Reset·Tech
AUSTRALIA

Response to the OAIC's *Children's Online Privacy Code Issues Paper*

Reset.Tech Australia
July 2025

Summary

Reset.Tech Australia welcomes the opportunity to respond to the OAIC's *Children's Online Privacy Code Issues Paper.* This submission focuses on:

- **The scope of the services covered (question set 1).** The initial list of Social Media Services, Designated Internet Services and Relevant Electronic Services is a strong start, and we recommend inclusion of EdTech products and AdTech (Online data brokering services, including the Real-Time Bidding system). Children's rights are best advanced by wide coverage of the COPC, and all additional coverage is welcome.

- **When and how the COPC should apply to APP entities (question set 2).** If the aim of the COPC is to enhance privacy, this requires maximising coverage which generally favours lowering thresholds for inclusion. The merits of a formulation for a likely to be accessed standard consisting of two conditions is outlined, using the UK and Irish experience. Here, platforms would be considered likely to be accessed where they are:

    1. *Likely to be accessed because they are directed to or intended for children, or*
    2. *Likely to be accessed by children as demonstrated by either:*
        a. *Evidence that children's use of the service is more than de minimis or;*
        b. *It is the type of service that is likely to attract children*

    We do not believe there was intended to be a high-bar for significance test and note that the 'Likely to be accessed' standard in the UK does not include a significance test based on the number of child users alone. We do not believe that additional age gating or access controls are necessary to meet the requirements of the COPC, nor for this formulation of the 'Likely to be accessed' standard.

- **APP 1 – steps platforms should take to ensure children can easily make privacy-related inquiries or complaints (question 4.4).** Consulting with experts who run advice and help lines for children, and young people themselves, we have developed a list of requirements for platforms regarding their inquiry and complaints systems, that the COPC code could codify. These include:

    - Requirements to provide clear, plain language information about children's privacy rights
    - Requirements to offer a range of accessible and flexible avenues for complaints and inquiries
    - Requirements about what responses to child inquiries or complaints should look like, especially with regards to timeframes, avenues for response and language requirements.
    - Requirements for the right to review decisions
    - Requirements to inform children about appropriate external support and advocacy services
    - Requirements to comply with all relevant federal Child Safe Standards
    - Requirements to presume complaints and inquiries from children are valid
    - Requirements to allow advocacy for individual children's complaints and super-complaints
    - Requirements for regular transparency reports
    - Requirements to offer remedies that are meaningful to the child

- **Two outcomes we would like to see the COPC deliver for children;**

    - **Securing the right for children to delete their data.** The COPC would be well placed to ensure children have the right to data erasure. Multiple jurisdictions have introduced the right to delete for children (and adults) and the technical mechanisms to enable this have been widely created by many of the platforms covered by the COPC.

- **A presumption against the collection, use and disclosure of children's data for targeted advertising.** The COPC would be well placed to prohibit or presume against this practice on privacy grounds. Targeted advertising is a violation of children's right to privacy because of the data handling process it involves. Multiple jurisdictions have also presumed against the practice in comparable children's data codes and protections, including the UK, Ireland and the EU.

Contents

About Reset.Tech Australia & this submission

We welcome the opportunity to respond to the OAIC *Children's Online Privacy Code Issues Paper*. Reset.Tech Australia is an Australian policy development and research organisation. We specialise in independent and original research into the social impacts of technology, including social media. We are the Australian affiliate of Reset.Tech, a global initiative working to counter digital harms and threats.

Reset.Tech Australia has been advocating, alongside a number of children's organisations,[1] for the introduction of a Children's Online Privacy Code ('COPC') since 2020 and we are delighted to see the progress of the COPD to date. We are deeply supportive of this policy agenda and welcome the complex and nuanced debate that the OAIC is fostering with this issue paper. The paper outlines critically important issues for consideration, and we are heartened to see these discussed and consulted on in advance of the draft COPC.

This submission focuses on the scope and application of the COPC (question sets 1 & 2), and the requirements for a child accessible inquiries and complaints process (question 4.4). It also outlines two outcomes we would like to see the COPC effect for children; a presumption against the collection, use and disclosure of children's data for targeted advertising and; securing the right to erasure for children.

Reset.Tech Australia has undertaken a dedicated, multi-year work program on privacy, with a special focus on children's privacy and collaborations across the children's sector. Our work on young people and privacy in Australia is generously supported by the Internet Society Foundation and the Jessie Street Trust. Our published research include:

- *Likely to be Accessed in the Children's Online Privacy Code*[2]
- *Targeted Advertising and the Children's Online Privacy Code*[3]
- *Consultation documents with children and young people, and child rights experts*[4]
- *The APPs x Children's Rights*[5]
- *Best Interests and Targeting: Implementing the Privacy Act Review to advance children's rights*[6]
- *Australians for Sale: Targeted Advertising, Data Brokering and Consumer Manipulation*[7]
- *Realising young people's rights in the digital environment*[8]
- *Capacity of the consent model online*[9]

