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

[redacted]
Office of the Australian Information Commissioner
[redacted]

26 July 2025

By email

Dear [redacted],

RE: Children's Online Privacy Code

Electronic Frontiers Australia welcomes the opportunity to provide a submission to the Office of the Australian Privacy Commissioner (**OAIC**) regarding the proposed Children's Online Privacy Code (**Code**). This Code, mandated by the *Privacy and Other Legislation Amendment Act 2024 (Cth*), represents a crucial step towards solving a long standing structural flaw in Australia's privacy law regime and to put in place corrective standards and architectures for the safeguarding children's privacy in Australia's current digital landscape which favours surveillance based data extraction and the exploitation of children.

Our submission is contained in the following pages. For the purposes of brevity and efficiency EFA has summarised select issues that are of significant concern to EFA and which were also the subject of substantial representations in our earlier submissions on the review of the *Privacy Act 1988 (Cth).*

About EFA

Established in 1994, Electronic Frontiers Australia, Inc. (**EFA**) is a not-for-profit national organisation that works to ensure that technology makes our lives better, not worse. We promote the idea that digital rights are human rights.

EFA was formally incorporated under the Associations Incorporation Act (S.A.) in May 1994. In September 2024 EFA was approved as a registered charity with the Australian Charities and Not-for-Profits Commission http://www.acnc.gov.au . EFA's charity status was backdated to 01/07/2023.

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 online digital rights. EFA members and supporters come from all parts of Australia and from diverse backgrounds. They are people who recognise that preserving freedoms and rights always depends on the willingness of people to defend them and that combating the threats posed by anti-civil libertarian forces, unfettered technological solutionism and ill-informed reports in the media requires constant vigilance and support.

Yours sincerely,

[redacted]

Electronic Frontiers Australia Inc.

Submission to the Office of the Australian Privacy Commissioner on the Children's Online Privacy Code: Recognizing the Best Interests of the Child, Prioritising Privacy by Default, Acknowledging the Fiction of Notice, Choice and Consent, and the Redundancy of the Australian Privacy Principles.

Introduction

Electronic Frontiers Australia (**EFA**) welcomes the opportunity to provide a submission to the Office of the Australian Privacy Commissioner (**OAIC**) regarding the proposed Children's Online Privacy Code (**Code**). This Code, mandated by the *Privacy and Other Legislation Amendment Act 2024 (Cth),* represents a crucial step towards appropriately safeguarding children's privacy in Australia's mature and fast moving digital landscape. However, the current approach as proposed by the OAIC of developing a Children's Privacy Code based on the archaic, historically inadequate and flawed Australian Privacy Principles (**APPs**) will only serve to replicate existing structural weaknesses in a seriously outdated and sub-standard privacy rights 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

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

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 pervasive and exploitative nature of surveillance-based personal data extraction, coupled with endemic algorithmic behavioural modification that defines our experiences on-line, remains a profound concern for EFA[4] as not only children and young people but also adults are similarly exploited while participating on-line and navigating our so called "digital economy".

EFA believes that effective privacy protection in the digital age cannot be achieved through atomistic, post-hoc individual vigilance as per the current model. And for this precise reason, the APPs should **not** be used as the foundation of the new Children's Privacy 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 responsible, safe and fair data handling. This addresses the root causes of privacy harms by applying privacy as the default state, rather than attempting to bolt on a compromised version of privacy, often facilitated by the relatively unchecked collection of personal data, coupled with frequently unethical and potentially unlawful use of the concept of consent to authorise a range of unrelated uses and disclosures of personal data.

In applying these foundational principles, children, as a particularly vulnerable demographic, merit specific and robust privacy protections online[5]. 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[6].

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 [7], information being misused by predators or abusive partners or family members, impersonation, identity theft, and scamming, surveillance, image-based abuse, and a host of other major and unprecedented privacy violations children face online today. This approach is considered far more sensible than broad, 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[8]. The Code, therefore, must represent a nuanced, human rights-aligned solution that avoids the pitfalls of of laws resulting in unchecked technological innovation and unfettered Big Tech powers, positioning it as an effective policy instrument to mitigate against the entrenched harms of Big Tech and the surveillance based data extractive industrial complex. Arguments that law 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.

