Receiving Officer
COPC@oaic.gov.au
Office of the Privacy Commissioner
GPO Box 5288
Sydney NSW 2001

Electronic Frontiers Australia Inc.
ABN: 35 050 159 188
W: www.efa.org.au
E: Chair@efa.org.au

By email

31 May 2026

Dear Receiving Officer,

Re: Children's Online Privacy Code Submission

Electronic Frontiers Australia (**EFA**) welcomes the opportunity to provide a submission to the Office of the Australian Privacy Commissioner (**OAPC**) regarding the proposed Children's Online Privacy Code (**Code**).

EFA's submission is contained in the following pages.

We would welcome the opportunity to provide further commentary if required. We consent to this submission being published on the OAPC web site.

About EFA

Established in January 1994, EFA is a national, membership-based, not-for-profit organisation representing Internet users concerned with digital freedoms and rights.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties in the digital context.

EFA members and supporters come from all parts of Australia and from diverse backgrounds. Our major objectives are to protect and promote the civil liberties of users of digital communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political, and civil liberties issues involved in the use of digital communications systems.

Yours sincerely,

[redacted]
Chair
Electronic Frontiers Australia

Introduction

Electronic Frontiers Australia (**EFA**) welcomes the opportunity to provide a submission to the Office of the Australian Privacy Commissioner (**OAPC**) regarding the proposed Children's Online Privacy Code (**Code**).

The draft Code, mandated by the *Privacy and Other Legislation Amendment Act 2024 (Cth),* represents an important step towards appropriately safeguarding children's privacy in Australia's rapidly evolving digital landscape. However, as per EFA's previous submission, the approach as proposed by the OAPC for developing the Code continues to be based on the historically inadequate and flawed Australian Privacy Principles (**APPs**). Despite several positive and welcome privacy protections in the Code, these provisions risk replicating the structural weaknesses of our outdated and inadequate privacy framework

EFA's engagement in this consultation is rooted in its longstanding advocacy for strong privacy reforms and the recognition of digital rights as fundamental human rights in Australia[1]. EFA has long asserted that Australia requires a Federally enforceable human rights framework with comprehensive privacy provisions, drawing lessons from jurisdictions like the European Union, where privacy is treated as a fundamental human right and a bulwark against the disproportionate power wielded by government and large technology and commercial interests[2].

For EFA, "privacy" extends beyond mere individual benefit; it is a collective good, essential for societal well-being and democratic health[3]. The exploitative extraction of personal data and widespread algorithmic manipulation that defines today's online experience and digital economy remains a major concern for EFA[4], affecting children, teens and adults alike.EFA believes that effective privacy protection in the digital age cannot be achieved through atomistic, post-hoc **individual vigilance** as per the current 'notice and choice' model[5]. For this reason, the EFA does not consider the APPs an appropriate foundation for the Code.

Privacy is about power. To be effective, the law must respond to this inescapable fact. It requires a paradigm shift from the current consumer-protection model, where individuals are expected to assess potential risks and protect themselves, to a data governance/data fiduciary model, where systemic controls ensure fair, responsible, and safe data handling. This addresses the root causes of privacy harms by applying privacy as the **default state** and going one step further than 'privacy by design'.

Children, as a particularly vulnerable demographic, merit specific and robust privacy protections online[6]. EFA has consistently advocated for policies that prioritise the best interests of the child, acknowledging their graduated autonomy and evolving decision-making abilities as they mature[7].

---

[1] https://www.aph.gov.au/DocumentStore.ashx?id=332e8158-57d0-4420-b502-3dc11449be1a&subId=768049

[2] Ibid.

[3] https://www.efa.org.au/wp-content/uploads/2023/03/2022-01-10-Privacy-Act-Review-Submission.pdf

[4] https://www.aph.gov.au/DocumentStore.ashx?id=332e8158-57d0-4420-b502-3dc11449be1a&subId=768049

[5] https://www.researchgate.net/publication/368644785_Privacy_Decisions_are_not_Private_How_the_Notice_and_Choice_Regime_Induces_us_to_Ignore_Collective_Privacy_Risks_and_what_Regulation_Should_Do_About_It

[6] https://www.clarip.com/data-privacy/gdpr-child-consent/

[7] https://www.efa.org.au/wp-content/uploads/2023/03/2022-01-10-Privacy-Act-Review-Submission.pdf

From EFA's perspective, the Children's Privacy Code is not merely a regulatory instrument but a strategically vital and necessary vehicle for addressing the complex risks and harms children face online. This includes critical issues such as the targeted advertising of harmful products like alcohol, smoking, vaping, and gambling[8]. We believe that this approach is far more sensible than potentially rights-infringing measures, such as blanket social media bans for minors, which can carry significant negative implications for children's autonomy, agency, and human rights[9].