[1]Reset.Tech Australia 2025 *Children's Privacy Code* https://www.childrensprivacycode.org.au/
[2]Reset.Tech Australia 2025 *Likely to be Accessed in the Children's Online Privacy Code* see https://au.reset.tech/work for publication in late early August 2025
[3]Reset.Tech Australia 2025 *Targeted Advertising and the Children's Online Privacy Code* https://au.reset.tech/news/targeted-advertising-the-children-s-online-privacy-code/
[4]Reset.Tech Australia 2025 *Children's Online Privacy Code* https://au.reset.tech/news/children-s-online-privacy-code/
[5]Reset.Tech Australia 2025 *Briefing Paper on the APPs & Children's Rights* https://au.reset.tech/news/children-s-online-privacy-code/
[6]Reset.Tech Australia 2024 *Best Interests and Targeting* https://au.reset.tech/news/best-interests-and-targeting-implementing-the-privacy-act-review-to-advance-children-s-rights/
[7]Reset.Tech Australia 2023 *Australians for Sale* https://au.reset.tech/news/coming-soon-australians-for-sale-report/
[8]Reset.Tech Australia 2023 *Realising young people's rights in the digital environment* https://au.reset.tech/news/report-realising-young-people-s-rights-in-the-digital-environment/
[9]Reset.Tech Australia 2023 *Capacity of the consent model online* https://au.reset.tech/news/capacity-of-the-consent-model-online/

Questions outlined in the issues paper

Question 1: Scope of services covered by the Code

1.1 Are there additional APP entities, or a class of entities, that should be covered by the Code? Please provide reasons or evidence to support your view.

It is in children's best interests to have a digital world where privacy protections are widespread and safeguards follow them across the full range of online products and services they use. We note that the approach taken in the COPC — deriving from the *Privacy and Other Legislation Amendment Act 2024* — limits the coverage of the COPC to Social Media Services, Relevant Electronic Services and Designated Internet Services, but we feel that this is a good start reflecting some of the most privacy-risky services used by young people.

However, all additional coverage is welcome, and ideally all entities regulated by the *Privacy Act*, where they are Likely to be accessed should also comply with the Code. Noting that this might be a stretch goal, in the interim we would also like to see the COPC extend coverage to apply to two additional classes of entities, EdTech products and AdTech (or online data brokers and their services). We note there is also a strong rationale for the inclusion of IoT devices and 'wearables', but these are outside our scope of expertise.

EdTech

There are four reasons we believe EdTech products could be considered for inclusion:

1. Children are the main category of users for these products, making their inclusion coherent. Tertiary focussed applications aside, the vast majority of EdTech products are explicitly directed at and intended for school students who are predominantly under the age of 18. (And tertiary apps would be unlikely to pass the 'Likely to be accessed' standard).
2. Reliance on alternative models of 'notice and consent' to protect privacy is wholly inappropriate, making regulatory protection an appropriate measure. Firstly, the use of EdTech is often 'functionally compulsory', because children (and parents) are unable to meaningfully decline to use these products without significant consequences for their education, if they are able to decline at all. This means they cannot choose to avoid privacy intrusive products. Secondly, schools are often ill equipped to understand the privacy risks of these products, being notoriously overburdened and sometimes underfunded. Despite this, the use of EdTech products often falls to individual schools to decide.
3. Evidence suggests they are often high risk products from a privacy perspective. Research around five EdTech products recommended in Victoria[10] found extensive evidence of unnecessary and risky privacy violations built into their services, such as third party advertising trackers and tracking pixels, GPS location tracking and identifiable data enabling commercial profiling (See Appendix 1 for more details).
4. It would meet community expectations. There is widespread public support for the inclusion of EdTech products as an additional class of entities. In a poll of 1,500 Australian adults, conducted by YouGov in July 2025, 83% outlined that they would 'strongly support' or 'support' the inclusion of EdTech within the COPC (See Figure 1).

[10]Han Hye Jung 2022 *How Dare They Peep into My Private Life?* https://www.hrw.org/sites/default/files/media_2022/10/HRW_20220711_Students%20Not%20Products%20Report%20Final-IV-%20Inside%20Pages%20and%20Cover.pdf

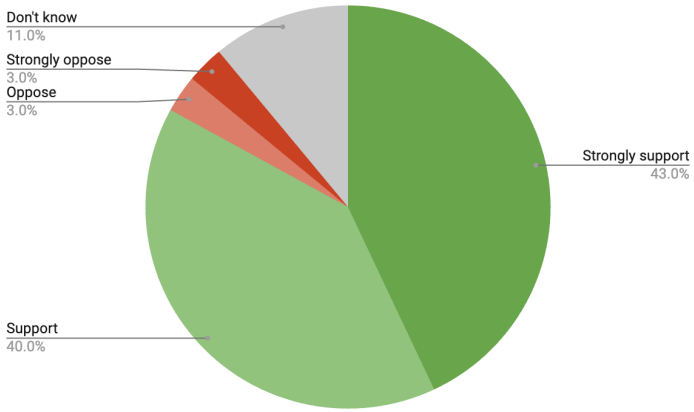


Figure 1: Responses to the question 'The Privacy Commissioner is currently drafting a Children's Online Privacy Code to provide additional protections for children's (under 18 years old) data when they are online. They are currently looking at which digital products and services should be covered by the Code. Would you support this Code covering 'EdTech', or websites and apps made specifically for school children, so that they would also have to protect children's data more carefully? (n= 1,500)

AdTech

There are four reasons we believe AdTech (online data brokers — including and especially the systems that service the Real-Time Bidding [RTB] system) — could be considered for inclusion:

1. Online data brokers, and the RTB technologies that drive them, share extensive and excessive amounts of data about Australian children. For example, each Australian, including children, has their GPS location disclosed on average 449 time a data within the RTB system, and this location data is identifiably linked to information that infers age such as markers for those ages 0-17 and various permutations of this (e.g. two year age bands), users attending high school, users watching children's television, female children and male children. This can include data that could be inferred to be sensitive, such as data regarding health and medical needs, such as users who visit health care clinics, purchased pregnancy tests or condoms, or those with chronic health problems.[11] This would meet any 'likely to be accessed' criteria, as demonstrated by the significant number of children who are 'users' of this service by way of having their data processed.
2. Reliance on alternative models of 'notice and consent' to protect privacy is also wholly inappropriate in this situation. Data brokers, and their RTB system, are largely unknown to the public. For example, 55% of Australians are not aware at all about which data brokers may have their data.[12] While some of the data that ends up in AdTech is derived from online experiences where users may have "clicked" yes to accept, these consent mechanisms are not meaningful for children. Firstly, it is unclear if there is meaningful transparency about how much data will flow from apps, websites and cookies into these systems and how it will be re-disclosed, and

[11]Reset.Tech Australia 2024 *Australians for Sale* Reset.Tech Australia 2023 *Australians for Sale* https://au.reset.tech/news/coming-soon-australians-for-sale-report/

[12]Polling conducted with YouGov in July 2025, asking 'Thinking about your own data that might have been collected when you are online, and who it might have been collected by or shared with — do you know which data brokers might have data about you?'. It found that only 10% of Australian adults felt were aware of all *or* most of the data brokers may have their data, 20% felt they were aware of a few, and 55% felt they were not aware at all. 15% did not know (n= 1,500).

re-combined. Secondly, these consent mechanisms themselves are wholly inappropriate for children. Research shows they are excessively complex and long to the point of incomprehension to children, and that children and young people rarely meaningfully engage or read them.[13]

3. Evidence suggests they are often high risk products from a privacy perspective. The number of end-users within the RTB system is unknown meaning disclosures are 'unlimited'. Further, there appear to be little or no restrictions on the ways these unknown end-users can use the data. For example, there is evidence that companies are selling data about users — which would include teenagers — who have visited family planning clinics in the US or firms that sell information about users with national security connections. It is impossible to know what 'risky' uses of data happen with children's data once it is collected and disclosed within the RTB system.[14]
4. It would meet community expectations. There is widespread public support for the inclusion of data brokers and RTB products as an additional class of entities. In a poll of 1,500 Australian adults, conducted by YouGov in July 2025, 77% outlined that they would 'strongly support' or 'support' the inclusion of AdTech and online data brokers in the COPC (See Figure 2).

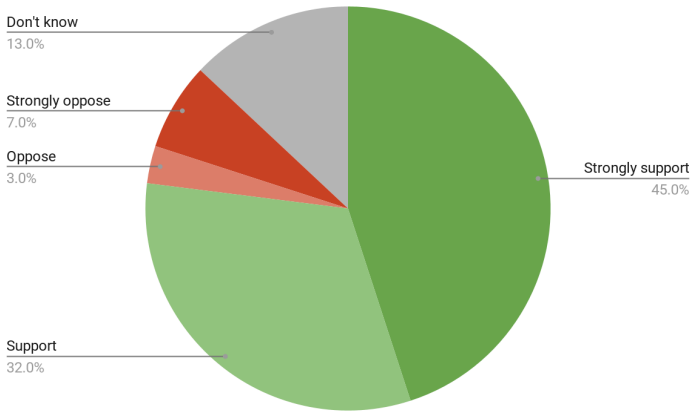


Figure 2: Responses to the question 'Data brokers are companies that gather personal information from many sources—such as websites you visit, mobile apps, loyalty programmes and public records—combine it into detailed profiles, and then sell or share those profiles with advertisers, insurers, credit agencies and other organisations. Would you support this Code covering online data brokers, and online systems that trade and share children's data largely for advertising purposes, so that they would also have to protect children's data more carefully? (n= 1,500)

1.2 Are there any APP entities, or a class of entities, that should be excluded from the Code's application? If so, on what basis?

We are aware that there is concern among generalist support providers, such as domestic violence charities that run an online help service, that the COPC might affect their offering their services. We do not believe the COPC would necessarily apply to them or negatively affect their offer, but would encourage the OIAC to make this clear to some key sector leads to address concerns.

[13]Reset.Tech Australia 2021 *Did We Really Consent To This?* https://au.reset.tech/news/did-we-really-consent-to-this-terms-and-conditions-young-people-s-data/

[14]See for example, Reset.Tech Australia 2024 *Any buyer accepted* https://au.reset.tech/news/any-buyer-accepted-unregulated-data-markets-create-personal-security-risks/, Irish Council on Civil Liberties 2024 *Australia's Hidden Security Crisis* https://www.iccl.ie/digital-data/australias-hidden-security-crisis/ and Brigid Kennedy 2022 'A controversial data firm is selling abortion clinic visitors' location data' *The Week* https://theweek.com/roe-v-wade/1013221/a-controversial-data-firm-is-selling-abortion-clinic-visitors-location-data

1.3 Is there criteria that should be used to determine whether a particular APP entity, or class of entities, is appropriately included or excluded from the scope of the Code?