---

[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.clarip.com/data-privacy/gdpr-child-consent/

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

[7] Ibid.

[8] Ibid

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. EFA believes that "Privacy by Design," while valuable as a guiding philosophy, is insufficient on its own to achieve these critical objectives for children, often leading to unsatisfactory outcomes if not rigorously applied with a default-first approach. EFA asserts that the prevailing regulatory model, heavily reliant on 'notice, choice, and consent,' is fundamentally flawed and inadequate for protecting the privacy of children and young people.

Given the profound limitations of individual privacy rights and their self-management, EFA advocates for a fundamental shift in privacy regulatory strategy. 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 controls ensure responsible data handling. This addresses the root causes of privacy harms by designing privacy at its highest default level, rather than attempting to bolt it on through compromised individual consent after the fact.

EFA's argument for robust children's privacy is not merely about their specific developmental needs but is deeply rooted in the broader human right to privacy. Our current failure to effectively protect children's privacy undermines the very notion of privacy as a fundamental right in the digital age.

Summary of Recommendations

1. **EFA recommends** the Code 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.

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 OAIC 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** a broad interpretation of "*services likely to be accessed by children*" be used to ensure comprehensive 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. This includes: Location services off by default; Public sharing/posting off by default; Direct messaging off by default; and No automatic sharing with third parties.

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, new, modern and GDPR equivalent privacy principles must be developed 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.

6. **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).

7. **EFA recommends** the Code adopt the principle of Data Minimisation as the Default: Organisations must be mandated to collect only the absolute minimum amount of personal information necessary to provide the core service. This principle should apply by default, without requiring any action from the child or parent/guardian; and, the Code should **clearly** and **narrowly** define what constitutes "necessary" data for typical services likely to be accessed by children and prohibit the collection of any additional data.

8. **EFA recommends** the Code impose strict data retention limits, requiring that children's personal information is securely deleted or permanently anonymised once the purpose of processing has been achieved, where the child revokes their consent or immediately after the expiry of any statutory requirement to retain data.

9. **EFA recommends** the Code adopt the principle of Purpose Limitation and Proportionality. Personal information collected from children should only be used for the specific purpose for which it was collected and that purpose must be clearly defined, legitimate, and in the best interests of the child; and, any use of data beyond this defined purpose, particularly for related secondary uses like analytics, research, marketing or service improvement, must be strictly prohibited unless it can be demonstrated to be strictly necessary, proportionate, and demonstrably beneficial to the child, and in a fully de-identified or aggregated form that cannot be re-identified.

10. **EFA recommends** the Code contain an up-dated, fit for purpose definition of personal information which explicitly includes modern day data collection and management practices such as online tracking technologies, individuation, location data, face and voice recognition, IP addresses, device identifiers, and inferred data.

11. **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.

12. **EFA recommends** the Code mandate the use of robust De-identification and Anonymisation techniques. Where data is used for lawful 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; and, the Code should explicitly prohibit the re-identification of de-identified or aggregated data pertaining to children.

13. **EFA recommends** the Code mandate use of simplified language and formats suitable for different developmental stages in privacy policies, notices, statements and legal terms and conditions, ensuring that information is genuinely accessible and comprehensible to its target audience - young people and parents/guardians.

14. **EFA recommends** that for the Children's Online Privacy Code to be truly effective, it must be robustly enforceable under the *Privacy Act 1988 (Cth)*, and provide equivalent human rights protections given under the *EU's General Data Protection Regulation (2018)* and other comparable international frameworks.

15. **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. The Code should aim to instill a culture where child-centric design,

with Privacy by Default and the Best Interests of the Child as its cornerstones, becomes an intrinsic part of product development, rather than a mere regulatory hurdle.

Key Issues for EFA.

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

EFA asserts 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**). The proposed Code should unequivocally adopt the "*best interests of the child*" as its primary guiding principle, superseding commercial interests or data exploitation paradigms.

