Privacy as prevention: children's online privacy in the age of advanced technologies and rising sexual violence in Australia

Submission to the Office of the Australian Information Commissioner regarding the Exposure Draft of the Privacy (Children's Online Privacy) Code 2026

5 June 2026

TEACH US
* CONSENT

“I’m a 15-year-old schoolgirl and like most teenagers I spend a fair portion of my spare time on social media, often scrolling through short-form videos on apps such as Instagram or TikTok. All of my friends use those apps, and many spend **multiple hours a day** on them. I actively try to avoid online misogyny, but I am met with it incessantly whenever I open my mainstream social media apps. It only takes a **few minutes before there’s subtle or overt misogyny**, such as comment sections on a girl’s post filled with remarks about her body, videos made by men or boys captioned with a degrading joke, and even topics such as **domestic violence or rape, trivialised and laughed about**."

- Anonymous 15 year-old Australian girl, The Guardian, 2026

Table of Contents

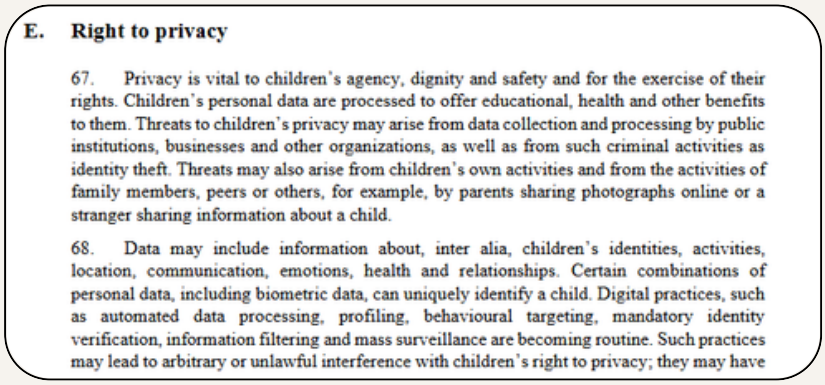
Introduction

1. Teach Us Consent Global Limited (Teach Us Consent) welcomes the opportunity to make a submission to the Office of the Australian Information Commissioner (OAIC) regarding the exposure draft of the Privacy (Children's Online Privacy) Code 2026.
2. The Code represents a significant and overdue step in protecting children's rights and privacy in digital environments. Teach Us Consent supports the intent of the Draft Bill and finds many of its substantive provisions crucial for advancing children's safety online. The submission particularly focuses on the Code's consent framework, the gap in protections relating to algorithmic profiling and recommender systems, the 'best interests of the child' framework standard, and questions of scope and enforcement.
3. Teach Us Consent's submission is informed by our direct work with young people, our Fix Our Feeds campaign calling for affirmative and informed consent to algorithmic feeds, and our long-term advocacy at the intersection of digital safety, young people's rights, and gender-based violence prevention.

About Teach Us Consent

4. Teach Us Consent Global Limited is a youth-led, registered Australian charity committed to eradicating normalised sexual violence through culturally relevant digital education assets for young people and through our advocacy work.
5. Established in 2021, our organisation launched a petition calling for more holistic and age-appropriate consent education in Australia, alongside a platform for people to share anonymous testimonies of sexual assault. After gathering over almost 7,000 testimonies, consent education was mandated in the national curriculum.
6. This came at a time where most Australians understood consent in theory but were yet to understand how to apply consent in practice (A. James, L. Moor & A. Waling, 2024). Research from that period revealed widespread "confusion" about what consent actually means (ANROWS, 2019) and this sentiment was reflected in the thousands of testimonies from victim-survivors across the country about their experiences. Together, these accounts painted a harrowing picture of a culture in which sexual violence had become deeply normalised.
7. The movement shone a light on a critical gap in our nation's prevention efforts: the curriculum. That proposed change was embraced by every state and territory, quickly becoming a national requirement for all students, from years K-10. Students across Australia are now receiving the consent education their parents likely never had.
8. Our organisation's expertise in consent - spanning its principles, practical application, and the consequences of its absence - directly informs our engagement with the Draft Bill. We bring to this submission a consent-specific lens and an awareness of the real-world harms which take place when young people are denied meaningful control over what happens to them, online or elsewhere.

Young peoples' right to online privacy



E. Right to privacy

67. Privacy is vital to children's agency, dignity and safety and for the exercise of their rights. Children's personal data are processed to offer educational, health and other benefits to them. Threats to children's privacy may arise from data collection and processing by public institutions, businesses and other organizations, as well as from such criminal activities as identity theft. Threats may also arise from children's own activities and from the activities of family members, peers or others, for example, by parents sharing photographs online or a stranger sharing information about a child.