The Code must therefore, provide a nuanced, human rights-aligned solution that avoids enabling unchecked technological innovation and unfettered Big Tech powers. Arguments that laws will "stifle innovation" ironically underestimate the power of technology. If the law poses a challenge, technology will find a solution; after all, technology is designed to solve problems. The law must challenge and guide technology, not be driven by it.

This submission argues for a new regulatory baseline of "Privacy by Default" coupled with the overarching principle of the "Best Interests of the Child" as the necessary solution for establishing a truly safe and empowering internet and digital environment for Australian children.

The draft Code improves significantly upon the APPs but further reform is needed. EFA believes that "Privacy by Design," is a valuable guiding principle but it is insufficient on its own without a strong "Privacy by Default" approach. EFA further argues that the prevailing regulatory model which is heavily reliant upon 'notice, choice, and consent' is fundamentally inadequate for protecting the privacy of children and young people.

EFA's call for strong children's privacy protections is grounded not only in their developmental needs, but in privacy as a fundamental human right at every stage of life. Our failure to adequately protect children's privacy undermines privacy itself as a fundamental right in the digital age.

[8] Ibid.
[9] Ibid

Summary of Recommendations

1. **EFA recommends** that the Code must explicitly state that the determination of a child's best interests is the obligation of the State, not technology companies. Companies are obligated to *act on* these determinations, but their commercial interests inherently preclude them from being the primary arbiters of what constitutes a child's best interests.

   EFA recommends that the Code include a broad definition of “best interests of the child” to ensure comprehensive and well reasoned protection.

   EFA recommends that Clause 10 of the Code be amended to include a mandatory obligation for an APP entity to do a Best Interests of the Child Assessment as part of the further obligations under Clause 38 to conduct a Privacy Impact Assessment.

2. **EFA recommends** the Code mandate a continuous process of Child Rights Impact Assessments (**CRIAs**) for all services “likely to be accessed by children”. These assessments must go beyond eliminating mere data privacy or algorithmic bias, taking a holistic view of all children's rights and well-being. The OAPC should actively work towards developing a practical tool for companies to undertake CRIAs, potentially leveraging UNICEF's ongoing work in this area.

3. **EFA recommends** the Code include a broad definition of "*services likely to be accessed by children*" be used to ensure comprehensive and well reasoned protection.

4. **EFA recommends** the Code adopt the principle of mandatory Privacy by Default. Organisations must be legally required to embed privacy protections into the design and operation of their online services, applications, and products from the outset. Privacy settings should be configured to the highest privacy level by default, ensuring that children’s data is protected automatically without requiring active configuration.

5. **EFA recommends** that the Code must move beyond a primary reliance on Notice, Choice and Consent principles as they have demonstrably failed to provide meaningful privacy protection for adults and children alike, they unfairly place the burden of risk assessment/impact on the individual and are inherently skewed towards benefiting the commercial interests of organizations instead of protecting individuals.

   EFA recommends that the current version of the APPs should **not** be used to draft the Code. Instead, the draft Code should use GDPR equivalent privacy principles to ensure Australia treats privacy as an important human right, which recalibrates rights back to individuals, away from corporate interests, Big Tech and the surveillance-based data extraction apparatus that permeates our online lives.

EFA recommends a limited reliance on consent for exceptional circumstances only. Consent should be a genuinely exceptional mechanism, reserved for cases where data collection is truly optional, clearly explained in age-appropriate language, and where the child (or capable parent, guardian or carer) can genuinely understand and freely choose to provide it without detriment to service access. Consent must be easily withdrawable at any time. The Code should outline stringent requirements for obtaining valid consent from children, with consideration of evolving capacities as they mature, ensuring it is not bundled within the terms of service (as is frequently the case under the APPs).

6. **EFA recommends** an improved definition of personal information should be included in the Code which explicitly includes online tracking technologies, individuation, location data, face and voice recognition, IP addresses, device identifiers, and inferred data.

   EFA recommends the use of robust De-identification and Anonymisation techniques. Where data is used for research or statistical purposes, the Code must mandate the use of genuinely robust de-identification and anonymisation techniques that prevent re-identification or disambiguation, even with the application of sophisticated algorithms or linkages with other datasets. The Code should explicitly prohibit the re-identification of de-identified or aggregated data pertaining to children.

7. **EFA recommends** the Code must explicitly prohibit the collection and use of children's data for the purpose of profiling, behavioural advertising, and targeted marketing. This includes data collected from the child themselves, their device, or inferred from their activity.

8. **EFA recommends** the Code avoid mandating age verification technologies as a privacy protection mechanism. The success of the Code in mandating better privacy practices limiting data collection, restricting secondary uses of personal information and embedding BIC for children could set a powerful precedent for higher privacy standards across all age groups and sectors.

9. **EFA recommends** that the draft Code be amended to include a definition of ‘child’ as a person under the age of 18.