The "*best interests of the child*" (**BIC**) is a multifaceted concept, recognised globally as a substantive right, a fundamental legal principle, and a rule of procedure[9]. Its importance is rooted in international law, is enshrined in Article 3(1) of the United Nations Convention on the Rights of the Child (**UNCRC**) and further articulated in Article 24(2) of the Charter of Fundamental Rights of the European Union[10]. This principle mandates that in all actions concerning children—whether undertaken by public authorities, private social welfare institutions, courts of law, administrative bodies, or legislative bodies—the child's best interests shall be a primary consideration[11]. Fundamentally, BIC implies the "*full and effective enjoyment of all the rights recognised in the UNCRC and the holistic development of the child*" in both the immediate and longer term[12]. This holistic development encompasses the child's physical, psychological, moral, and spiritual integrity, actively promoting their human dignity[13].

---

9 https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migration-glossary/glossary/best-interests-child-bic_en

10 Ibid

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

12 https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migration-glossary/glossary/best-interests-child-bic_en

13 https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migration-glossary/glossary/best-interests-child-bic_en

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[14]. 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) and their fundamental right to be heard (Article 12 UNCRC)[15]. Active and meaningful child participation in policymaking, as well as in the design and development of digital technologies, is crucial to ensure that their inputs genuinely lead to safer, more inclusive, and empowering digital experiences for all children[16].

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[17]. 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[18]. Making individual BIC determinations for millions of children online is simply impractical; consequently, assessments often must be made collectively on behalf of all children, regardless of their individual circumstances[19].

A critical 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[20]. 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 **has failed as evidenced by the current state of our digital environment.** 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 legitimate a "one-size-fits-all" approach that disregards children's diverse circumstances, or to suggest that any single right can unilaterally trump all others[21]. 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[22]. **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**[23]. 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 and Big Tech and all commercial organisations 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] https://www.unicef.org/innocenti/media/10571/file/UNICEF-Innocenti-Best-interests-child-digital-environment-brief-2025.pdf

[15] Ibid.

[16] Ibid

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

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

[19] https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migration-glossary/glossary/best-interests-child-bic_en

[20] https://www.digital-futures-for-children.net/our-work/best-interests

[21] Ibid.

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

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

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.

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[24] , 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[25]. 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, that 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.

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 OAIC should actively work towards developing a practical tool for companies to undertake CRIAs, potentially leveraging UNICEF's ongoing work in this area.

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 OAIC's initial feedback from children and young people. The onus should be on the service provider to

[24] Ibid.
[25] Ibid.

demonstrate that children are *not* likely to access their service if they wish to avoid the Code's obligations

EFA Recommends a broad interpretation of "*services likely to be accessed by children*" be adopted in the Code to ensure comprehensive protection.

The Insufficiency of Privacy by Design for Children's Privacy

Privacy by Design (**PbD**), as conceptualized by Ann Cavoukian[26], 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)[27]. 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[28]. 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[29].

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"[30] , 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[31]. Consequently, relying on children (or even 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"[32] , is particularly pertinent to children, whose capacity for truly informed consent is inherently limited by their age and evolving capacities.

[26] https://en.wikipedia.org/wiki/Privacy_by_design
[27] https://www.onetrust.com/blog/principles-of-privacy-by-design/
[28] Ibid.
[29] Ibid.
[30] Ibid.
[31] https://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf
[32] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4333743

The risk of "balancing" interests under a broad interpretation of Privacy by Design can significantly compromise children's privacy without a strong, explicit default. The principle of "best interests of the child" itself, while foundational, involves a "balancing exercise" where competing interests and rights can 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"[33]. 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.

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"[34] 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"[35] 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"[36] and explicitly prohibits "nudge techniques" that encourage lower privacy[37]. **It fundamentally shifts the responsibility for privacy protection from the vulnerable child to the service provider, where it rightfully belongs.**

---

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

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

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

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

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

"Privacy by Default" is a critical 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 [38]. It is a direct and actionable implementation of the second principle within the broader "*Privacy by Design*" philosophy: "*Privacy as the Default Setting*"[39]. 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**[40]. In contrast, "Privacy by Design" is a more encompassing set of seven foundational principles that guide the *entire* development process, aiming to embed privacy throughout[41]. While Privacy by Design *includes* the default setting, its broader scope does not inherently mandate it as the sole or overriding principle, which is precisely why it is insufficient on its own for children.