68. Data may include information about, inter alia, children's identities, activities, location, communication, emotions, health and relationships. Certain combinations of personal data, including biometric data, can uniquely identify a child. Digital practices, such as automated data processing, profiling, behavioural targeting, mandatory identity verification, information filtering and mass surveillance are becoming routine. Such practices may lead to arbitrary or unlawful interference with children's right to privacy; they may have

General comment No. 25 (2021) on children's rights in relation to the digital environment

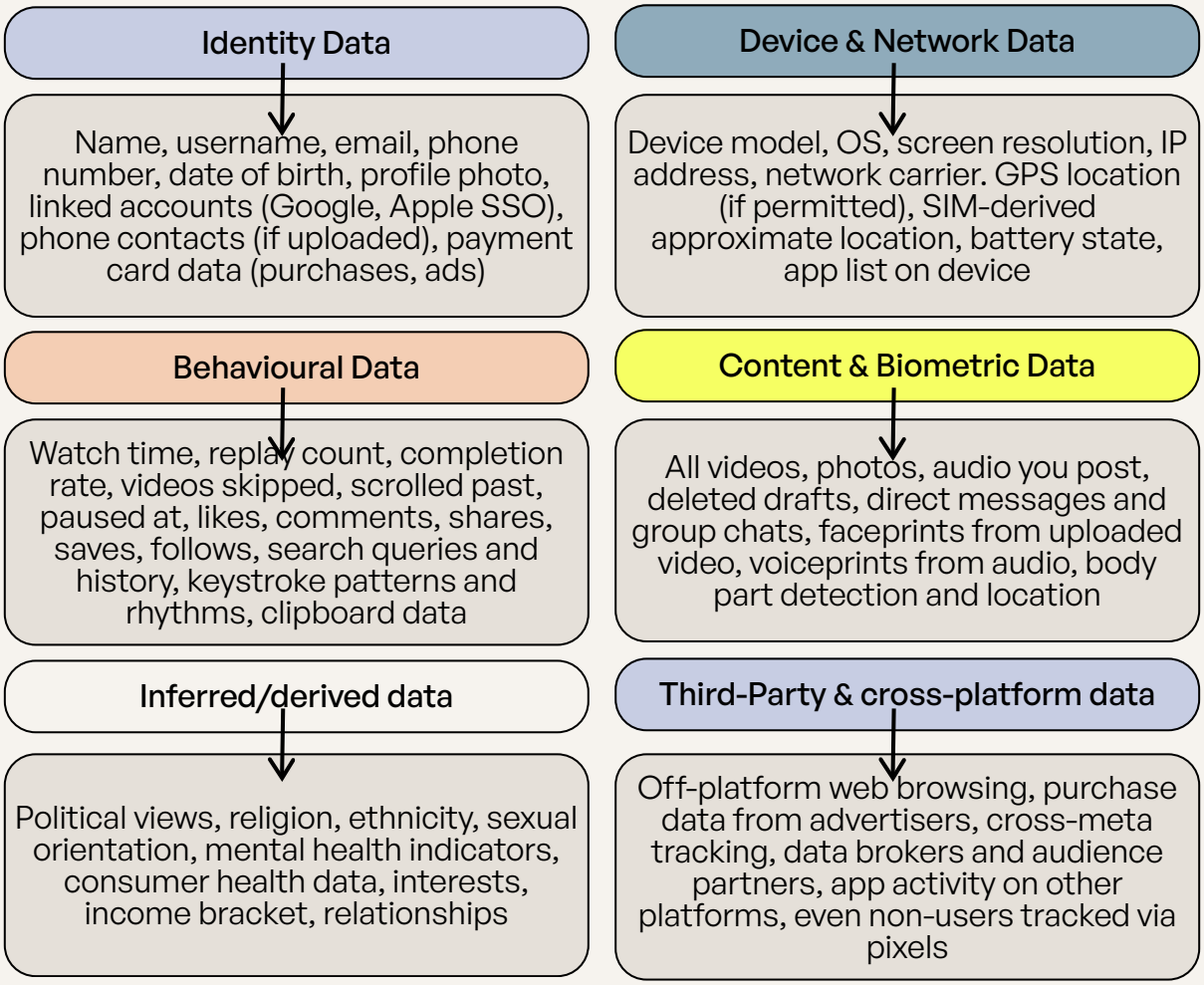
9. All children have the right to privacy, as outlined in Article 16 of the United Nations (UN) Convention on the Rights of the Child (UNCRC).
10. It is essential that this right is reflected in domestic legislation and enforced to prevent harm, including on social media - our organisation's primary concern as it relates to this Draft Bill.
11. The United Nations Committee on the Rights of the Child stated in 2021 that "certain combinations of personal data, including biometric data, can uniquely identify a child. Digital practices, such as automated data processing, profiling, behavioural targeting, mandatory identity verification, information filtering and mass surveillance is becoming routine. Such practices may lead to arbitrary or unlawful interference with children's right to privacy".
12. Emerging technologies have essentially normalised these practices - especially on social media. Thus, children's privacy laws in Australia are not suited for the digital age. Specifically, they don't reflect the immense amount of data social media companies retrieve from people, nor how they use that data to power personalised feeds through algorithmic recommender systems. This is creating harm for young people.