10. **EFA recommends** that access requests made to private sector organisations under Clause 28(1) of the draft Code for or on behalf of children should be fee free.

11. **EFA recommends** for better accountability Clause 38(2) of the draft Code be amended to mandate the conduct of a BIA Assessment to ensure the best interests of the child have been determined and that the form of the BIA assessment be prescribed by the Code. For better transparency under the Code EFA recommends amending Clause 39 (2) in the public PIA register such that all PIA's be published in full, or in part - where there is a lawful reason for doing so.

12. **EFA recommends** that the draft Code be amended to include an 'objects and purposes' clause to favour privacy enhancing interpretation.

Key Issues for EFA

Human Rights Framework and the Best Interests of the Child in a Digital Environment

EFA believes that children's privacy awareness is complex, often distinguishing between interpersonal privacy and institutional data privacy. It also stresses that data collection and processing practices are not merely "e-safety" issues but fundamental data privacy concerns requiring distinct regulatory approaches. A child rights-respecting approach necessitates a shift from a commercially biased 'harm reduction' model to a proactive 'privacy by default' framework that supports children's evolving digital literacy and autonomy.

EFA asserts that children's online privacy must be understood and protected as a fundamental human right, consistent with Article 16 of the UN Convention on the Rights of the Child (**CRC**) and Article 17 of the International Covenant on Civil and Political Rights (**ICCPR**).

EFA recognises the proposed Code has adopted the "*best interests of the child*" (**BIC**) as its primary guiding principle, superseding commercial interests or data exploitation paradigms.

Upholding BIC in the digital environment necessitates a holistic, rights-based approach, as outlined in General Comment No. 25 on Children's Rights in Relation to the Digital Environment[10]. This comprehensive approach involves a thorough assessment of what it truly means to grow up in a digital world, extending even to children without internet access, and understanding the multi-faceted impacts of digital technologies and policies on children's rights. A key element of this approach is the imperative to respect children's evolving capacities (Article 5 UNCRC).

However, applying BIC in the complex and rapidly evolving digital landscape presents significant challenges. These complexities arise from the need to account for diverse needs among children, ensuring coverage for vulnerable cohorts such as LGBTIQ, their varying evolving capacities, persistent inequalities in access and digital literacy, and the relentless pace of technological advancements[11].

The Committee on the Rights of the Child distinguishes between "*best interests assessment*"—which involves evaluating and balancing all necessary elements for a decision concerning a specific child or group—and "*best interests determination*," a more formal process with strict procedural safeguards[12].

A key observation from international bodies is that determining the best interests of a child or children is the *obligation of States* and cannot be delegated to technology companies[13]. While companies may be required through law and other regulatory tools to act on such determinations, allowing them to be the primary arbiters of what constitutes a child's best interests, or even those of adults', has failed as evidenced by the current state of our digital environment and the behaviour of Big Tech players.

[10] https://www.unicef.org/innocenti/media/10571/file/UNICEF-Innocenti-Best-interests-child-digital-environment-brief-2025.pdf
[11] https://www.unicef.org/innocenti/media/10571/file/UNICEF-Innocenti-Best-interests-child-digital-environment-brief-2025.pdf
[12] https://www.unicef.org/innocenti/media/10571/file/UNICEF-Innocenti-Best-interests-child-digital-environment-brief-2025.pdf
[13] https://www.digital-futures-for-children.net/our-work/best-interests

The principle of BIC is not intended to be a substitute for the full range of children's rights, nor should it be used to legitimize a "one-size-fits-all" approach that disregards children's diverse circumstances, or to suggest that any single right can unilaterally trump all others[14]. This is particularly relevant when children's rights are in tension (e.g., privacy versus freedom of expression) or when third-party claims, especially commercial interests, jeopardise children's rights[15].

The concern here is that the concept of "best interests" can be misused or manipulated to prioritise commercial interests, often due to the inherent technical, operational, and legislative complexities involved[16].

If the Code merely mandates a general "consideration" of BIC without clear procedural safeguards and an explicit allocation of responsibility to the State for its determination, it risks becoming a hollow phrase, easily co-opted or diluted by commercial interests, who profit from capturing and exploiting our personal data and surveilling our on-line activities. This would undermine the very protection it aims to provide.

[14] Ibid.

[15] https://www.unicef.org/innocenti/media/10571/file/UNICEF-Innocenti-Best-interests-child-digital-environment-brief-2025.pdf

[16] https://www.unicef.org/innocenti/media/10571/file/UNICEF-Innocenti-Best-interests-child-digital-environment-brief-2025.pdf

1. **EFA recommends** that the Code must explicitly state that the determination of a child's best interests is the obligation of the State, carried out by the OAPC and not technology companies. Companies are obligated to *act on* these determinations, but their commercial interests inherently preclude them from being the primary arbiters of what constitutes a child's best interests.