Learnings could be drawn from models for human right-based assessments of businesses and commercial products, to help identify classes of entities that warrant inclusion. While human-rights assessments vary between methods, the Danish Institute for Human Rights has synthesised commonalities across methodologies.[15] Applying their analytic methods surfaces four considerations around assessing human rights,[16] that may be helpful in identifying high-risk classes of entity for the COPC:

1. Potential seriousness of the privacy impact if something goes wrong in the sector: Where classes of entities have the capacity to generate severe risks to children's privacy, they should be considered for inclusion Evidence of severity of harms could include factors such as the nature of the data collected and used by the class of entities, including sensitive or identifiable information, or the nature of their service provision.
2. Irreparability of the harm caused by the impact if something goes wrong in the sector: Some privacy harms can be irremediable, such as when biometric data is leaked or lost, or sensitive personal identifying information exposed in breaches. Evidence of irremediability might include analysis of the types of data involved, analysis of data handling practices across the class of entities, and understanding about historical issues and the harms arising from them.
3. Number of people affected if something goes wrong in the sector: Where significant numbers of children are using a class of entity, it could be considered for inclusion. Evidence for significant child-use could include research or marketing materials that demonstrate high-levels of child-use proportionate their user-base or the Australian child population, or evidence to suggest rapid expansion among Australian child-users. (Note, this alone would not be a comprehensive enough criteria).
4. Probability of harms: Where there is evidence to suggest that privacy harms are likely within a class of entity, for example because of systemically lax protections, inclusions should be considered. Evidence of likelihood could include a history of breaches, or excessive levels of data harvesting for example.

We would encourage the OAIC to set ongoing review dates for the coverage of the COPC, and to establish mechanisms for academics, civil society or industry to present evidence to trigger ad-hoc reviews of coverage.

Question 2: When and how the Code should apply to APP entities

General comments regarding application

If the aim of the COPC is to enhance children's privacy, this requires maximising coverage which generally favours lowering thresholds for inclusion.[17] Below we discuss the merits of a formulation for a likely to be

[15]The Danish Institute for Human Rights 2020 *Human Rights Impact Assessments Guildance and Toolbox* https://www.humanrights.dk/files/media/document/HRIA%20Toolbox_Phase%203_ENG_2020.pdf

[16]According to research around human rights impact assessments, there is a fifth consideration — ease of impact mitigation/remediation.We are uncertain as to the extent that this final criteria would add value in this scenario.

[17]In this regard, the EU's 'accessible to children' standard sets a high bar for protection of children. It also reverses the onus of burden of proof; platforms need to demonstrate to regulators that young people cannot access their platform to avoid compliance, rather than regulators having to demonstrate young people's use of a platform to require compliance. Noting that this is not within the scope of the *Privacy and Other Legislation Amendment Act 2024* legislation and may require age assurance mechanisms which add complications

accessed requirement consisting of two conditions, building on the UK and Irish experience. Under this formulation, platforms would be considered likely to be accessed where they are:

1. *Likely to be accessed because they are directed to or intended for children, or*
2. *Likely to be accessed as demonstrated by either:*
    a. *Evidence that children's use of the service is more than de minimis or;*
    b. *It is the type of service that is likely to attract children*

2.1 What threshold should determine when a service is considered 'likely to be accessed by children'?

We do not believe the *Privacy and Other Legislation Amendment Act 2024* intended for there to be a high-bar for significance test, for two reasons:

- According to the second reading speech, the *Privacy and Other Legislation Amendment Act 2024* enacted in recognition that Australia's privacy laws had "not kept pace with the adoption of digital technologies."[18] The COPC is a direct response to this legislative deficit. The speech made clear that this Act is urgent and has an ambitious agenda for protection. The Attorney General highlighted the alarming amount of data that is collected about children, and outlined that this "high volume of data collection has created serious risks that can turn into real and serious harms", both now and into the future. This intent of this legislative context demands a regulatory response that is systemic and preventative, not narrow and reactive.
- The classes of entities identified for initial coverage were selected precisely because their services have high levels of privacy-risks inherently.

However, we appreciate that some thresholds or significance considerations will also be necessary in order to meaningfully describe what counts as 'evidence' that the service is used by children (or in the formulation above, part 2A).

We note that guidance around the UK's *Age Appropriate Design Code* ('AADC') outlines that significant use from children does not require a large number of children need to be using a service, nor that they must form a substantial proportion of users. It simply means that child users must be more than a de minimis group.[19] Determining what is significant requires exploration of both the numbers of child users and the risks posed to their data that this COPC is intended to redress.

As a further caution against the notion of using a numeric measure of significance alone; the population of Australian children aged under 18 is small. There are around 5.7m children aged 0-17,[20] which works out around 335,000 children in each year of age if evenly divided. This means numerically low levels of use could still represent a sizable portion of Australia's age cohorts. For example, it would still be possible for a platform to reach half of all Australian 16 & 17 year olds (which would be huge market penetration), while failing to reach a 0.5m threshold.

'Children's use' also warrants some further clarification. Often children are not 'active users' of a service in so far as they login or register for accounts, rather passive data subjects. Where children's data is being collected, used or disclosed by a service, children are in effect, users of the service.