Young people on social media

13. Children and young people remain among the most active, and most vulnerable, users of digital services in Australia. Prior to Australia's social media delay implemented in late 2025, 96% of children aged 10 to 15 had used social media, and the majority used communication platforms to message, call or video call others (eSafety Commissioner, 2024).
14. Around 1.3 million children aged between 8 and 12 were estimated to have been using social media in 2024, with YouTube, TikTok and Snapchat among the most popular platforms (eSafety Commissioner, 2024).
15. Since the implementation of the social media delay, while platforms deactivated up to 4.5 million social media accounts (eSafety, 2026) across platforms, at least 20% of teenagers aged 13-15 years-old still use social media (Qustodio, 2026).

16. The Privacy Act Review 2023 recognised that children are increasingly reliant on online platforms, social media, mobile applications and internet-connected devices, and that these online services regularly collect and use large volumes of personal information about children, leading to growing community concern about the extent to which children are being 'datafied' (OAIC, 2026).
17. This 'datafication' is the product of deliberate design choices that treat children's attention and emotional states as commercial assets (OAIC, 2026). The OAIC's consultation found that children want greater transparency, stronger protections, and information designed for them. Their voices should shape the final form of this Bill.
18. This is why Teach Us Consent is particularly concerned with the role of algorithmic recommender systems in shaping what children believe.

The data social media companies collect from us



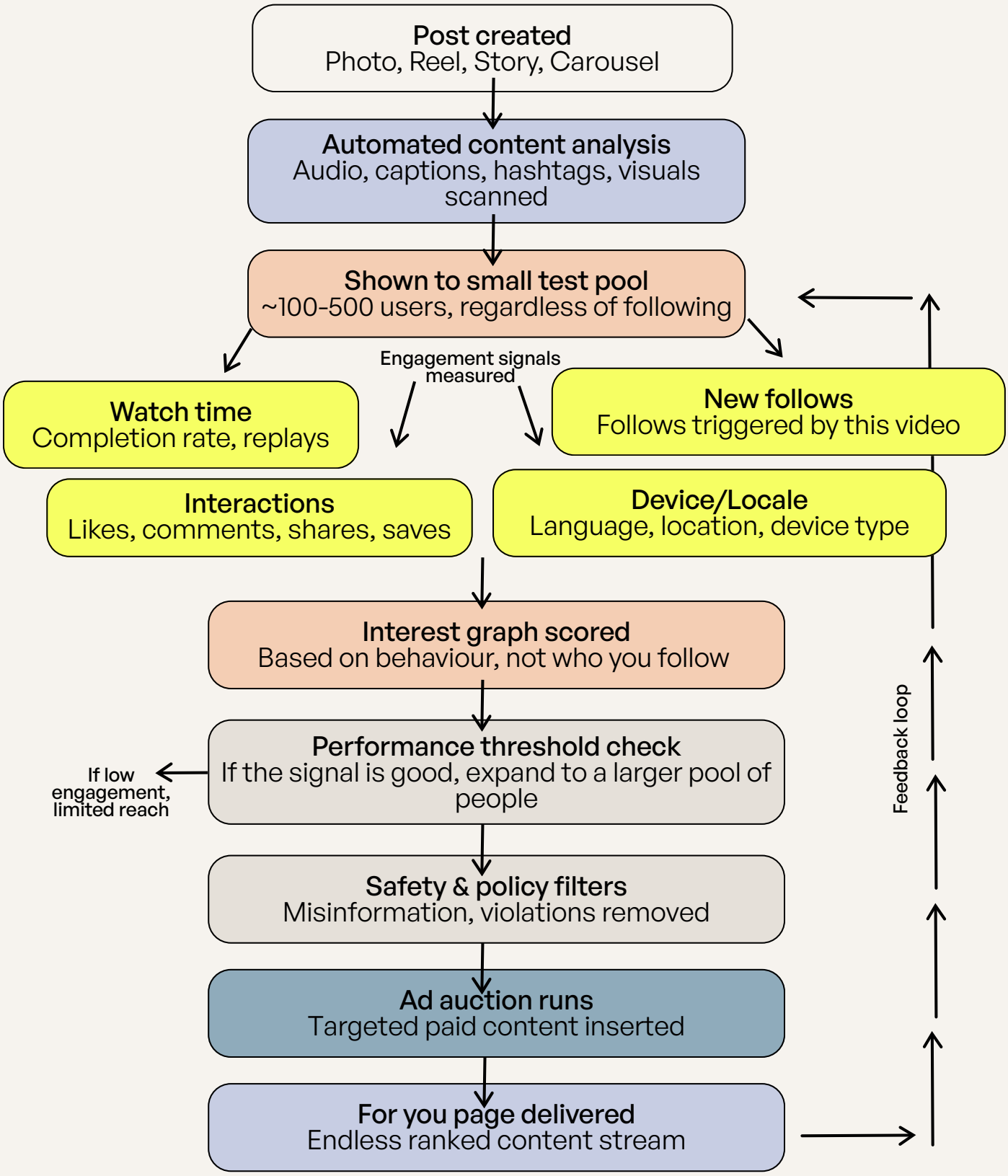
Note: this information collection does not specifically relate to every single social media platform, but broadly reflects the data collected across Facebook, Instagram, TikTok, WhatsApp and other mainstream platforms.