   EFA recommends that the Code include a broad definition of “best interests of the child” to ensure comprehensive and well reasoned protection.

   EFA recommends that Clause 10 of the Code be amended to include a mandatory obligation for an APP entity to do a Best Interests of the Child Assessment as part of the further obligations under Clause 38 to conduct a Privacy Impact Assessment.

When data extractive, surveillance based technology companies, driven by profit motives and data-intensive business models, are permitted to unilaterally determine or even significantly influence what constitutes a child's "best interests," the principle's original intent is compromised.

The commercial imperative to collect and process vast amounts of data for advertising, profiling, or engagement metrics creates an inherent conflict of interest. This conflict can lead to "best interests" being invoked to justify practices that are commercially beneficial but not genuinely child-centric, thereby eroding privacy protections.

Therefore, for the Code to be truly effective, it must not only mandate the consideration of BIC but also establish robust governance/fiduciary structures, notably, Privacy by Design and Default. This includes requiring independent Child Rights Impact Assessments (**CRIAs**), as proposed by the Committee[17], and clearly defining the State's role in making BIC determinations, with companies obligated solely to *act upon* those determinations. Without this clarity, the principle risks becoming a performative gesture rather than a substantive safeguard.

Furthermore, policies concerning the digital environment must be designed to be future-proof and technology-agnostic, given the rapid advancements in artificial intelligence and other emerging technologies[18]. This means that the Code should not be overly prescriptive about specific technologies or current online platforms, which could quickly become outdated.

Instead, it should focus on establishing enduring principles and mechanisms, such as mandatory default privacy settings and robust Child Rights Impact Assessments, which are applicable across evolving digital landscapes. This approach ensures the Code's long-term relevance and effectiveness in upholding children's rights amidst continuous technological change, rather than requiring constant legislative updates to address new forms of data collection or processing.

[17] Ibid.
[18] Ibid.

2. **EFA recommends** the Code mandate a continuous process of Child Rights Impact Assessments (**CRIAs**) for all services “likely to be accessed by children”. These assessments must go beyond mere data privacy or algorithmic bias, taking a holistic view of all children's rights and well-being. The OAPC should actively work towards developing a practical tool for companies to undertake CRIAs, potentially leveraging UNICEF's ongoing work in this area.

Services likely to be Accessed by children

EFA supports a broad interpretation of "*services likely to be accessed by children*" to ensure comprehensive protection. The Code should apply not only to services explicitly designed for children but also to general audience services that attract a significant child user base, regardless of stated age restrictions. This aligns with the practical realities of children's online engagement, as highlighted by the OAPC's initial feedback from children and young people. The onus should be on the service provider to demonstrate that children are *not* likely to access their service if they wish to avoid the Code's obligations.

3. **EFA recommends** the Code include a broad definition of "services likely to be accessed by children" be used to ensure comprehensive and well reasoned protection.

The Insufficiency of Privacy by Design for Children's Privacy

Privacy by Design (**PbD**), as conceptualized by Ann Cavoukian[19], offers a valuable and comprehensive framework built upon seven foundational principles:

Proactive not reactive;
Privacy as the default setting;
Privacy embedded into design;
Full functionality (positive-sum);
End-to-end security (lifecycle protection);
Visibility and transparency; and
Respect for user privacy (user-centric)[20].

[19] https://en.wikipedia.org/wiki/Privacy_by_design
[20] https://www.onetrust.com/blog/principles-of-privacy-by-design/

These principles advocate for embedding privacy considerations into the core architecture of IT systems and business practices from the outset, rather than treating privacy as a mere add-on or afterthought[21]. This proactive approach is generally beneficial for data protection across all user demographics, fostering a privacy-first attitude and aiming to prevent risks before they materialise[22].

However, while "Privacy as the Default Setting" is indeed one of PbD's seven principles, **relying on the broader PbD framework alone proves inadequate as the *sole* or primary safeguard for children's privacy.**

The inherent flexibility within PbD, particularly its emphasis on "full functionality"[23], can create a subtle but significant tension. This tension arises when other functionalities - such as personalised content, targeted advertising, or extensive data analytics - are deemed equally legitimate design goals from a commercial perspective. For adult users, this might involve mechanisms for the misleadingly named "notice, consent and choice" mechanisms, but for children, this choice is completely illusory.

Children face complex privacy decisions and risks early in their digital lives, often before their media literacy fully prepares them, and their understanding of intricate data practices, including how data is monetised, remains partial and difficult to grasp, even for older children, parents/guardians, and teachers[24]. Consequently, relying on children (or their parents/guardians) to actively navigate complex privacy settings or comprehend nuanced data flows, even if "designed" to be transparent, is unrealistic and places an undue burden on them. Furthermore, the broader critique of consent mechanisms in privacy law, which highlights the "fictions of consent"[25], is particularly pertinent to children, whose capacity for truly informed consent is inherently limited by their age and evolving capacities.

