Privacy (Children's Online Privacy) Code 2026

Submission on the Exposure Draft

About IAB Australia

IAB Australia is the industry body for digital advertising in Australia. We bring together members from across the digital advertising supply chain including media owners, ad tech providers, platforms and agencies to share knowledge and insights to support policy making.

Digital advertising is a critical enabler of Australia's broader media, information and tech ecosystem, funding journalism, content creation, and the delivery of online services used by millions of Australians every day. It also plays a crucial role in uplifting small and medium sized businesses and promoting jobs and economic development in Australia.

IAB Australia is one of 47 IAB offices globally, committed to supporting the digital advertising industry and pioneering global solutions and technical standards that promote trust and improve ad experiences for consumers, advertisers, platforms and media.

IAB Australia has a local member base of approximately 180 organisations. The Board includes representatives from Carsales, Domain, Google, Guardian News & Media, Meta, News Corp Australia, Nine Entertainment, REA Group and Southern Cross Media.

Executive Summary

IAB Australia welcomes the opportunity to comment on the Exposure Draft of the Privacy (Children's Online Privacy) Code 2026 (**COPC**) and the accompanying Explanatory Statement. We support the objective of strengthening children's privacy protections online and recognise the importance of ensuring that online services handle children's personal information responsibly.

However, we have significant concerns about aspects of the COPC as drafted.

The COPC should be amended to be consistent with the Privacy Act and the legislative mandate for the COPC, which is to set out how the APPs '*are to be applied or complied with in relation to the privacy of children*'.[1] This may be achieved by:

(i) **making compliance practically possible** so that entities are not forced to apply a code intended to protect children to all end-users (adult and children alike);

(ii) recognising 'that the protection of the privacy of individuals is **balanced with the interests of entities** in carrying out their functions or activities'[2]; and

(iii) **removing obligations that introduce new concepts and rights** that go beyond the Privacy Act.

[1] Privacy Act, s 26GC
[2] Privacy Act, s 2A(b)

Particular concerns:

- **The COPC risks operating as an indirect amendment to the Privacy Act, bypassing the legislative process that such changes would ordinarily require.** The OAIC's stated preference that entities apply the COPC to all users — treating every user as a child — would effectively impose the COPC obligations on the entire digital economy, going far beyond the Code's stated purpose. The COPC also introduces new concepts and rights that are inconsistent with Australian privacy law, including the new right to destruction (s32) and the OAIC's broad reading of the term 'direct marketing' to include targeted advertising.[3]
- **The threshold of 'likely to be accessed by children' is unclear.** Services will be unable to self-assess with confidence, leading either to over-compliance (treating all users as children regardless of actual risk), restricting access to 18+ (often not technically possible), or to inconsistent compliance outcomes as different entities make different decisions.
- **The 'strictly necessary' standard is too narrow and inconsistent with the 'reasonably necessary' threshold in APP 3.** 'Strictly necessary' is a new standard, not used in the Privacy Act 1988 (**Privacy Act**) or in the UK Age Appropriate Design Code (**AADC**). It is unclear whether it permits recommender systems, content personalisation, safety filtering or personalisation of advertising to ensure children receive appropriate content. It should be replaced by the well understood standard of 'reasonably necessary' consistent with APP 3.
- **The 'best interests of the child' standard is unclear and difficult to implement.** The best interests of the child obligation is currently framed as a procedural step to be applied in each individual case. This obligation is unworkable. Commercial entities, with no specific safeguarding expertise, cannot reasonably assess a concept that varies by child, context and circumstance. A better approach would be to incorporate the best interests of the child obligation as an overarching design principle to be applied when designing and operating online services, rather than as a case specific procedural step. This would be in line with the AADC.
- **The consent framework creates significant practical difficulties and burdens on parents and children.** Ascertaining whether a user is under 15, obtaining and verifying parental consent, and managing up to three separate age thresholds - U15, U16 (social media) and U18 - is practically unworkable at scale. When individuals are subjected to repeated consent requests during their digital journey, 'consent fatigue' leads them to agree reflexively and without engagement.
- **The COPC may fundamentally change the nature of the open web.** If compliance obligations under the COPC prove too onerous, service providers may face a commercial decision to restrict access to users aged 18+ (often not technically possible), removing the compliance risk entirely. This outcome would be deeply counterproductive, as an overly burdensome Code could effectively exclude children

[3] This is inconsistent with the recommendations made by the Attorney General in the Privacy Review Report 2022, which explicitly distinguished between 'direct marketing' and 'targeted advertising' in the Privacy Act - discussed further below.

from the very services and information they need to learn, grow, and engage as digital citizens.