19. Social media platforms use our personal data to serve recommended content that optimises time spent on the platform to view advertisements and ultimately bolster their billions in revenue. This means that algorithms often prioritise content that provokes the strongest emotional reactions; outrage, validation, fear, arousal and anger drive 'successful' posts. In turn, our feeds have become fertile ground for extreme content.
20. The use of algorithms also extends to comments; the comment section of a post on most popular social media platforms is most likely to reflect those comments which are inflammatory or those comments which we agree with at the top, to encourage us to interact with these comments (liking, responding, etc) and further boost engagement.
21. Importantly, this structure incentivises users to create and disseminate content that evokes intense emotional reactions. Notably, this is even moreso incentivised in jurisdictions where payment structures for 'successful' posts, such as the TikTok Creator Fund, are permitted, such as the United States.

Fix Our Feeds

22. Teach Us Consent acknowledges that the landscape young people are growing up in has shifted. Consent education remains as vital as ever. Yet, these education efforts are being actively undermined by the predatory social media algorithms that repeatedly target young people with harmful content, including that which promotes misogyny. This is, in part, possible due to the lack of privacy restrictions preventing social media companies from retrieving data from users and using that data to target users with content.
23. In 2025, Teach Us Consent launched the Fix Our Feeds campaign, calling on the Australian Government to require social media platforms to offer an opt-in model for algorithmic feeds, bringing the principle of affirmative and informed consent to young people's online experiences. The campaign has attracted broad cross-sector support, including from public health experts, gender-based violence experts, men's mental health advocates and organisations, and young people.
24. Research underlying the Fix Our Feeds campaign shows that, based on the data platforms source from us, social media accounts mimicking a 16 to 18-year-old boy can be fed extreme misogynistic content within 23 minutes of account creation. Such outcomes are the predictable product of systems engineered to provoke emotional reactions without meaningful consent from the young people exposed to them.
25. This is creating real harm. Attitudes common in the "manosphere" - like undermining women's independence and the excuse of men's violence - are linked with support for violence against women (Nicholas et al., 2024). Research consistently links sustained exposure to misogynistic content with attitudes supportive of violence against women (Nater, C., Felber, L., Lüke, R.). The content algorithmically fed to children shapes how they understand themselves and others (Seberger, Razi et al.).
26. This Draft Bill reflects the intent of the Fix Our Feeds campaign and offers an opt-in feature for children. We strongly support this use of privacy legislation as a way to prevent harm and urge the Government to extend this protection to adults.

Attachment A: A visual interpretation of an algorithm



Algorithmic recommender systems are rarely made available to the public. This visual interpretation does not claim to be entirely accurate, and is based upon the information we know from the TikTok Newsroom (2020) and public experience/commentary.