(European Commission 2022 *Digital Services Act* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065)
[18]Mark Dreyfus 2024, *Second Reading Speech: Privacy and Other Legislation Amendment Bill https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result/Second_Reading_Speeches?BillId=r7249*
[19]TaylorWessing 2024 *Likely to be accessed* https://www.taylorwessing.com/en/global-data-hub/2024/february---childrens-data/likely-to-be-accessed-by-children
[20]UNICEF 2023 *How Many Children are there in Australia?* https://data.unicef.org/how-many/how-many-children-under-18-are-there-in-australia/

Evidence that children use the service — or in the formulation above part 2A — can come in many forms, and determining a threshold could require considerations of a range of evidence. The ICO's *Likely to be Accessed Guidance*[21] provides a comprehensive starting place that would be applicable to Australian, including:

- Data platforms have about the number of users aged under 18 on their services in Australia
- Research — internal or external from academics, market research, news stories etc — that suggests that Australian young people are using a service. (We note here that evidence of effect age-gating aimed at 'keeping out' under 18 year olds could be submitted as evidence that a platform is not likely to be accessed by children, but that this would not be required by or apply to all services). We note that eSafety already runs an annual survey documenting young people's use of online platforms[22]
- Information used or created for advertising purposes, such as data available in the RTB process or other advertising codes that suggest users are children
- Information received about complaints about child users, or complaints from child users.

Evidence that the service is likely to attract children — or in the formulation above part 2B — can also come in many forms, and could include considerations of the following for example;

- Use of the types of content, design features or activities which are likely to be attractive to children. Internal and external research can be useful in describing what this sort of content, features and activities are
- Whether children are known to access similar services
- The business model of the company
- If the company markets itself as having child users.

Given the extensive use of the Likely to be accessed standard internationally, it would be valuable to include as evidence in the Australian context, 'a previous determination that a service or part of a service is 'Likely to be accessed' in a similar determination conducted in the UK under the *AADC* or *Online Safety Act*, or Ireland under the *Fundamentals to a child-oriented approach to data processing* (the 'Fundamentals').

2.2 'Likely to be accessed by children' is the same standard as the *Age Appropriate Design Code*. Is there any evidence as to the practical effectiveness of the threshold in that context?

The 'Likely to be accessed' standard has been widely used. It is the standard for determination in:

- The UK's *AADC* where it applies to "relevant information society services which are likely to be accessed by children"[23]
- The Irish *Fundamentals* which covers services directed at, intended for, or likely to be accessed by

[21]UK Information Commissioner's Office 2020 *Likely to be accessed by children* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/
[22]Office of the eSafety Commissioner 2025 *The online experiences of children in Australia* https://www.esafety.gov.au/research/the-online-experiences-of-children-in-australia
[23]UK Information Commissioner's Office *Age Appropriate Design Code* 2020 https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/,

children[24]
- The UK's *Online Safety Act*, which places additional safety requirements on platforms likely to be accessed, and outlines what a 'children's access assessment' looks like[25]
- It is also the basis of some US State laws, such as the California *Age Appropriate Design Code*.

Most of the online platforms and services that will fall under the coverage of the COPC will have experience in completing 'Likely to be accessed' assessments, and this is helpful for both policy harmonisation and reducing burden on platforms, but also creating evidence that is useful for the Australian context.

The passage of the UK's *Data (Use and Access Act)* means that all guidance is currently being reviewed, which we would assume includes guidance around the Likely to be accessed test. We are not aware of any evaluations academic nor governmental in the meantime.

2.3 What steps should APP entities reasonably be expected to take to assess whether children are likely to access their services?

The use of 'reasonable steps' within Australian digital regulation has a long legal standing in Australia, in both the *Online Safety Acts* and privacy frameworks.[26] However, what is considered 'reasonable' is often contested including in the courts, and platforms have a track record of not undertaking activities described as examples (e.g. not undertaking example reasonable steps described in online safety guidance). Given this, taking a strong initial approach to expectations around 'reasonable steps' would be in children's best interests, and a more precautionary approach.

Reasonable steps could be used to bolster the evidence standards associated with various thresholds. These could include for example, requirements to take reasonable steps to:

1. Evidence whether their service is directed to or targeted at children
    - Evaluate market research data and advertising data describing who the audience of the platform is
2. A. Evidence whether children's use of the service is more than de minimis
    - Capture data about the number of users aged under 18 on their services
    - Undertake internal research or commission research to understand the number of users aged under 18 on their services
    - Keep abreast of, and have mechanisms for actively receiving, external research or evidence that describes or implies use of their service by under 18 year olds
    - Create internal systems that document the use of their service by child users, such as for example, tracking the age of inquiries or complaints from or about children, analysing internal data or user data for evidence of age. This may include evidence of effective age assurance systems, where they are already in use to 'keep out' children under 18, but this is not required
    - Referencing international 'likely to be accessed' determinations for a service, or similar service
2. B. Evidence whether their service is the type of service likely to attract children
    - Undertaking or commissioning internal and external research to explore if the sorts of content, features and activities deployed within a platform are likely to attract children

[24]Ireland, Data Protection Commission 2021 *Fundamentatls for a Child Oriented Approach to Data Protection* https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf,
[25]UK *Online Safety Act* 2023 https://www.legislation.gov.uk/ukpga/2023/50
[26]Reset.Tech Australia 2025 *Reasonable steps in platform regulations* https://au.reset.tech/news/reasonable-steps-in-digital-platform-regulation-what-is-reasonable-and-to-whom/

- Researching whether children are known to access similar services
- Analysing the platform's marketing material, to understand if it markets itself as having child users
- Referencing international 'likely to be accessed' determinations for a service, or similar service

If the aim is to drive up privacy standards, and ensure compliance with proposed reasonable steps, measures to improve transparency — for regulators and the 'public' — and auditing this evidence should also be considered in the COPC.