Key characteristics of Privacy by Default include:

- **Automatic Highest Privacy Settings:** The Code must ensure that the default settings of any product or service accessed by children automatically offer the highest level of privacy protection[42]. This means children's personal data should only be visible or accessible to other users if they, or their parent/guardian, actively and explicitly choose to change those settings[43]. This default must be maintained even after service updates[44].
- **Data Minimisation:** A core tenet of Privacy by Default is strict data minimisation. Companies must limit the amount and types of data collected and processed to only what is strictly necessary for the service's core functionality, for one specific purpose, and with no additional processing or sharing without explicit consent[45].
- **Opt-in Consent:** Privacy by Default inherently relies on an 'opt-in' approach to user consent[46]. For children, this is typically operationalised through requirements for verifiable parental consent *before* any personal information is collected, with narrowly defined exceptions.

---

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

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

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

41 https://www.onetrust.com/blog/principles-of-privacy-by-design/

42 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/

43 https://ondato.com/blog/uk-age-appropriate-design-code/

44 Ibid.

45 https://www.onetrust.com/blog/principles-of-privacy-by-design/

46 https://cookiefirst.com/what-is-privacy-by-default/

- **Retention Limits:** Data collected from children should only be stored for as long as is reasonably necessary to fulfill the purpose for which it was collected, and then promptly and securely deleted[47].
- **Security Measures:** Robust technical and organisational measures, such as encryption of data in transit and at rest, are essential to ensure the confidentiality, integrity, and availability of children's personal data[48].

Privacy by Default is essential for children due to their evolving capacities, limited digital literacy, and susceptibility to manipulative design and dark patterns. Children's "*evolving capacities*"[49] 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*"[50]. A critical observation from the ICO's Children's Code is that "*Many children just accept whatever privacy settings you provide and never change them*"[51]. This underscores why strong default protections are paramount, rather than relying on children to actively seek out and activate them[52]. 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.

International precedents strongly support this approach. The UK's Age-Appropriate Design Code (**Children's Code**) explicitly mandates "*highest privacy settings by default*" for services accessed by children under 18. This statutory requirement has led to significant positive changes from major tech companies, such as Instagram making under-18 accounts private by default. Similarly, Children's Online Privacy Protection Act (**COPPA**) in the USA implements principles akin to Privacy by Default through its stringent verifiable parental consent requirements and limitations on data use.

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*"[53], directly led to tangible, privacy-enhancing changes by major tech platforms. For the OAIC's 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 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[54]. 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.

---

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

[48] Ibid.

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

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

[51] 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/

[52] Ibid.

[53] 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/

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

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. This includes: Location services off by default; Public sharing/posting off by default; Direct messaging off by default; No automatic sharing with third parties.

The Failure of Notice, Choice, and Consent in Children's Online Privacy (and the concept of privacy more generally!)

EFA asserts that the prevailing regulatory model, heavily reliant on 'notice, choice, and consent,' is fundamentally flawed and inadequate for protecting privacy, particularly for children. As articulated by Professor Daniel J. Solove in his work "Murky Consent: An Approach to the Fictions of Consent in Privacy Law,[55] *" 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, both domestically and internationally, to do a wide range of other uses and disclosures of personal data completely unrelated to 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, particularly on young children, making genuinely informed decisions practically impossible. 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

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

mechanisms assume a level of data literacy and foresight that is unrealistic for the general population and particularly absent in children.

- **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.

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, new, modern and GDPR equivalent privacy principles must be developed 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).

Data Minimisation and Retention Limits.

The Code must reinforce the principle of data minimisation, ensuring that only the absolute minimum amount of personal information necessary for the service's specific, stated core function is collected. This directly aligns with EFA's broader advocacy for limiting ubiquitous data extraction and algorithmic behavioural modification.

Furthermore, the Code must not only enforce strict data minimisation, it needs to also explicitly prohibit manipulative design. Services must collect only the absolute minimum amount of personal data necessary to provide the core functionality of the service, and for one specific purpose. Any design features, prompts, or "nudge techniques" that encourage children to share more data or lower their privacy settings must be prohibited. Instead, design should actively guide children towards stronger privacy options.