Analysis | Interest graph | Signals | Filters | Ads

Best interests of the child

27. Teach Us Consent strongly supports the introduction of the 'best interests of the child' (BIC) standard as a governing principle for the collection, use, and disclosure of children's personal information under Sections 10 and 11 of the Code. Indeed, our organisation supports the definition guiding this understanding of ‘best interest’, based on Article 3 of the United Nations Convention on the Rights of the Child (UNCRC).
28. The Explanatory Statement sets out the factors entities must consider when assessing BIC compliance, including mental, physical and developmental impacts on the child; the child's ability to develop and express their identity; and whether particular groups may be disproportionately affected, including First Nations children, children from culturally and linguistically diverse backgrounds, and children with disabilities. Teach Us Consent strongly supports this intersectional approach and urges it be retained in the final Code.
29. Section 9 of the Draft Bill states that “a child should be able to turn on or off additional elements such as personalised content, targeted advertising or recommendations that rely on the handling of a child’s personal information”. The Section clearly addresses that the default setting for social media would be to ensure a de-personalised feed, rid of advertising or recommendations that rely on the handling of a child’s personal information. Teach Us Consent strongly supports this detail of the draft legislation, and reflects a strong safety-by-design feature that is world-leading. We urge the Federal Government to consider this measure as it relates to adults over 18 years of age, and implement a de-personalised default setting on social media platforms.
30. Teach Us Consent notes that the BIC obligation is qualified through using the phrase "reasonably consistent" - a standard that risks introducing a balancing test between commercial interests and children's welfare rather than establishing a clear floor. We urge the OAIC to clarify that "reasonably consistent with the best interests of the child" means that entities must be able to demonstrate a genuine BIC assessment was conducted and that children's interests were treated as the primary consideration.

Division 2 - Consent

31. Consent is the foundation of Teach Us Consent's work, building on the principle that meaningful consent must be freely given, informed, specific, current and withdrawable at any moment. We find it significant that Division 2 of the Code establishes these elements as the standards for consent to children's data collection and urge the Government to proceed with this section in full.
32. Several provisions are deserving of specific recognition - the prohibition on bundled consent requests (s 14(3)(b)); nudge techniques (s 21); the requirement that consent be unambiguous (s 19); the 12-month expiry on consent (s 15(4)); the withdrawal mechanism (s 17). These provisions allow consent to be genuinely given, and reflect the understanding that true consent must be communicated clearly, and not assumed at any given point in time.
33. Teach Us Consent further supports the assent mechanism for children under 15 (s 20) and sees it as an appropriate provision. However, "age appropriate" as defined in Section 4 of the Code is narrower than it first appears. Where a service does not target a specific age range, the default standard is information appropriate for a child aged 10–12. This creates a lowest common denominator problem - consent notices designed for a 10-year-old are unlikely to be meaningful for a 17-year-old, and vice versa. The definition applies only to the presentation of information and notices, not to the design of consent mechanisms themselves. There is no requirement that consent mechanisms be tested with actual children to verify they are genuinely understood. Teach Us Consent urges the OAIC to broaden the definition of "age appropriate" to encompass the design of consent mechanisms, and to require that those mechanisms be tested with children across different age groups before the Code commences.
34. Our organisation believes three additional areas of the consent framework require further attention.
35. First, the requirement that entities should take "reasonable steps" to verify parental responsibility (s 13(2)) is undefined. The Explanatory Statement offers examples, including email communication, bank vouching, government digital ID, but sets no minimum standard. The OAIC should define a minimum standard for parental verification that is proportionate to the sensitivity of the data being collected.
36. Second, the exceptions to parental consent for children under 15 (s 13(4)) are potentially too narrow. Currently in the Draft Bill, a child under 15 may personally consent only when seeking legal or health-related support in connection with a person with parental responsibility. This does not account for circumstances where the person with parental responsibility is themselves the source of harm or actions conflict with their best interests - for example, in cases when a child is seeking support from a violence response service, a child safety organisation, or a mental health service in the context of abuse at home. Teach Us Consent notes the OAIC may consider broadening Section 13(4) to include any circumstance involving a person with parental responsibility that would not be in the child's best interests, consistent with the BIC standard that governs the rest of the Code.

37. Finally, several phrases in Division 2 require clarification. "Reasonable steps" in Section 13(2), "simple means" in Sections 17 and 29, and "accessible" across Division 2, are all undefined. While Teach Us Consent acknowledges that these terms may be intentionally broad, so as not to prescribe certain terms that may be dated by time or emerging technology, perhaps examples should be provided through secondary legislation to establish guidance on the minimum standards the OAIC expects.