The risk of "balancing" commercial interests under a broad interpretation of Privacy by Design can significantly compromise children's privacy without a strong, explicit default. The current business friendly drafting of the APPs amplifies this aberration. The principle of "best interests of the child" itself, while foundational, involves a "balancing exercise" where competing interests and rights will create considerable tension.

Without a strict mandate for "privacy by default," the broad principles of "Privacy by Design" could allow for this balancing act to be swayed by powerful commercial interests.

This occurs when data collection for profiling, targeted advertising, or engagement metrics is justified under the guise of "full functionality" or enhancing "user experience." The UNICEF paper critically notes that the concept of "best interests" can be "manipulated and exploited... to prioritize commercial interests"[26]. If Privacy by Design is not explicitly and strictly interpreted through the lens of *Privacy by Default* for children, it leaves ample room for such manipulation, inevitably resulting in unsatisfactory outcomes where children's data is collected and used in ways that are not genuinely in their best interests.

---

[21] Ibid.
[22] Ibid.
[23] Ibid.
[24] https://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf
[25] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4333743
[26] https://www.unicef.org/innocenti/media/10571/file/UNICEF-Innocenti-Best-interests-child-digital-environment-brief-2025.pdf

This highlights that the inherent "balancing act" within the broader "Privacy by Design" framework, if not tightly constrained by a "Privacy by Default" mandate, creates a loophole for commercial interests to override the "best interests of the child." Privacy by Design's principle of "Full functionality – Positive-sum, not Zero-sum"[27] suggests that privacy and functionality can both be achieved without trade-offs. However, for children, the reality of data-driven business models often creates a zero-sum game where commercial interests (e.g., maximizing targeted advertising revenue or engagement metrics) directly conflict with their privacy. The potential for "manipulation and exploitation of 'best interests'"[28] is a direct consequence of this tension.

Therefore, the Code must acknowledge this inherent tension. It cannot rely on the optimistic "positive-sum" ideal of Privacy by Design alone. Instead, it needs to impose a regulatory "zero-sum" outcome on data practices that are harmful to children, specifically by mandating "Privacy by Default" as the non-negotiable standard that overrides competing commercial objectives.

For children, "Privacy as the Default Setting" must be elevated from merely one of seven principles within Privacy by Design to a mandatory overarching requirement. This ensures that the highest level of privacy protection is automatically afforded to children, removing the burden of choice from them and their parents or guardians. This approach aligns with the ICO's Children's Code, which specifically mandates "highest privacy settings by default"[29] and explicitly prohibits "nudge techniques" that encourage lower privacy[30].

It fundamentally shifts the responsibility for privacy protection from the vulnerable child to the service provider, where it rightfully belongs.

Privacy by Default: The Non-Negotiable Baseline for Children's Privacy

"Privacy by Default" is the best, human rights based approach to privacy and data protection that mandates products and services be designed with the highest possible level of privacy enabled automatically upon their release[31]. It is a direct and actionable implementation of the second principle within the broader "*Privacy by Design*" philosophy: "*Privacy as the Default Setting*"[32]. The fundamental distinction lies in the requirement for user action. Privacy by Default ensures that individuals are *not* required to take any extra steps to protect their privacy; **it is automatically safeguarded**[33].

---

[27] https://www.onetrust.com/blog/principles-of-privacy-by-design/

[28] https://en.wikipedia.org/wiki/Privacy_by_design

[29] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/designing-products-that-protect-privacy/childrens-code-design-guidance/protect-children-s-privacy-by-default/

[30] https://ondato.com/blog/uk-age-appropriate-design-code/

[31] https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en

[32] https://cookiefirst.com/what-is-privacy-by-default/

[33] https://em360tech.com/tech-articles/what-privacy-design-and-default-essential-guide#:~:text=While%20privacy%20by%20design%20focuses,action%20to%20protect%20personal%20information.

Privacy by Default is essential for children due to their evolving capacities, limited digital literacy, and susceptibility to manipulative design. Children's "*evolving capacities*"[34] mean they may not fully grasp the risks, consequences, and safeguards associated with data sharing and their understanding of how data is recorded, tracked, aggregated, analysed, and monetised is "*partial and difficult to grasp, even for older children, parents, and teachers*"[35].

An important observation from the ICO's Children's Code is that "*Many children just accept whatever privacy settings you provide and never change them*"[36]. This underscores why strong default protections are paramount, rather than relying on children to actively seek out and activate them[37].

Privacy by Default directly counters manipulative design practices, often referred to as "dark patterns," which might encourage children to share more data or lower their privacy settings. It ensures that choices are presented neutrally, or even that "nudge techniques" are used *only* to strengthen privacy settings for younger children. EFA notes that the draft Code has taken steps to ameliorate that problem in part, but not in full.