- **The COPC goes beyond the UK AADC.** Elements of the AADC appear to have been adopted but many aspects of the COPC extend beyond the AADC, without a clear rationale or evidence in support, such as the under 15 consent requirements and the inflexible 'strictly necessary' threshold. Balancing aspects of the AADC, such as the principle of proportionality, have been omitted. Contrary to its initial mandate, the OAIC acknowledges that the Code departs from '*equivalent international instruments such as the UK's Age Appropriate Design Code*' and instead introduces '*some novel protections*'[4].

Recommendations

Overarching considerations

- The COPC should uplift privacy protections for children while maintaining consistency with the existing Australian privacy law and the UK AADC, in line with the Government's mandate to the OAIC. To the extent that additional protections are required to protect young people, these should be evidenced, risk-based and proportionate.
- The OAIC should clarify that the COPC is not intended to apply to all users as a default compliance strategy.
- The COPC should be amended so that the 'best interests of the child' obligation is incorporated as an overarching design framework in alignment with the UK AADC. It should be applied as a holistic assessment that balances privacy with other children's rights, rather than as a mandate at every individual step of collection, use and disclosure of data.
- The COPC should be amended to make compliance practically possible, so that entities are not forced to apply a code intended to protect children to all end-users (adult and children alike) or age-gate their services to 18+ (often not technically possible).
- The COPC should be carefully reviewed to ensure its children's privacy protections do not, by default, displace the framework that Parliament intended to apply to all end-users or introduce new rights or restrictions that exceed those in the Privacy Act, such as:
  - the 'strictly necessary' default threshold;
  - the right to request destruction of personal information under section 32 of the COPC;
  - the OAIC's broad reading of the term 'direct marketing' to include targeted advertising in section 29.

[4] OAIC media release, 31 March 2026 - https://www.oaic.gov.au/news/media-centre/oaic-releases-exposure-draft-of-the-childrens-online-privacy-code

Specific recommendations

The following recommendations would ensure a risk-based, proportionate approach that uplifts children's privacy while balancing multiple interests (of children, adults and entities) and minimising unintended consequences.

- **Likely to be accessed by children'** (section 7). The OAIC should produce guidance that provides an objective and straight forward way to apply this threshold. It should only capture services targeting children or where there is evidence of a significant number of children on the service. Services that have low or negligible child privacy risks should have no obligations, or fewer obligations that reflect their level of risk.
- **Age assurance**. The COPC should recognise that it may be difficult for entities to determine the age of its users and should explicitly provide for a risk-based, proportionate approach to age assurance, with a spectrum of age assurance methods (including self-declared age) consistent with principles of data minimisation. The obligation to take 'reasonable steps' should not involve an unreasonable financial or administrative burden.
- **Default 'strictly necessary' settings**. The 'strictly necessary' provision at section 9 should be replaced by a 'reasonably necessary' test, consistent with APP 3. Recommender systems, content and advertisement personalisation and safety filtering should all be expressly permitted as part of the core service.
- **Best interests of the child**. The 'best interests of the child' obligation should be incorporated as an overarching design framework in line with UK AADC. The OAIC should publish guidance on 'best interests of the child' before consultation on the COCP is closed. This should explicitly recognise that personalisation to provide age appropriate experiences, personalised content and targeted age appropriate advertising are consistent with the best interests of the child.
- **Consent**. Consent requirements should be removed to reduce the burden on children, parents and business. The requirement to verify parental consent under section 13 should be removed, as should the novel under 15 assent provision under section 20.
- **Internal compliance.** Section 25 should be removed from the COPC. Entities should be able to decide for themselves how to comply with the COPC, without prescribed review cycles.
- **PIAs**. Section 39 of the COPC should be amended to remove the requirement to publish a PIA register online.
- **Mandatory review if Privacy Act is amended**. The COPC must be subject to a mandatory review if the Privacy Act is substantively changed. The Code's scope and obligations were designed with the current Act in mind and amendments to it could have unintended and significant consequences for regulated entities.
- **Implementation timing**. There should be a minimum 18-24 month period following the registration of the COPC before it is enforced.