Other sections of interest

38. Scope (s7): The Code applies to services "likely to be accessed by children" or "primarily concerned with the activities of children," but neither term is defined. The OAIC should provide explicit guidance on what "likely" means in practice before the Code is finalised, based on current access data.
39. The Code permits self-declaration of age as a "reasonable step" toward age assurance. The eSafety Commissioner's March 2026 compliance report has demonstrated that self-declaration is routinely circumvented under the Social Media Minimum Age scheme. For higher-risk services, self-declaration alone should be insufficient. The OAIC should establish a risk-based minimum standard for age assurance proportionate to the nature of data being collected.
40. Teach Us Consent also notes the tension this may create. Robust age verification requires collection of sensitive identity documents, introducing its own privacy risks. The Code cannot resolve this tension by leaving it entirely to entity discretion. Explicit guidance, which would balance verification rigour with data minimisation, should be explored.
41. Section 24: Notification of the collection of personal information: Our organisation supports that clear, concise, transparent, easily accessible and age-appropriate notifications of the collection of personal information is essential. We recommend that these notifications are explicitly different and easily distinguishable from existing push-notifications that platforms currently employ. This reflects the fact that notifications on social media are often naturally dismissed and unacknowledged, and that there should be an additional effort made by platforms to differentiate the notifications. This would help to ensure that the content is being genuinely engaged with by young people and consent is truly obtained.
42. Section 29: Opting out of direct marketing: Teach Us Consent strongly supports an opt-in direct marketing approach, as opposed to an opt-out approach, in order to accurately be consent-based. An opt-out process assumes that young people a) are aware of their ability to opt-out, b) understand the harms that direct marketing of certain content can bring and c) comprehend how direct marketing works, by optimising personal data.

43. In addition to requiring platforms to not use design practices to make it hard for a child to opt-out of direct marketing, we strongly urge the OAIC to explicitly ensure that platforms ensure that the marketing-free experience of their platforms is as functional as that of the marketing experience of their platforms. For example, they should not be permitted to implement 'dark patterns' that create a less intuitive, functional and enjoyable experience of marketing-free features. This is crucial to avoid instances of malicious compliance.
44. Algorithmic Profiling (s 28): Teach Us Consent supports the Section 28 provision in giving children the right to request information about automated decision-making, including profiling. However, meaningful algorithmic transparency requires more than acknowledgment that profiling exists. The OAIC should require entities to provide children with accessible, age-appropriate explanations of how recommendation systems use their data and what content they are being served as a result.
45. Division 3: Transparency: The Draft Bill explores the notion of transparency as it pertains to young people understanding privacy policies in a clear and accessible way, and transparency regarding the way in which tech platforms utilise data to curate their online experiences.
46. Our organisation notes the OAIC's intention to create a sense of transparency around privacy laws and the ways in which tech platforms use personal data. Teach Us Consent supports these efforts and acknowledges the importance of young people understanding better how technology utilises their data.
47. Teach Us Consent notes that, while this measure is worthwhile for the benefit of young people, tech platforms withhold a significant amount of information from the public, preventing genuine transparency from being achieved.
48. Due to the largely opaque operations of tech companies and their notoriously secretive algorithms, harms created by social media platforms in particular are seldom understood in full. Therefore, it should be noted to young people that the information currently available about harms created by social media platforms in particular, as a result of using users' personal data, is not publicly available. This would help to ensure true informed consent.
49. Ambiguous Language - A Systemic Issue: A pattern of qualified obligation runs throughout the Code. "Reasonable steps," "strictly necessary," "reasonably consistent," "simple means," "accessible," "age appropriate", and "likely to be accessed" each appear multiple times, collectively creating a framework where obligations are subject to platform discretion. Without a companion guidance instrument setting minimum standard for each term, the Code risks becoming a framework that sophisticated legal teams can navigate around. Teach Us Consent suggests that the OAIC publish clear, binding guidance on each of these thresholds before the Code commences.

50. Teach Us Consent supports the provision of the right to request destruction of personal information. We suggest that the OAIC additionally considers its application to sharenting (the widespread practice of parents documenting their children's lives online, often from birth, without the child's knowledge or consent) (Avci H., Baams L., Kretschmer T.). The Code's current drafting does not explicitly address this scenario, and guidance clarifying that the destruction right extends to data collected and published by parents would be a meaningful protection and addition.