The effectiveness of mandating "Privacy by Default" for children is directly proportional to the stringency of its implementation and the regulatory oversight, as evidenced by the UK Children's Code.

The UK's Age Appropriate Design Code, by mandating "*high privacy by default*"[38], directly led to tangible, privacy-enhancing changes by major tech platforms. For the OAPC's draft Code, this implies that simply *recommending* privacy by default is insufficient; it must be a *mandated, enforceable standard* with clear expectations for implementation, similar to the UK model, to achieve meaningful impact and overcome potential resistance from commercial interests.

The draft Code must unequivocally require that all online services, websites, and applications likely to be accessed by children (as defined by the Code) have their privacy settings automatically set to the highest possible level of protection upon release and continuously maintained[39]. This means personal data should not be visible or accessible to other users by default. This approach aligns with EFA's call for defaults that prioritise privacy as safeguards against unintended consequences and function creep.

---

[34] https://www.unicef.org/innocenti/media/10571/file/UNICEF-Innocenti-Best-interests-child-digital-environment-brief-2025.pdf

[35] https://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf

[36] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/designing-products-that-protect-privacy/childrens-code-design-guidance/protect-children-s-privacy-by-default/

[37] Ibid.

[38] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/designing-products-that-protect-privacy/childrens-code-design-guidance/protect-children-s-privacy-by-default/

[39] https://cookiefirst.com/what-is-privacy-by-default/

4. **EFA recommends** the Code adopt the principle of mandatory Privacy by Default. Organisations must be legally required to embed privacy protections into the design and operation of their online services, applications, and products from the outset; Privacy settings should be configured to the highest privacy level by default, ensuring that children's data is protected automatically without requiring active configuration.

The Failure of Notice, Choice, and Consent in Privacy

EFA asserts that the prevailing regulatory model and the Australian Privacy Principles enshrined in Australian law is heavily reliant on 'notice, choice, and consent,' is fundamentally flawed and inadequate for protecting privacy in general, but is amplified for children. As articulated by Professor Daniel J. Solove in his work "Murky Consent: An Approach to the Fictions of Consent in Privacy Law,[40] *" the concept of consent in privacy law is often "fictional" or "murky."*

Australia's *Privacy Act 1988 (Cth)* and the APPs made under it are based on the flawed concept of "decisional privacy" which was thought to offer individuals the freedom to act and to make important decisions about how they live their lives, without unjustifiable interference from the state or commercial entities. It gave people the illusion of control over their personal data but this fictional sense of control is frequently wrested forcibly from consumers through abuse of consent mechanisms.

Consent, as evidenced over the last 25 years by the behaviours of Big Tech and innumerable online commercial entities, is used as a '**magic wand**' in the digital/surveillance based economy, to utilise personal data in ways that are completely unrelated to, and/or unnecessary for the particular purpose for which that data was first collected. Consent, although legally flawed, is used by these organisations to use and disclose personal data in ways that would - and should - otherwise be prohibited or curtailed by effective, consumer protective privacy laws.

EFA asserts that the Notice, Choice and Consent model embedded in the APPs has been broken from the start, and has had a predispositional bias to supporting Big Tech and commercial interests more broadly. The following flaws are demonstrable in a clear eyed reading of the APPs:

- **Ambiguity and Manipulation:** Consent is frequently obtained through ambiguous means, and users, including children, can be manipulated into agreement.
- **Cognitive Burden:** The sheer volume and complexity of privacy policies and notices impose an unrealistic cognitive burden on individuals, making genuinely informed decisions practically impossible. This burden is amplified for children and young people. Users often suffer from "consent fatigue."
- **Lack of Understanding:** Individuals, especially children, often lack the capacity or understanding to comprehend the implications of data collection, processing, and future uses. Consent mechanisms assume a level of data literacy and foresight that is unrealistic for the general population and particularly absent in children.

[40] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4333743

- **Ineffectiveness in Modern Data Practices:** In an era of pervasive data collection, aggregation, and re-identification, including through web-scraped AI datasets and sophisticated adtech, individual consent becomes a perfunctory exercise that fails to genuinely empower individuals or constrain data exploitation. Consent is frequently used by organisations on-line as the 'magic wand' that permits all types of unrelated and unnecessary personal data use cases.

For children, all of these failures are amplified. There is no magic age of capacity for understanding complex data practices, and parental consent mechanisms are often equally flawed due to a lack of parental understanding and the sheer volume of digital interactions. In addition there are specific and very difficult challenges posed by targeted advertising and profiling of children, where data is collected and processed in ways that are opaque and beyond the comprehension or control of children and often their parents and guardians.

Children's perceived vulnerability, incapacity for rational decision-making and dependence on adults have been used to justify depriving children of decisional privacy rights and subjecting them to the exercise of adult power over the conditions of their lives. Replicating the flaws of the APPs, including by developing a Code heavily reliant on Notice, Choice and Consent, maintains the privacy status quo and is no great leap forward for children's privacy rights.