1. The COPC risks operating as a back-door amendment to the Privacy Act

The OAIC's preference is to apply the Code to all users

The OAIC has repeatedly indicated that its first preference is for entities to apply the COPC to all users rather than taking steps to ascertain the age of their users:

- section 8(5) provides that an entity is not required to ascertain the age of users if it applies the COPC to all end-users regardless of age.
- The OAIC states on its website that the Code '*will also play an important role in uplifting privacy practices across entities more broadly*'.
- The OAIC's guidance note confirms that '*online services might have to either give everyone better privacy protections or check the age of users*'.

If the 'treat all users as children' approach becomes the expected default compliance pathway, the practical effect would be to extend the 'strictly necessary' standard (and the ban on personalised advertising and indirect funding models) to all users of all services.

New rights introduced by the COPC

The COPC introduces new rights and obligations that extend far beyond those contemplated by the Privacy Act and the APP obligations. For example:

- 'strictly necessary' is a new concept that does not appear in the Privacy Act or the APPs;
- OAIC's broad reading of the term 'direct marketing' (to include targeted advertising) in section 29 of the COPC is inconsistent with recommendations made by the Attorney-General in the Privacy Review Report 2022, which explicitly distinguish between "direct marketing" and "targeted advertising" in the Privacy Act;
- the new right to request destruction (s 32) goes beyond the existing APP 11.2 (which instead requires de-identification of personal information). This new obligation will impact on services' ability to use aggregate data for safety and integrity purposes;
- a new under 15 two-step consent plus assent requirement (s 20) that is not present in Australian privacy law or in the UK AADC; and
- the COPC does not balance multiple interests, contrary to the Privacy Act's objective to '*recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities'*.

If implemented in its current form, the COPC would operate as a significant, and largely unscrutinised, amendment to the Privacy Act 1988, without the parliamentary debate or regulatory impact analysis that would normally accompany such a change.

Recommendation

The COPC should be carefully reviewed to ensure its children's privacy protections do not, by default, displace the framework that Parliament intended to apply to adults or introduce new rights that far exceed those in the Privacy Act, particularly:

- the 'strictly necessary' default threshold
- the OAIC's broad reading of the term 'direct marketing' to include targeted advertising in section 29
- the right to request destruction of personal information under section 32 of the COPC.

2. It is near impossible to apply the 'likely to be accessed by children' test without collecting substantial amounts of additional PI or restricting the information that children are able to access

The COPC applies to any APP entity that provides a social media service, relevant electronic service or designated internet service within the meaning of the Online Safety Act 2021.

eSafety has previously explained that *designated internet services* include:

> '*online services such as websites and apps, which are not social media services or relevant electronic services (noting that relevant electronic services mainly provide online communication services)*' [5].

It appears that any provider of an online service, including websites, apps, social media, messaging and other online communication services, will need to consider whether the service is likely to be accessed by children. [6]

While the threshold may initially appear straightforward, its practical application raises significant concerns for services seeking to comply.

It is difficult to know whether a service is 'likely to be accessed by children' without collecting additional data

To work out whether the COPC applies, an entity must determine whether its service is likely to be accessed by children.

The service provider must have some basis for making this determination. Yet for many services, robust age data is unavailable without implementing age-verification or age-estimation mechanisms.

This creates a paradox where complying with the threshold may itself require the collection of additional personal information. This runs counter to the COPC's broader privacy protective objectives. Services that have deliberately minimised data collection (including

[5] eSafety Fact Sheet, June 2024 - Registration of the DIS Standard https://www.esafety.gov.au/sites/default/files/2024-06/Fact-sheet-registration-DIS-Standard.pdf
[6] Part 2, section 7, COPC.

those without logged in users) are, perversely, least equipped to make the assessment the COPC demands.

The 'likely to be accessed' standard is unclear

Neither the COPC nor the Explanatory Statement defines what 'likely to be accessed by children' means in objective quantitative or operational terms. This raises a number of questions:

- What proportion of a service's users must be children before the threshold is crossed?
- Does it turn on actual usage data, the design and content of the service, or both?
- Is a service that is theoretically accessible to children but not marketed to them "likely" to be accessed by them?
- How might the answer to the question vary depending on dynamic content of the site and broader contextual trends in content attracting under 18s?
- How is it possible to differentiate between the type of content or service that will appeal to a 16 or 17 year old, as opposed to an 18 or 19 year old?