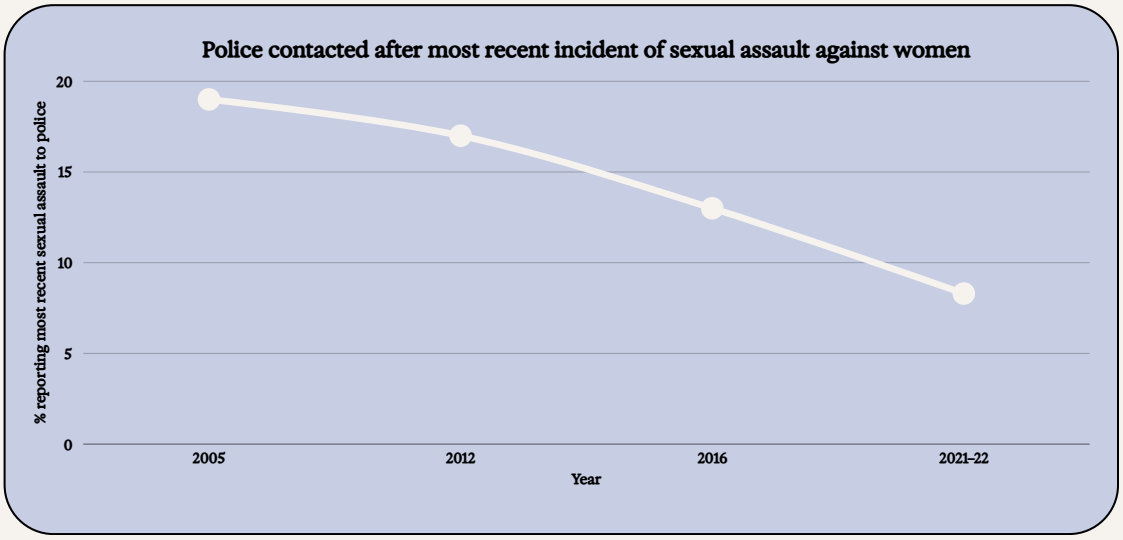
Conclusion

51. The Privacy (Children's Online Privacy) Code 2026 is a meaningful effort to protect children in digital environments, and Teach Us Consent supports its intent and the vast majority of it’s detail.
52. The consent framework in particular reflects principles our organisation has long championed, and we commend the OAIC for centering them here.
53. A Code is only as meaningful as its enforcement, and its definitions. Without explicit guidance on binding minimum standards for ambiguous obligations, and a credible enforcement commitment, the protections in this Code will become aspirational rather than operative.
54. Young people are rights-holders who deserve the same standard of meaningful, affirmative consent online that we ask of every other domain of their lives. This Code can deliver that, but only if it is resourced and enforced with the seriousness the stakes demand.

Attachment B: The State of Sexual Violence in Australia

Sexual violence across the country is rising (ABS, 2025), while reports of sexual assault made to police are falling (AIHW, 2026).

The rate of police reports of sexual assault are falling, from 13% to 8.3% in the 5 years between 2016 and 2021, according to the Australian Bureau of Statistics Personal Safety Survey.



The nature of perpetration is also changing: the latest Australian Child Maltreatment Study (ACMS, 2024) reports that, while sexual abuse perpetrated by adults against adolescents is decreasing, child sexual abuse perpetrated by adolescents against other adolescents is increasing.

Through this submission, Teach Us Consent aims to demonstrate how stronger privacy laws could prevent this devastating rise in sexual violence from continuing.

Attachment C: Fix Our Feeds: a campaign to allow users to turn our algorithms off and on at will.

In December 2025, Teach Us Consent launched a campaign to address the harms social media algorithms are causing - Fix Our Feeds. It calls on the Federal Government to introduce a world-first reform: an "opt-in" feature for algorithms on social media platforms. The campaign comes at a crucial point in time when the Albanese Government is reviewing the Online Safety Act (2021) (OSA) and crafting a new Digital Duty of Care (DDOC).

The purpose of this policy is to directly target the algorithmic recommender systems that are responsible for the mass and predatory dissemination of content that creates harm.

Key features of opt-in algorithms would include:

- This policy is content-neutral in that it doesn't seek to remove content. Rather, it acknowledges that, while online content can be innately harmful, it is the recommender systems themselves, powered by algorithms, that create the pathways for radicalisation, among other harms.
- Preferences would be fixed until intentionally changed by the user. An opt-in feature would allow users to change their preference at any point and across platforms. We propose users should be able to turn their algorithms on and off at will, and that this preference should be fixed until users change them.
- An opt-in feature is based on the principles of consent. An opt-in algorithm would provide people who use social media with greater autonomy over how they consume content. In practice, 'opting-in' to an algorithm would require the platforms to ask for informed and affirmative consent to use our behavioural data to inform algorithms and shape the content we see. For the first time, we would be offered a genuine choice between content curated by social media platforms based on algorithms, or content from accounts they follow only and without recommender content.

