation to APP 3.

9.2. With respect to the safeguards (q. 9.2), these should be reconciled with any requirements under applicable legislation for a company to be able to demonstrate its compliance to a regulator.

10. APP 7 – Direct marketing

10.1. DIGI agrees with the views expressed by the Australian Government in its response to the Privacy Act reform recommendations[5], where they note that some forms of direct marketing are unlikely to cause harm, such as a person under 18 signing up for a mailing list to be notified about new products. Direct marketing should not be received from third-party businesses where consent has not been obtained. The OAIC guidance on 'the best interests of the child' that we have recommended should include guidance on direct marketing, noting that certain products and services (e.g. educational materials) may fall into this category.

11. APP 8 – Cross-border disclosure

11.1. In its response to the Privacy Act review, the Australian Government agreed with a recommendation in the Privacy Act reform report to introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs under APP 8.2(a). DIGI also broadly supports this proposal in principle, assuming that related data transfers would be similar to those facilitated through adequacy agreements under the GDPR. Taken together, prescribing countries and adequacy agreements could provide an effective mechanism to ensure that children's data is protected when transferred across borders (q. 11.1).

11.2. With respect to the steps that should be taken to communicate with children (or parents) about cross-border data transfer risks (q. 11.2), the OAIC should be mindful of how many notices are being provided to children and parents, and the relative importance to consumers of each of the proposed notices. In a globalised economy, cross-border data transfers are common, and the risks may be better managed in other ways, such as adequacy agreements between countries with comparable legislative protections for personal information.

12. APP 10 – Quality of personal information

12.1. With respect to the question of the meaning of 'accurate', 'up-to-date', 'complete' and 'relevant' mean in the context of children's data (q. 12.1), OAIC guidance would be beneficial. While we appreciate the intent of this is to ensure the data subject's continued permission, 'up-to-date' or 'current' may cause issues if it requires continued communication with the child from the service. 'Accurate' may pose tensions with APP 2 on anonymity and pseudonymity.

13. APP 11 – Security of personal information

13.1. The Issues Paper acknowledges the importance of encryption in children's privacy, and highlights the awareness that young people have in relation to its role in protecting the security of personal information. Encryption of personal information continues to be a

[5] Australian Government, *Government Response to the Privacy Act Review Report*, Attorney-General's Department (28 September 2023), https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF.

critically important technological safeguard used to comply with APP 11. DIGI members' investment in user privacy is complemented by extensive investments in the cyber security of their users, which often includes the use of end-to-end encryption.

13.2. With respect to the question of how APP entities ensure their data retention policies are appropriate for children's data, DIGI also agrees with the Australia Government's recommendation[6] that a review be undertaken of all legal provisions that require retention of personal information, in order to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information.

14. APP 12 – Access to personal information

14.1. DIGI considers that children and adults should have greater consumer rights over their data, including access and deletion, beyond APP 12 which is limited to access. As noted, DIGI is extremely supportive of offering consumers strengthened consumer rights, such as the right to erasure, the right to access and the right to object, which mirror similar laws under the GDPR. The approach to these laws and any related guidance from regulators may prove useful in operationalising APP12 in the COPC.

15. APP 13 – Correction of personal information

15.1. With respect to APP 13, DIGI reiterates our input in relation to APP 12. Some consideration is needed on alignment with journalistic guidelines in relation to minors, to guide participants when journalistic information is republished or quoted on digital services.

Summary of recommendations this submission

A. DIGI encourages consistency with international approaches in the COPC, particularly with the UK Age Appropriate Design Code

B. DIGI recommends that the UNCRC's 'best interests of the child' concept must be foundational to the COPC.

C. DIGI recommends that the OAIC develop technical and operational guidance for all industry practitioners that translates the UNCRC 'best interests of the child' into a digital environment.

D. For SMS, DIS and RES services subject to other regulatory instruments that require a form of age assurance, such as the OSA codes or standards and the SMMA, the OAIC should provide

[6] Australian Government, *Government Response to the Privacy Act Review Report*, Attorney-General's Department (28 September 2023), https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF.

input and align with the approaches that are required of industry – noting that these are still forthcoming at time of writing.

E. The OAIC should give due consideration as to if or how the COPC should be implemented on services that are required to prohibit minors under the age of 16 under the SMMA.

F. The UK has provided guidance under the AADC asking regulated entities to consider the content and design of a service and whether this is likely to appeal to children, as well as any measures in place to restrict or discourage their access to the service. DIGI recommends a similar approach.

G. In relation to the steps that APP entities should reasonably be expected to take to assess whether children are likely to access their services, DIGI recommends a risk-based approach to age assurance.

H. DIGI recommends that the COPC works appropriately with the SMMA Rules and Reasonable Steps. Further, the OAIC might consider issuing joint guidance with eSafety to industry to ensure a co-ordinated approach.

I. For services with higher likelihood of minor access, the OAIC may consider providing an option for services where there is no need for age assurance or verification, and the service may choose to apply the COPC to all of its users indiscriminately (i.e., minors and adults alike).

J. To the extent that the OAIC is considering restrictions on targeted advertising, it is worth considering how these restrictions align with other areas such as broadcasting advertising restrictions.

K. To the extent that child-friendly summaries of privacy policies are a requirement under the COPC, there should be legal protections for APP entities in the COPC that any summaries or graphics do not provide a comprehensive picture of data processing.

L. In relation to the communication methods APP entities should use to ensure privacy policies are meaningfully understood by children of different ages, abilities and backgrounds, DIGI recommends the OAIC produce guidance on the meaning of 'understood' in this context for relevant age groups.

M. Rather than placing broad restrictions on anonymous users, DIGI recommends a more targeted and risk-based approach.

N. With respect to the meaning of ‘lawful’ and ‘fair’, care must be taken to not precede the ‘fair and reasonable’ test that has been endorsed by the Government in the wider reform of the Privacy Act.