This uncertainty is particularly acute given the significant compliance burdens the Code imposes once the threshold is crossed. These include:

- Prohibition of default collection of PI under Part 3, Division 1, section 9.
- Consent framework under Part 3.
- Best interests of the child obligations under Part 3, Division 1, sections 10 and 11.

Services will be unable to self-assess with confidence, leading either to over-compliance (treating all users as children regardless of actual risk), restriction of services to 18+ (often not technically possible), or to inconsistent compliance outcomes as different entities make different decisions.

Proportionality

Even if a service meets the 'likely to be accessed by children' threshold, it may not have any, or minimal, child privacy risks. The COPC treats all services meeting the 'likely to be accessed' threshold the same, regardless of their risk profile.

Services that have low or negligible child privacy risks should have no obligations, or fewer obligations that reflect their level of risk.

Fundamental change to access to the open web

The COPC has the potential to fundamentally change access to the open web. Almost all services are accessed through websites or apps that are openly available. Even if a user then needs to log on or subscribe for further services or content, the initial access is to an open website or app. All such websites and apps are potentially subject to the COPC and must therefore assess whether they are likely to be accessed by children.

These services would have:

- no user record against which age indicators can be assessed;
- no consent architecture that distinguishes adults from children; and

- no practical mechanism for applying the differentiated protections that the COPC contemplates for adults and children.

Whether a website has a subscription model, or is entirely free, or has a combination of free/logged in/subscription content, is immaterial – all are accessed through the open web and will need to consider the requirements of the COPC.

Access to the open web is how children develop digital literacy, access educational resources, engage with news and information and participate in civic and cultural life. A framework that is appropriately protective of children's data is welcome. However, if compliance obligations under the COPC prove too onerous, service providers may face a commercial decision to restrict access to users aged 18 and over, removing the compliance risk entirely.

This outcome would be deeply counterproductive, as in seeking to protect children online, an overly burdensome Code could effectively exclude children from the very services and information they need to learn, grow, and engage as digital citizens.

The Code creates a perverse regulatory incentive to collect *more* user data in order to demonstrate compliance, undermining the privacy protective purpose of the Code. Alternatively, entities might decide to restrict access to 18+, limiting children's access to the open web. Neither of these outcomes are in the best interests of the child.

Recommendations

- The OAIC should produce guidance that provides an objective and straight forward way to apply this threshold. It should only capture services targeting children or where there is evidence of a significant number of children on the service.
- Services that have low or negligible child privacy risks should have no obligations, or fewer obligations that reflect their level of risk.

3. Treating all users as children is a disproportionate response

Section 8(5) provides that the age-ascertainment obligation in section 8(1) does not apply if the entity:

> *'applies this Code, other than this section, in relation to the entity's service regardless of the age of end-users of the service.'*

In other words, the COPC offers entities a compliance shortcut where they can bypass age ascertainment entirely by treating all users (adults and children alike) as subject to the COPC's full protections.

While we understand the practical intent of this provision, IAB Australia is concerned that it may, by necessity, become the default position for many services. Where age ascertainment is technically or commercially infeasible, section 8(5) will function less as an option and more as an obligation.

The result is that the Code's protections would apply to the entire user base of a service, the overwhelming majority of which are adults.

Alternatively, services may simply restrict access to their services to 18+ users because the requirements under the COPC are too onerous and costly to implement. This goes against the objective of digital inclusion and will shut children out from the digital ecosystem.

Treating every adult user as a child for privacy purposes is not a calibrated response to risk. It would impose substantial compliance burdens, constrain product design, erode commercial viability of businesses funding content and services through advertising, and potentially degrade the experience of adult consumers.

Recommendations

- The OAIC should clarify that the COPC is not intended to apply to all users as a default compliance strategy.
- The COPC should be amended to make compliance practically possible, so that entities are not forced to apply a code intended to protect children to all their end-users (adult and children alike) or age-gate their services to 18+.