References

Amnesty International UK. (2025, March 21). Toxic tech: New polling exposes widespread online misogyny driving Gen Z away from social media. https://www.amnesty.org.uk/latest/toxic-tech-new-polling-exposes-widespread-online-misogyny-driving-gen-z-away-social/

Avci, H., Baams, L., & Kretschmer, T. (2024). A systematic review of social media use and adolescent identity development. Adolescent Research Review, 10, 219–236. https://doi.org/10.1007/s40894-024-00251-1

Birkett, S., & Kwee, C. (2026, April 2). Australia: Exposure draft of Children's Online Privacy Code signals tougher standards. Privacy Matters (DLA Piper). https://privacymatters.dlapiper.com/2026/04/australia-exposure-draft-of-childrens-online-privacy-code-signals-tougher-standards/

Burton, M., Minihan, S., Nicholas, M., Connor, J., & Trengove, K. (2025, April 28). Regulating image-based abuse: An examination of Australia's reporting and removal scheme. Journal of Online Trust and Safety, 2(5). https://doi.org/10.54501/jots.v2i5.222

Corrs Chambers Westgarth. (2026, April 9). OAIC's Children's Online Privacy exposure draft: From consultation to code. https://www.corrs.com.au/insights/oaics-childrens-online-privacy-exposure-draft-from-consultation-to-code

eSafety Commissioner. (2026, March). Social media minimum age: Compliance update. https://www.esafety.gov.au/sites/default/files/2026-03/SocialMediaMinimumAgeComplianceUpdateMarch2026.pdf

5Rights Foundation. (n.d.). Submission: Privacy in the digital age. Office of the UN High Commissioner for Human Rights. https://www.ohchr.org/sites/default/files/documents/cfi-subm/privacy-digital-age/subm-privacy-digital-age-cso-3-5rights-foundation.pdf

Human Rights Watch. (2024, September 11). Australia commits to protecting children's privacy online. https://www.hrw.org/news/2024/09/12/australia-commits-protecting-childrens-privacy-online

McEleny, C. (2026, May 13). "By the time a child turns 13, there are 72 million pieces of data on them": Dan Richardson on Australia's Children's Online Privacy Code. ExchangeWire. https://www.exchangewire.com/blog/2026/05/13/by-the-time-a-child-turns-13-there-are-72-million-pieces-of-data-on-them-dan-richardson-on-australias-childrens-online-privacy-code/

References

Nater, C., Felber, L., Lüke, R., Eagly, A. H., Greitemeyer, T., Miller, D. I., & Dorrough, A. R. (2026). Misogynous messages in the media increase hostility to women: Evidence from a meta-analysis of 257 experimental and nonexperimental studies. Psychological Bulletin, 152(1), 1–32. https://doi.org/10.1037/bul0000513

Office of the Australian Information Commissioner. (2026). Draft explanatory statement: Exposure draft, Children's Online Privacy Code. https://www.oaic.gov.au/__data/assets/pdf_file/0019/262630/Draft-Explanatory-Statement-Exposure-Draft-Childrens-Online-Privacy-Code.pdf

Office of the Australian Information Commissioner. (2026, March 31). Exposure draft: Privacy (Children's Online Privacy) Code 2026. https://www.oaic.gov.au/__data/assets/pdf_file/0020/262631/Exposure-Draft-Childrens-Online-Privacy-Code.pdf

Office of the Australian Information Commissioner. (2026). Children's Online Privacy Code. https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes/childrens-online-privacy-code

Office of the Australian Information Commissioner. (2026). Draft Children's Online Privacy Code (consultation for industry, civil society, academia). https://www.oaic.gov.au/engage-with-us/consultations/draft-childrens-online-privacy-code-consultation-for-industry,-civil-society,-academia

Rountree, D., Guyot, I., Smith, G., Bloch, V., Coote, W., & Griffith, R. (2026, April 9). Draft Children’s Online Privacy Code: Proposed protections for children's privacy online to have material impact. Allens. https://www.allens.com.au/insights-news/insights/2026/04/draft-childrens-online-privacy-code-proposed-protections-to-have-material-impact-on-online-services/

The Project. (n.d.). Today's children have had their lives documented online by their parents [Video]. Facebook. https://www.facebook.com/TheProjectTV/videos/999738045663730

Swan D. (2026, March 31). Roblox, Youtube caught in major children’s privacy overhaul. The Sydney Morning Herald. https://www.smh.com.au/technology/roblox-youtube-caught-in-major-children-s-privacy-overhaul-20260330-p5zjta.html