2.4 What role, if any, should age gating or other access control mechanisms play in meeting obligations under the Code?

Age gating produces many tricky questions, however we do not believe it was the intent of the *Privacy and Other Legislation Amendment Act 2024,* nor Parliament, that the COPC address them. There are many problems in the online world for children, but a COPC cannot and will not fix all of them, nor could it be reasonably expected to.

We do not believe that additional age gating or access controls are necessary to meet the requirements of the COPC, and that it might be unnecessary, complicated or disproportionate to require them. Requirements for age assurance add complications and we believe these could be avoided where they are not necessary.

This raises the common question 'but how do platforms know if the data belongs to a child'? We believe there is a relatively straight forward solution to this learning from the Irish *Fundamentals*:

- For platforms that are directed to or intended for children, platforms should simply assume all user data is children's data and apply the requirements in the COPC. (Barring obvious exceptions, for example where they allow parents or teachers to hold a linked account, or parents' credit card data).
- For platforms that are general use, and have adult and child users, where a user has self-identified as a child, or the platform suspect they are a child through any other already in place age assurance mechanism, the platform should assume that data is children's data.

This often raises a follow-on question about 'what to do about children who fib about their age online and pretend to be over 18?'. This is tricky for compliance with other regulations, but not so for the COPC:

- Where a user has identified that they are an adult but a platform has *any conflicting data* that raises suspicions that they are a child, the platform should err on the side of caution and treat that data as children's data.There are no 'downsides' to having additional data protections applied if in doubt. Suspicions about 'adults who might actually be children' can and are already derived from existing forms of age assurance such as analysis of their online behaviour, reports from other users, or other mechanisms.
- Where a platform genuinely has no reason to suspect a user is a child, they can treat the data as adult data.

We are aware that a few children-who-fib may go unprotected as a result of being undetected, in which case, they will have the same levels of privacy protection as they currently do in 2025. This will be an ever diminishing number of children, as requirements for age assurance from other regulations — both Australian and international — drive age detection across many platforms.

There is no perfect solution for this, but the perfect need not be the enemy of the good and proportionality is key. It would be an unfortunate outcome if the complexity of seeking a perfect solution to also protect children-who-fib derails the capacity of the COPC to be effective and immediately implementable. This would create a situation where no child receives any additional privacy protection (including those who fib and those who do not).

Specifically with regards to the 'Likely to be accessed' standard, age assurance is not a necessary part of the process. However, there is a formulation of a standard that would allow effective age gating to be a means of exclusion from the COPC's requirements, along the lines of the UK's *Online Safety Act*. In this instance, the standard would look something along the lines of Likely to be accessed demonstrated by a platform being:

1. *Likely to be accessed because they are directed to or intended for children, or*
2. *Likely to be accessed because they are in whole or in part, accessible to children; where there is either:*
    - *A. Evidence that children's use of the service is more than de minimis or;*
    - *B. It is the type of service that is likely to attract children*

Under this version of the standard, age assurance would only be required *if a platform chooses to claim exemption* because it does not meet the 'Likely to be accessed' standard, precisely because it has effectively age assured children out of their service. This approach shifts the onus of responsibility on to platforms; age assurance becomes a business choice available to platforms to make should they wish to avoid having to comply with regulations. Guidance around the UK's *Online Safety Act* provides clarity about how this might work (see Appendix 2).

We do not believe providing an age-assurance exemption is necessary in the context of the COPC. This is because the COPC covers social media services, designated internet services and relevant electronic service providers, and is deliberately not intended to cover wholly restrictive access services (i.e. services that may attempt to age assure all children away from their platform, like gambling apps or pornography services).

2.5 Are there alternative approaches APP entities could take to meet their obligations under the Code, beyond age gating or age verification methods? If so, is there any evidence on the impact of such approaches on children's access to services or privacy outcomes?

Neither the UK's *AADC* nor the Irish *Fundamentals* requires additional age assurance. We are unclear why additional age assurance would be required in the Australian context for the COPC.

Pre-existing mechanisms and knowledge that platforms already hold should be sufficient to determine who might be a child-user for the purposes of the COPC, such as self-reported date-of-birth data provided at registration, other age assurance mechanisms that are already in place, and data about user behaviour that they already process. Compliance with other regulations domestically and internationally is increasingly driving a need for more effective age assurance measures; enforcement of the COPC will benefit from this, but it does not need to contribute to this.

On the flipside:

- The COPC might have a lot to say about age-assurance mechanisms that are being introduced in order to comply with other legislative reforms. We appreciate this is beyond the scope of this consultation however (question 5.3 aside).