4. The 'strictly necessary' standard is too narrow and inconsistent with APP 3

The COPC requires entities to implement technical and organisational measures ensuring that only personal information that is 'strictly necessary' to provide the service is collected, used or disclosed by default.[7]

Narrow definition of strictly necessary

The Explanatory Statement confirms that 'strictly necessary' is a narrower threshold than 'reasonably necessary', only permitting the collection of personal information that is:

> '*essential to provide the service… In other words, an entity needs to collect, use and disclose personal information in that way in order to actually deliver the elements of the service the child has signed up for …*[this] '*does not include the collection, use or disclosure of personal information for broader business purposes (e.g. for marketing, service improvement or as part of an indirect funding model*)'

'Strictly necessary' significantly departs from the standard under APP 3

The COPC introduces a materially more onerous privacy framework than currently exists under the Australian Privacy Principles (APPs). Under APP 3.2, entities are permitted to collect personal information where it is:

> *'reasonably necessary for the organisation's functions or activities*'.

[7] Part 3, Division 1, section 9 COPC.

The COPC replaces this with a *strictly necessary* standard which the Explanatory Statement makes clear is deliberately more demanding. Under the COPC information must be '*essential to provide the service*', rather than reasonably necessary for the entity's broader functions.

The practical significance of this shift is considerable:

- '*Reasonably necessary*' accommodates a proportionality assessment - it asks whether collection is justified given the entity's legitimate purposes.
- '*Strictly necessary*' admits no such flexibility. If the information is not essential to deliver the core service (as defined by the OAIC), it cannot be collected by default.

This framework would prevent personalised advertising to children. This is not in the best interests of the child, as it would mean that service providers cannot personalise advertisements to give age appropriate content. Targeted advertising protects children by restricting their exposure to harmful material, as well as giving children (particularly teens) access to adverts that may benefit them, and which they may not wish to share with their parents, such as child support, health services or education and travel options.

IAB's concern is that entities that are unable to conduct age verification or age assurance will be forced to treat all users as though they are under 18. This will result in a near complete ban on personalised advertising, meaning that children may not receive age appropriate advertising content and information. It will also harm businesses who will be subject to a near complete prohibition on data driven direct marketing under the COPC, including in relation to their adult end-users.

The commercial implications of the COPC's departure from the APP framework is significant for services operating ad-supported or marketing-funded business models. This is particularly so for any service that, faced with the practical impossibility of age ascertainment, elects to apply the Code to its entire user base under section 8(5). In that scenario, the marketing restrictions that Parliament intended to apply to children would apply, without differentiation, to all users of the service.

Recommendation

- ➢ The 'strictly necessary' provision should be replaced by a 'reasonably necessary' test, consistent with APP 3.

Permitted uses

It is vital that any standard that is adopted permits the default collection of personal information for the following functionalities. These functionalities must not be considered additional features that would need to be switched off by default:

- **Recommender systems:** Personalised recommendations based on a user's activity are a core feature of many services, including streaming, news and educational platforms.

- **Content personalisation:** Personalising the content shown to a user based on their interests and past behaviour improves user experience and is a fundamental aspect of many digital services.
- **Safety filtering:** Personal information is routinely used to protect children by filtering inappropriate content and advertising, and by promoting safety-related content to younger users (for example, online safety messaging).
- **Personalised advertising:** Personalising marketing content so that it is age appropriate.

If these functions are not permitted by default, it may lead to an erosion in the quantity and quality of services available to children, together with fewer safety controls. The onus will be on children and parents to switch on aspects of a service that enhance its quality. This is a significant obligation when multiplied by the number of online platforms, services and content that each consumer accesses every day.

Recommendation

Recommender systems, content personalisation and safety filtering should all be expressly permitted as part of the core service.

5. The 'best interests of the child' standard is unworkable without clear and business friendly guidance

The COPC makes the concept of 'best interests of the child' central to its framework. Sections 10 and 11 require that the collection, use and disclosure of a child's personal information is consistent with the best interests of the child. Section 10(3) provides that collection through means that are not consistent with the best interests of the child will not be 'lawful and fair' under APP 3.5. As noted above, we recommend that OAIC amend the COPC to incorporate the best interests of the child principle as an overarching interpretive framework, rather than as a mandate at each individual step of data handling.

As the best interests obligation would remain key to the COPC, businesses would require practical guidance on the meaning of best interests of the child to support compliance. While the Explanatory Statement provides a list of factors entities should consider, it acknowledges that 'best interests' will vary depending on the individual child and the context in which the service is used. It states that '[i]*n certain instances, an entity will need to act consistently with the best interests of a particular individual child*'.

IAB Australia is concerned that this standard is near-impossible for businesses to assess in practice, for reasons that include:

- The concept of 'best interests' is inherently subjective and context dependent. It does not translate readily into a compliance standard that can be reliably applied at scale.
- Commercial entities that provide online content and services are not specialists in assessing the best interests of a child.