EFA recommends adopting the principle of Data Minimisation as the Default. Organisations must be mandated to collect only the absolute minimum amount of personal information necessary to provide the core service. This principle should apply by default, without requiring any action from the child or parent/guardian; and, The Code should clearly define what constitutes "necessary" data for typical services likely to be accessed by children and prohibit the collection of any additional data.

The Code should also impose strict data retention limits, requiring that children's personal information is deleted using reasonable measures once it is no longer necessary for the purpose for which it was collected. This prevents indefinite retention and potential future misuse. Cyber risks are also reduced.

EFA recommends the Code impose strict data retention limits, requiring that children's personal information is securely deleted or permanently anonymised once the purpose of processing has been achieved, where the child revokes their consent or immediately after the expiry of any statutory requirement to retain data.

Purpose Limitation and Proportionality

The "Purpose Limitation" principle dictates that personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes. This prevents "function creep," ensuring data isn't used for unforeseen reasons without a new legal basis.

The "Proportionality" principle (often linked with data minimisation) means that the personal data collected must be adequate, relevant, and limited to what is necessary for the stated purpose. Any use of data beyond this defined purpose, particularly for secondary uses like analytics, research, or service improvement, must be strictly prohibited unless it can be demonstrated to be strictly necessary,

proportionate, and demonstrably beneficial to the child, and in a fully de-identified or aggregated form that cannot be re-identified.

EFA recommends the Code adopt the principle of Purpose Limitation and Proportionality based on the corresponding principles found in the *EU General Data Protection Regulation (2018).* Personal information collected from children should only be used for the specific purpose for which it was collected and that purpose must be clearly defined, legitimate, and in the best interests of the child; and, any use of data beyond this defined purpose, particularly for related secondary uses like analytics, research, or service improvement, must be strictly prohibited unless it can be demonstrated to be strictly necessary, proportionate, and demonstrably beneficial to the child, and in a fully de-identified or aggregated form that cannot be re-identified.

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[56]. 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[57].

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.

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 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.

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

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

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 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.

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.

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; and The Code should explicitly prohibit the re-identification of de-identified or aggregated data pertaining to children.

Transparency and Age-Appropriate Information.

While advocating for a shift away from notice and consent, EFA acknowledges the importance of clear communication. Any information provided to children and their parents/guardians must be in plain, accessible, and age-appropriate language, avoiding legalistic jargon. User interfaces should empower children (where appropriate) and parents/guardians with clear, easily discoverable, and understandable privacy controls.

The Code must require privacy policies and information about data collection and use to be presented in a clear, concise, and age-appropriate manner, understandable by children and their parents. This includes using simplified language and formats suitable for different developmental stages, ensuring that information is genuinely accessible and comprehensible to its target audience. While "Privacy by Default" reduces the need for children to make active choices, transparency remains vital for parental oversight and for older children to develop digital literacy. This recommendation supports the "Visibility and Transparency" principle of Privacy by Design.

EFA recommends the use of includes using simplified language and formats suitable for different developmental stages in privacy policies, notices, statements and legal terms and conditions , ensuring that information is genuinely accessible and comprehensible to its target audience - young people and parents/guardians.

Robust Enforcement and Accountability.

The Code should require transparency, explainability, and auditable mechanisms for any automated decision-making systems that use children's personal information, with a right to human review for significant decisions. This is crucial for accountability in an increasingly algorithmic digital environment.

EFA recommends that for the Children's Online Privacy Code to be truly effective, it must be robustly enforceable under the *Privacy Act 1988 (Cth)*, and equivalent to the human rights protections given under the EU's General Data Protection Regulation (2018) and other international frameworks.

Age Verification Technologies

Finally, the 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 OAIC 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.

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. The 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.

Conclusion: 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 not merely desirable but 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[58].

As demonstrated throughout this submission, the principle of the "Best Interests of the Child" must serve as the overarching ethical and legal compass for the Code, with its determination residing firmly and unequivocally with the State. Operationalising this principle, and truly protecting children's privacy in a meaningful way, necessitates the mandatory implementation of "Privacy by Default." This ensures that privacy is not an option children or parents must actively seek out, navigate, or understand complex settings to achieve, but rather an inherent, automatic protection embedded in every digital service they encounter.