- There is an argument to be made that if additional data protections are provided to children online, children have one small reason not to fib about their age. Currently, there is little benefit to accurately self-identifying as a child online; all children get for being honest about their age is service limitations and restrictions. Children are concerned about their privacy,[27] and if there were privacy benefits to honestly self-identifying as a child, it might provide one small upside to encourage disclosure. To be clear, we are not saying this alone will supplant any need for age assurance emerging from other policy debates, we are simply noting that there are currently almost no upsides to self-identifying as a child online, and this may create one small benefit.

We note that concerns about age assurance processes are often weaponised in a way that paints privacy invasive, age verification as a necessity to implement any child protection standards, and thereby undermining support for the latter. However, this is not the case for the COPC, which is one of its unique strengths.

Figure 3: Deep dive into Comparative approaches to the 'Likely to be accessed' standard

In July 2025, Reset.Tech Australia hosted a policy roundtable exploring the 'Likely to be Accessed' standard from a comparative perspective. Thirteen policy experts discussed comparative approaches to the standard, noting:

- The experience from the implementation of the US' *Child Online Privacy Protection Act* (COPPA) suggests that where thresholds or standards are set without rigour, digital services tend to avoid compliance, rather than voluntarily adopt best practice protections. The 'actual knowledge' test outlined in COPPA created significant loopholes that allowed online services and products to 'skirt' the law, and avoid compliance. The actual knowledge standard sits alongside a 'directed at children' standard, but the large failure of the former created a very narrow set of coverage for American platforms.
- One of the consequences of the *Online Safety Amendment (Social Media Minimum Age) Act 2024* may be an inference that data about children under 16 will not be processed by social media platforms, so the COPC should not apply. This will simply not be the case, as data about 16 & 17 year olds will still be collected, and 13 - 15 year olds might still use platforms without registering for an account. 'Actual knowledge' standards or claims that 'these platforms are no longer directed at children because of the minimum age requirements' are not sound.
- The UK has two different types of LTBA-style determinations in operation:
  - The LTBA determination under the *AADC*: Platforms need to determine if their service is intended for use by children, or if not, if they are still accessed by or likely to attract children
  - The 'Children's Access Determination' under the UK O*nline Safety Act*: Platforms need to determine if their service is accessible to children (i.e. if they prevent child access). If not, they must then consider if their platform is accessed by or is the type of service likely to attract children.
- The EU's *Digital Services Act* has an even more broad standard, applying requirements for the protection of minors on platforms that are 'accessible to minors'.[28]
- Children's rights are an important consideration to centre in these discussions. A well defined LTBA assessment can help advance children's rights, and consideration of children's rights could help to define any thresholds within a LTBA standard

See Appendix 3 for the notes from the roundtable.

[27]Reset.Tech Australia 2023 *Realising young people's rights in the digital environment* https://au.reset.tech/news/report-realising-young-people-s-rights-in-the-digital-environment/
[28]European Commission 2022 *Digital Services Act* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065

Question 4: APP 1 – open and transparent management of personal information

4.4 What steps should APP entities take to ensure children, and their parents, can easily make privacy-related inquiries or complaints, and how should APP entities respond in a child appropriate way?

Figure 4 outlines a list of ten key features of good privacy inquiry and complaint mechanisms for a child rights perspective. These features were derived from consultations with Australian experts and children.

We believe that these requirements could become the basis for requirements for reasonable steps. For example, the COPC could include:

- Requirements to provide clear, plain language information about children's privacy rights. This should include a focus on what is okay for the platform to collect, use and especially share and disclose. It should also provide clear information about what they are allowed to inquire and complain about, and any potential outcomes of a complaint. It is difficult for children to complain where they are not sure what their rights are.
- Requirements to offer a range of accessible and flexible avenues for complaints and inquiries that are child friendly.
- Requirements about what responses to child inquiries or complaints should look like. These needs to include issues such as:
    - Time frame. Children want and expect rapid responses. While this might not always be possible, children can be sent rapid responses to acknowledge the receipt of their inquiry or complaint, and regular updates where it is taking more than a week to respond.
    - Avenues for response. Children may expect to be replied to via the mechanisms they initially used (e.g. if they sent an inquiry in-app, they might expect an in-app response), or clear guidance about where replies will be sent.
    - Child-accessible language. Responses need to be comprehensible to children.
    - Training for staff. Adequate staff training for those handling complaints from children is necessary to ensure processes are child-centric.
- Requirements for a 'review process', to provide children with the right to challenge a platform's decision. This should include requirements to inform children of their right to challenge a platform's decision and guidance about how to do so.
- Requirements to provide information about pathways and information about appropriate external support services and advocacy support as necessary. This includes information about:
    - Support for children experiencing harms, such as helplines etc
    - Support for children who may want help in making their complaint or requesting a review of a complaint, such as YouthLaw etc.
- Requirements to comply with all relevant federal Child Safe Standards (such as the National Principles for Child Safe Standards). This would include requirements to undertake consultation with children and young people to proactively solicit feedback about potential systemic issues *in addition* to having adequate complaint mechanisms.
- Requirements to presume complaints and inquiries from children are valid, and to not create unnecessary technical or bureaucratic objections to complaints (such as rejecting complaints because they've been made in the wrong format, or have passed an arbitrary time threshold).
- Requirements to provide confidentiality for unauthorised activities on platforms (subject to regulatory or legal requirements).
- Requirements to enable advocacy support for individual children's complaints, and for indirect complaints to be made by advocacy organisations, including mechanisms for super-complaints.
- Requirements for regular transparency reports on complaints, mechanisms, and outcomes and collaborate with the regulator to build knowledge on systemic trends.