- Entities will have limited information about individual children using their services, particularly where those services are open to all users.
- Reasonable entities may reach different conclusions about what is in a child's best interests, creating uncertainty and inconsistency in compliance outcomes.
- The potential for retrospective enforcement based on the OAIC's own assessment of what was in a child's best interests creates significant legal risk for entities who have acted in good faith.

The OAIC has indicated it will publish guidance on the meaning of 'best interests'. IAB Australia submits that this guidance must be published before consultation on the COPC is closed, given the centrality of the concept to the framework set out under the Code.

Recommendations

- The 'best interests of the child' obligation should be incorporated as an overarching design framework in line with UK AADC.
- The OAIC should publish guidance on 'best interests of the child' (before consultation on the COCP is closed).
- The COPC should explicitly recognise that personalisation to provide age appropriate experiences and targeted age appropriate advertising are consistent with the best interests of the child.

6. The consent framework creates significant practical difficulties

Onerous for children and parents

The complex consent requirements are impractical and onerous for children, parents and services.

Under the COPC young people and their parents risk being bombarded with consent and transparency requests which will likely be overwhelming. When individuals are subjected to repeated consent requests during their digital journey, 'consent fatigue' leads them to agree reflexively. The result is a degradation of the informed decision making that consent is designed to protect.

Age verification and the collection of additional data

The COPC requires entities to ascertain whether:

- an end-user is **under 15** (to determine whether parental consent is required); and
- **under 18** (for the COPC generally).

Additionally, social media companies must determine whether a child is **under 16** under the separate social media minimum age obligations.[8]

Managing up to three separate age thresholds creates a complex and potentially unworkable compliance environment, particularly for entities whose services are accessed by a broad range of users.

Section 8 requires entities to take reasonable steps to ascertain the age of their end-users, with the level of steps required scaling to the risk of harm from data collection.

While IAB Australia supports a risk-based approach to age assurance, we are concerned that, in practice, it will be very difficult for entities to ascertain age, particularly as it is not easy to distinguish between users within such narrow age bands:

- under 15
- aged 15–17
- 18 and over.

It is hard to see how these age bands could be determined without collecting significant additional personal information. This is inconsistent with the data minimisation requirements in the APPs - a Code designed to protect children's privacy may require entities to collect more data about users in order to comply.

The COPC should encourage entities to use existing data for age assurance where possible, starting with the most privacy preserving age assurance methods before using more intrusive means.

Parental consent verification

Section 13 requires that, for children under 15, consent must be obtained from a person with parental responsibility. Section 13(2) requires entities to take:

> '*reasonable steps to confirm that the person giving consent is a person with parental responsibility for the child*'.

It is very difficult to see how entities will be able to verify parental consent without obtaining further personal information, such as identity documents or government digital ID.

The examples in the Explanatory Statement include:

- email communication
- bank or school vouching
- video conference with customer service
- government digital ID

These mechanisms are all potentially privacy invasive and operationally burdensome, particularly for smaller entities or high-volume services. We strongly urge the OAIC to remove the requirement to verify parental consent.

[8] Online Safety Amendment (Social Media Minimum Age) Act 2024

Consent requirements on open services

The COPC applies equally to open websites. For these services, the entity will have little or no information about the age of their users. The OAIC has suggested that if an entity cannot determine whether its service is accessed by children, it should apply the Code as though all users are children.

This approach creates an impossible situation for open websites, which cannot identify whether a visitor is a child, let alone whether they are under 15 or under 18. It cannot seek age-appropriate consent from a user it cannot identify, and it cannot obtain parental consent from a parent it has no way of contacting.

Open websites would be forced to fundamentally change their access models to comply with the COPC, possibly by requiring logged in users or limiting access to 18+. This would fundamentally change the information available to society via websites and apps, including vital health and well-being information for U15s. Children would have less access to online information or would be able to access it only with parental consent, which may put the child in a worse position, particularly if the information sought relates to issues such as the child's health or family violence.

Recommendations

- The consent requirements should be removed to reduce the burden on children, parents and business.
- The COPC must expressly recognise that entities may not be able to verify the age of their users, and reasonable steps will not involve an unreasonable financial or administrative burden.
- The requirement to verify parental consent under section 13 should be removed, as should the novel under 15 assent provision under section 20.