O. While parental consent is an effective approach, contemplation must be given to circumstances where parental consent is not appropriate, such as access to assistance or health information.

P. The recommended OAIC guidance on ‘the best interests of the child’ should include guidance on direct marketing, noting that certain products and services (e.g. educational materials) may fall into this category.

Q. Taken together, prescribing countries and adequacy agreements could provide an effective mechanism to ensure that children's data is protected when transferred across borders.

R. With respect to the question of the meaning of 'accurate', 'up-to-date', 'complete' and 'relevant' mean in the context of children's data, DIGI recommends OAIC guidance.

S. DIGI agrees with the Australian Government's recommendation that a review be undertaken of all legal provisions that require retention of personal information, in order to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information.

C. Members' privacy protections for minors

15.2. DIGI's relevant members make major investments in children's privacy and safety, and have extensive technical experience in these areas. In this section are six high-level trends in DIGI's members' approaches to minors' privacy, and some non-exhaustive examples.

16. Default privacy settings for minors

16.1. DIGI's relevant members are enacting strict default privacy settings for minors. Some examples include:

16.1.1. Meta: Instagram Teen Accounts are private by default.

16.1.2. Microsoft: Xbox 'child' accounts have restrictive privacy presets by default.

16.1.3. Pinterest: Under-16s have private profiles as default and only option; 16–17-year-olds must opt-in for public profiles.

16.1.4. Snapchat: All accounts private by default with contact limited to known users.

16.1.5. TikTok: Users aged 13-15 have accounts set to private by default; Others can't use their videos, download posts, or add posts to their stories. Users 16-17 have private by default accounts, but can adjust these to public.

17. Restrictions on unwanted contact

17.1. DIGI's relevant members are enacting restrictions on unwanted contact toward minors. Some examples include:

17.1.1. Apple: Communication Limits lets parents manage who their kids contact. Children must send requests to parents to communicate with new phone numbers.

17.1.2. Discord: When a teen receives a direct message from a user for the first time, Discord will detect if a safety alert should be sent with info on blocking and safeguarding.

17.1.3. Meta: Teens can only be messaged by connections or those they follow on Facebook and Instagram, and have messaged before on Messenger.

17.1.4. Microsoft: Xbox child accounts enable friends-only chat and require approval for friend requests.

17.1.5. Pinterest: Users under 16 can only message mutual followers invited via profile link; 16-17-year-olds receive message requests only from followed users.

17.1.6. Snapchat: Teens can only communicate with mutually accepted friends or saved contacts; teens are blocked from search results unless connected.

17.1.7. TikTok doesn't allow direct messages to be sent to accounts held by under 16s.

17.1.8. Twitch: By default, Twitch blocks private messages from unknown users.

18. Restricting advertising to minors

18.1. DIGI's relevant members have a range of restrictions on advertising toward minors. Some examples include:

18.1.1. Apple: Safari blocks third-party cookies from tracking by default.

18.1.2. Google: Minors have default safeguards to prevent personalised ads and ads from age-sensitive categories.

18.1.3. Meta: Prohibits ads about restricted topics (e.g., alcohol, weight loss) to under 18s.

18.1.4. Microsoft: Does not allow personalised ads for child accounts. Microsoft Edge Kids Mode prevents tracking.

18.1.5. Twitch: Twitch prohibits targeted advertising directed at users under the age of 18.

18.1.6. Yahoo: Provides an ad-free experience for logged-in users under 18.

19. Integrated privacy & safety features

19.1. While this submission does not include an account of the extensive safety features on DIGI member services, there is integration of privacy considerations in safety features. Some examples of this integration include:

19.1.1. Apple: New 'PermissionKit' API allows parental oversight on communications across third-party apps.

19.1.2. Discord: Partnered with safety experts Thorn to design minors' privacy features.

19.1.3. Meta: Facebook and Instagram automatically turn on the most restrictive version of its anti-bullying feature, Hidden Words, so offensive words and phrases are filtered out of teens' comments and DM requests.

19.1.4. Twitch: Twitch uses labels which identify content that may not be appropriate for all audiences. Inappropriate labelled content is unavailable to users who are under 18, or those not logged-in.

20. Family controls

20.1. DIGI's relevant members are enacting various layers of family controls, ranging from the operating system-level to the platform level. Some examples include:

20.1.1. Apple & Google: Applications to enable family sharing and limitations on children's phones and tablets, including privacy settings, content filtering, screen time limits and other features to safeguard experiences online.

20.1.2. Meta: Parental supervision tools on Teen Accounts allow parents to manage privacy settings, time limits, and break schedules.

20.1.3. Microsoft: Family Safety dashboard and Xbox Family Settings allow control over content, screen time, spending, and communication.

20.1.4. Pinterest: Parental Passcode locks certain settings for under-18 accounts

20.1.5. Snapchat: Parents can see which Snapchat friends or Groups their teens have communicated with in the last seven days, in a way that still protects their privacy by not revealing the actual contents of their conversations.

21. Data rights for minors

21.1. As noted, DIGI is extremely supportive of offering all Australians strengthened consumer rights, such as the right to erasure, the right to access and the right to object, which mirror similar laws under the GDPR. DIGI's relevant members offer a full suite of data rights for minors and adults to honour more expansive consumer rights under the EU GDPR. Some examples include:

21.1.1. Meta: Facebook and Instagram self-service tools to enable access, download, and transfer of data about themselves.

21.1.2. Microsoft: Parents can view or delete their child's data via Family Safety tools.

21.1.3. Google: Removal of personal images for under 18s from Google Images results can be requested by kids or parents; 'Results about you' allows anyone to request removal of personal contact info from Google search.