5. **EFA recommends** that the Code must move beyond a primary reliance on Notice, Choice and Consent principles as they have demonstrably failed to provide meaningful privacy protection for adults and children alike, they unfairly place the burden of risk assessment/impact on the individual and are skewed towards benefiting the commercial interests of organizations instead of protecting individuals.

   EFA recommends that the current version of the APPs should not be used to draft the Code. Instead, the draft Code should use GDPR equivalent privacy principles to ensure Australia treats privacy as an important human right and there is a recalibration of rights back to individuals, away from Big Tech and the surveillance based data extraction apparatus that controls our online lives.

   EFA recommends a limited reliance on consent for exceptional circumstances only. Consent should be a genuinely exceptional mechanism, reserved for cases where data collection is truly optional, clearly explained in age-appropriate language, and where the child (or capable parent, guardian or carer) can genuinely understand and freely choose to provide it without detriment to service access; Consent must be easily withdrawable at any time; and The Code should outline stringent requirements for obtaining valid consent from children, considering evolving capacities and ensuring it is not bundled with terms of service (as is frequently the case under the APPs).

Fixing the Definition of Personal Information

The definition of "personal information" within the *Privacy Act 1988 (Cth)* as it applies to the Code, has not kept pace with technological advances despite being couched in a set of principles that were claimed to be “technologically neutral”.

The definition must be broadened to explicitly include online tracking technologies, individuation, location data, face and voice recognition, IP addresses, device identifiers, and inferred data[41]. This comprehensive definition is essential to ensure protection against both existing and emerging, sophisticated methods of identification and profiling, addressing concerns about harms from inferred data, such as the widely publicised example of a teenage girl's pregnancy being inferred from grocery purchases[42].

6. **EFA recommends** the Code adopts an improved definition of personal information which explicitly includes online tracking technologies, individuation, location data, face and voice recognition, IP addresses, device identifiers, and inferred data.

   EFA recommends the use of robust De-identification and Anonymisation techniques. Where data is used for research or statistical purposes, the Code must mandate the use of genuinely robust de-identification and anonymisation techniques that prevent re-identification or disambiguation, even with the application of sophisticated algorithms or linkages with other datasets.

Profiling and Targeted Advertising to Children

Specific high-risk data types, such as geolocation information and data used for behavioral profiling (including algorithmic curation and targeted advertising), must be turned entirely off by default.

Any collection or use of such data should require explicit, verifiable, and informed opt-in consent from a parent or guardian, with clear, time-limited options for temporary changes. This directly addresses EFA's concern about the targeted advertising of harmful products to children.

By mandating Privacy by Default, the Code shifts the burden of protection from the child, who lacks full capacity and agency, to the service provider. This is a practical and essential application of the "best interests of the child" principle, acknowledging that children and/or their guardians are unlikely to navigate complex privacy settings or resist manipulative design. The demonstrated success of the UK Children's Code in driving industry change provides a strong precedent for the effectiveness of this approach.

[41] https://efa.org.au/electronic-frontiers-australia-demands-urgent-privacy-reform/

[42] https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

7. **EFA recommends** a prohibition on Profiling and Targeted Advertising for children. The Code must explicitly prohibit the collection and use of children's data for the purpose of profiling, behavioural advertising, and targeted marketing. This includes data collected from the child themselves, their device, or inferred from their activity.

Age Verification Technologies

The draft Code should avoid mandating age verification technologies as a privacy protection mechanism. EFA has significant concerns about such technologies, including their potential to coerce the adoption of digital ID systems and their broader implications for human rights and privacy for all Australians. Implementing laws that are easily bypassed also risks undermining respect for the rule of law.

A strong Children's Online Privacy Code can serve as a catalyst for broader privacy reform and foster a culture of child-centric design. EFA views the Children's Privacy Code as a "sensible" and "appropriate vehicle" for addressing risks, and also advocates for broader modernization of Australia's privacy laws and the establishment of a human rights framework.

The success of the Code in mandating Privacy by Default and embedding BIC for children could set a powerful precedent for higher privacy standards across all age groups and sectors. The OAPC Code should aim to instill a culture where child-centric design, with privacy by default as its cornerstone, becomes an intrinsic part of product development, rather than a mere regulatory hurdle. This requires ongoing engagement, guidance, and potentially incentives for innovation in privacy-protective technologies.

8. **EFA Recommends** the Code avoid mandating age verification technologies as a privacy protection mechanism.The success of the Code in mandating Privacy by Default and embedding BIC for children could set a powerful precedent for higher privacy standards across all age groups and sectors.

Defining a Child

The Code does not define a child, but it makes special provision for privacy protections that apply to persons under the age of 18. It also tries to align with certain provisions of the Online Safety Act 2021 (Cth) where minors within certain age bands are restricted from accessing social media sites etc.