7. Concerns about Privacy Impact Assessments and Annual Reviews

Privacy impact assessment obligations

Section 38 requires entities to conduct a privacy impact assessment (PIA) before providing any new service or activity likely to be accessed by children, and before implementing any new or changed way of handling personal information that is likely to have a significant impact on the privacy of children. Section 39 requires entities to maintain a register of PIAs and publish it online.

IAB Australia supports the principle of privacy by design and the use of PIAs. However, the requirement to publish a register of PIAs online is likely to undermine the value of PIAs and creates potential commercial sensitivity or security-sensitive issues:

- **Public register requirement is onerous with limited public benefit.** The obligation to publish a register of PIAs online imposes a significant and ongoing administrative burden on regulated entities, many of whom will be conducting multiple PIAs each year as they develop new services or update existing ones.

This burden is not commensurate with any clear public benefit. A PIA register is not a consumer-facing document. It does not assist children or their parents to understand how their personal information is being handled, nor does it provide them with any actionable information.

- **PIAs contain commercially sensitive and confidential information.** PIAs necessarily document an entity's internal assessment of its data flows, risk profile, technical architecture and product development plans. This information is commercially sensitive, confidential and could include unreleased product features, competitive strategies, security vulnerabilities, or the details of third-party arrangements.

  Requiring this information to be published online (even in a register format) or provided to any third party creates risks of competitive harm.

- **Publication risk may undermine the quality and candour of PIAs.** The obligation to publish PIAs may undermine the very practice the OAIC is seeking to encourage.

  PIAs are most valuable when they are conducted with candour, when they identify risks, acknowledge uncertainty, and document the entity's internal deliberations about how to manage those risks.

  If entities know that their PIAs will be listed online and provided to the regulator on request, PIAs will become external-facing compliance documents rather than internal risk assessments. The result might be that PIAs become less useful and less open.

Recommendation

Section 39 of the COPC should be amended to remove the requirement to publish a PIA register online.

Annual review of privacy practices

Section 25 requires entities to review and update their privacy practices, procedures and systems at least annually, and to keep records of those reviews that must be provided to the OAIC on request.

While IAB Australia supports regular review of privacy practices, the annual mandatory review obligation, combined with the requirement to produce records on demand, creates a significant ongoing compliance burden.

Recommendation

Section 25 should be removed from the COPC. Entities should be able to decide for themselves how to comply with the COPC, without prescribed review cycles.

8. Adequate transition period

IAB Australia submits that a minimum 18 to 24 month transition period from the date of finalisation of the Code is required. This is required for entities to:

- conduct privacy impact assessments for all existing services likely to be accessed by children;
- uplift technical capabilities and find workable technical solutions;
- audit and reconfigure their data collection and consent frameworks;
- develop and implement age-appropriate privacy policies, notifications and complaint processes;
- establish education and training programs for staff.

Recommendation

There should be a minimum 18-24 month period following the registration of the COPC before it is enforced.

9. Changes to the Privacy Act could substantially extend the scope of the COPC

The COPC uses many of the definitions set out in the Privacy Act, for example, 'personal information' and 'direct marketing'.

This means that changes to the Privacy Act could substantially broaden the scope of the COPC after its implementation, without any further consultation on the Code itself.

IAB Australia understands that the definitions in the COPC should be tied to those in the Privacy Act, for reasons of consistency and future proofing. However, the impact of definitional changes on the scope of the COPC could be substantial.

Recommendation

The COPC must be subject to a mandatory review if the Privacy Act is substantively changed, as amendments to the Privacy Act could have unintended and significant consequences for regulated entities.

Conclusion

IAB Australia supports the goal of strengthening children's privacy protections online and recognises the importance of well-designed privacy regulation, that protects children's rights without stifling economic productivity. We appreciate the OAIC's consultation process and the opportunity to provide feedback on the Exposure Draft.

However, as set out in this submission, the COPC as drafted contains a number of provisions that are uncertain and unworkable. Addressing these concerns before the Code is

finalised will produce a more effective, proportionate and workable framework that genuinely protects children's privacy while preserving the benefits of the digital ecosystem on which Australians rely.

IAB Australia would welcome the opportunity to discuss these issues further with the OAIC and to participate in any ongoing industry consultation.

For further information please contact:
[redacted] — Director of Policy & Regulatory Affairs
[redacted]