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. 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 controls ensure responsible data handling.

By adopting these foundational principles rigorously, the OAIC 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.

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

Table 1: Key Differences: Privacy by Design vs. Privacy by Default (for Children's Privacy)

This table is crucial for clarifying the nuanced but critical distinction between "Privacy by Design" and "Privacy by Default," concepts that are often conflated. For a regulatory body like the OAIC, precision in terminology and scope is vital for effective policy implementation.

By visually contrasting their core characteristics, the table demonstrates why, for children, the specific *automaticity* and *highest protection* offered by Privacy by Default is paramount, even if Privacy by Design is the broader guiding philosophy. It directly addresses the need to explain why "Privacy by Design" alone renders unsatisfactory outcomes by highlighting where its broader scope might fall short without the explicit mandate of Privacy by Default.

Feature/Aspect	Privacy by Design (PbD)	Privacy by Default (PbD)
Definition/Scope	A holistic framework encompassing seven foundational principles for embedding privacy throughout the entire system lifecycle.	A specific application of Privacy by Design's second principle, ensuring the highest privacy settings are automatically applied throughout the information lifecycle..
Primary Focus	Proactive integration of privacy safeguards into system architecture, organizational priorities, and business practices from the outset.	Ensuring privacy is the *default state* of any system, product, or service, requiring minimal to no user action to protect personal information.
User Action Required	May still require user interaction for certain choices or to achieve maximum privacy if not fully implemented as a default. Aims to minimize, but doesn't eliminate, user burden.	Requires minimal to no user action for privacy protection. Users must *opt-in* to less private settings, rather than opt-out.
Risk for Children (if not strictly applied)	Can allow "balancing" that compromises privacy for functionality or commercial interests; relies on children's understanding and active choice, which is often limited.	Mitigates risks stemming from children's evolving capacities, limited digital literacy, and susceptibility to manipulative design ("dark patterns") by pre-setting protections.

Examples of Implementation	Implementing encryption protocols, pseudonymisation, or data minimization *as a design goal*.	Geolocation services turned off by default, children's personal data not visible to other users by default, parental consent as the default "no collection" for young children.
Relationship	A broader philosophical and operational framework that sets the stage for privacy-protective systems. It *encompasses* Privacy by Default as one of its core principles.	A critical, non-negotiable subset of Privacy by Design, particularly vital for vulnerable users like children, as it operationalizes the highest level of protection without user intervention.

Table 2: International Regulatory Examples of Privacy by Default for Children

This table provides concrete evidence of how leading jurisdictions are already implementing Privacy by Default principles for children, lending significant weight to EFA's recommendations. It demonstrates that these are not novel or theoretical concepts but established best practices that Australia can and should adopt. Furthermore, it highlights the global trend towards stronger child online privacy regulations, reinforcing the imperative for Australia to align with these international standards.

Regulation/ Framework	**Jurisdiction**	**Age Cap**	**Key Privacy by Default Mechanism (s)**	**Impact/Outcome**
UK Age Appropriate Design Code (Children's Code)	United Kingdom	Under 18	Mandates highest privacy settings by default; data minimisation; geolocation off by default; prohibits nudging towards lower privacy; private accounts by default.	Led to major tech companies adjusting defaults, e.g., Instagram private accounts for under-18s, Google SafeSearch default, YouTube autoplay off.

COPPA (Children's Online Privacy Protection Act)	United States	Under 13	Requires verifiable parental consent *before* collecting personal information; limited exceptions; data minimisation; retention limits; persistent identifiers for internal operations *only* (excluding behavioral advertising).	Ensures parents have control over data collection from children; establishes a privacy-by-default environment for young users online.
GDPR-K (General Data Protection Regulation - Children)	European Union (and Member States)	Under 16 (can be lowered to 13 by individual MS)	Mandates verifiable parental/guardian consent for children below the age of consent; requires child-friendly privacy notices; emphasizes data minimisation.	Provides comprehensive protection for children's data, applying to both online and offline processing; underscores children's unique vulnerabilities.

END

[redacted]

Electronic Frontiers Australia Inc
27 July 2025