In our view, a person below the age of 18 years is a child, unless majority is attained earlier under applicable law. Defining a child as an individual under 18 years of age will allow for the development of child-specific privacy protections in the Code. This position would also be consistent with the Online Safety Act 2021 (Cth) (Online Safety Act),the UK Age Appropriate Design Code and Ireland's Data Protection Act.

9. **EFA recommends** that the draft Code be amended to include a definition of 'child' as a person under the age of 18.

Right to request information about handling of personal information

Clause 28 (1) of the draft Code creates a right where a child, or a person with parental responsibility for a child, requests access to personal information about the child under Australian Privacy Principle 12.1, the child or person may also request information about the entity's handling of the child's personal information, to the extent the entity holds that information.

The expression of this right under the APPs may result in fees or charges being borne by the applicant. Given the infrequent nature of access requests received by private sector organizations, EFA proposes that the processing of access requests for or on behalf of children should be fee free.

10. **EFA recommends** that access requests made to private sector organisations under Clause 28(1) of the draft Code for or on behalf of children should be fee free.

Privacy Impact Assessments (PIA)

Clause 38 (1) of the draft Code provides that an APP entity must undertake a PIA where the entity proposes to provide a new service or a new activity that is likely to be accessed by children or will be primarily concerned with the activities of children or where it proposes to adopt any new or changed ways of handling personal information in relation to an existing service or activity that are likely to have a significant impact on the privacy of children. Further at Clause 39 (1) and (2) of the draft Code an entity must maintain a register of the PIAs that it conducts and must publish the register online.

EFA supports this proposed Code language **in part** as we feel the obligation is not strong enough for the perspective of both transparency and accountability.

11. **EFA recommends** for better accountability Clause 38(2) of the draft Code be amended to mandate the conduct of a BIA Assessment to ensure the best interests of the child have been determined and that the form of the BIA assessment be prescribed by the Code. For better transparency under the Code EFA recommends amending Clause 39 (2) in the public PIA register such that all PIA's be published in full, or in part - where there is a lawful reason for doing so.

Objects and Purposes of the Code

The draft Code, its effectiveness and ease of implementation from an entity's perspective would be improved if the Code were amended to include an 'objects and purposes' clause.

By adopting an appropriately drafted objects and purposes clause it would require entities to ensure that their decisions are framed in such a way to meet both the express and implied privacy protections offered to children in the draft Code. Such guidance in legal interpretation would reasonably ensure that human rights outcomes are achieved in respect of all parties subject to the draft code.

12. **EFA recommends** that the draft Code be amended to include an 'objects and purposes' clause to favour privacy enhancing interpretation.

Closing Comments: Securing a Safe Digital Future for all Australian Children

The digital environment is an integral and ever-expanding part of children's lives, offering immense opportunities but also presenting unique and evolving risks to their privacy and well-being. A strong, effective, and enforceable Children's Online Privacy Code is essential to safeguard the rights of Australian children in this interconnected world.

EFA firmly believes that the Code, with Privacy as the Default and the Best Interests of the Child as its foundations, can offer an appropriate and effective mechanism to address the complex challenges of children's online privacy, far more so than broad, rights-infringing measures like social media bans[43].

As demonstrated throughout this submission, the 'Best Interests of the Child' must be the guiding ethical and legal principle of the Code, with responsibility for its determination resting clearly with the State. Meaningful protection of children's privacy therefore requires the mandatory implementation of 'Privacy by Default', ensuring privacy is built into digital services automatically, rather than relying on children, guardians or parents to navigate complex settings to secure it.

Given the structural deficiencies of the APPs and the inherent absurdist approach to the self management of individual privacy rights, EFA advocates for a fundamental shift in privacy regulatory strategy.

[43] https://www.aph.gov.au/DocumentStore.ashx?id=1cea815d-201d-4484-9ec7-67cb64aed42c&subId=774044

EFA believes that effective privacy protection for both children and adults requires moving beyond placing the onus on individuals through the frequently abused processes of notice, choice and consent, and instead focusing on regulating the architecture that structures the way information is used, maintained, and transferred.

This systemic approach involves restricting data collection, use, storage, and transfer at an institutional level. Effective privacy protection in the digital age cannot be achieved through atomistic, post-hoc individual vigilance. It requires a paradigm shift from a consumer-protection model, where individuals are expected to protect themselves, to a data governance/fiduciary model, where systemic privacy by default controls ensure responsible data handling.

By adopting these foundational principles rigorously, the OAPC can establish a Children's Online Privacy Code that genuinely empowers children, fosters their holistic development, and secures a safe, rights-respecting digital future for all young Australians. This will position Australia as a leader in child online safety, fostering trust and enabling children to engage with the digital world securely and confidently.

END

[redacted]

Chair

Electronic Frontiers Australia

[redacted]

31/05/2026