- Requirements to offer remedies that are meaningful to the child, that acknowledge and respond to a child's views and expectations.

Figure 4: What does a good privacy inquiry and complaint mechanism look like on an online service?

Working with the Australian Child Rights Taskforce, Reset.Tech Australia held:

- A series of workshops to identify what 'good' looks like for children when it comes to inquiry and complaint mechanisms. Across June and July 2025, we worked with expert partners who routinely create processes and mechanisms to enable children to make complaints, disclosures or otherwise 'seek help', including Kids Help Line, ReachOut, YouthLaw Australia and academics. We iteratively created and refined a list of requirements for a good complaints or inquiry mechanism.
- Two workshops to review and refine this list with young people aged under 18 in July 2025, with 16 young people from Project Rockit taking part and 13 from Bravehearts.

The key requirements for a good complaints or inquiry mechanism emerging from this process include for example, suggestions that:

1. Platforms should provide clear information about privacy rights to children – including what privacy rights mean in practice, clear guidance about the responsibilities and limitations for data sharing in particular and how to complain and the potential outcomes of a complaint and
2. Platforms should provide a range of accessible and flexible avenues for complaints and inquiries that are child friendly. That is, there needs to be multiple ways children can reach out to platforms, and each of them should be accessible.
3. Platforms should have internal guidelines and processes that offer reliable and accessible responses to young people, including reasonable timeframes, appropriate avenues for response (e.g. email and 'in app' messaging), use of child-friendly language.
4. Platforms should make it clear that it is okay for children to disagree with their approach or decisions, and offer children the opportunity to challenge review decisions. This 'review' process needs to be child friendly.
5. Platforms should provide clear pathways and information about appropriate external support services (such as KidsHelpline) including advocacy support (such as YouthLaw).
6. Platforms should ensure their complaints and inquiries processes are compliant with all relevant Child Safe Standards. This includes:
    - Undertaking consultation with children and young people to proactively solicit feedback about potential systemic issues *in addition* to complaint mechanisms.
7. Platforms should not take technical objections to complaints (such as rejecting complaints because they've been made in the wrong format, or have passed an arbitrary time threshold). They should also provide confidentiality for unauthorised activities on platforms (subject to regulatory or legal requirements).
8. Platforms should allow for advocacy support for indirect complaints and mechanisms for super-complaints.
9. Platforms should provide regular transparency reports on complaints, mechanisms, and outcomes and collaborate with the regulator to build knowledge on systemic trends.
10. Platforms should offer remedies that are meaningful to the child, that acknowledge and respond to a child's views and expectations and thereby build children's confidence in the complaints process.

The Australian Child Rights Network's submission contains more information about this process.

Question 6: APP 3 — collection of solicited personal information

6.2 What does 'lawful 'and 'fair' mean in the context of children's personal information? How should these terms be applied specifically for children, given their evolving developmental and digital engagement stages?

The 'fair' collection of children's data could be considered in regards to their best interests. Given the additional rights children hold, and their unique vulnerabilities both developmentally and socially, fair collection of their data can only occur when it happens in children's best interests.

Considerations of children's best interests has precedent in determining lawful actions. 'Children's best interests' is an already existing principle in Australian law, and has also been applied in the context of international child rights treaties regarding the online environment (see Figure 5).

Figure 5: The Children's Best Interest Principle in children's data protection regulations

The Convention on the Rights of the Child introduces the concept of children's best interests in Article 3. It obligates national governments and their agencies, including Australia's, to consistently prioritise actions in children's best interests. It states: "In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration."[29]

The Committee on the Rights of the Child defines children's best interests as involving:

1. A substantive right: children's best interests should be the primary consideration in decisionmaking, including developing laws and policies, and can be invoked through legal challenges.
2. An interpretive legal principle: when legal decisions are open to interpretation, the one favouring children's best interests should be chosen.
3. A procedural rule: In decisions affecting children, their best interests should be a primary consideration in the process.[30]

More recently, this principle has been applied to children's experiences in the digital world. The Committee on the Rights of the Child emphasised this in its general comment on children's rights in a digital environment when it outlined that "the best interests of the child is a dynamic concept that requires an assessment appropriate to the specific context. The digital environment was not originally designed for children, yet it plays a significant role in children's lives."[31]

The COPC would not be alone in using the 'best interests' principle in guiding-decision making when it comes to determining what is fair or lawful processing of children's data. Many other countries and regions have already implemented it as a substantive right, including:

[29]UN General Assembly 1989 Convention on the Rights of the Child, https://www.ohchr.org/en/instrumentsmechanisms/instruments/ convention-rights-child

[30]Committee on the Rights of the Child 2013 *General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideratio*n, https:// www2.ohchr.org/english/bodies/ crc/docs/gc/crc_c_gc_14_eng.pdf, Paragraph 6

[31]Committee on the Rights of the Child 2021 G*eneral comment No. 25 (2021) on children's rights in relation to the digital environment*., https://www.ohchr.org/en/documents/general-commentsand-recommendations/generalcomment-no-25-2021-childrensrights-relation, Paragraph 12 & 13

- The UK's *AADC* outlining how the UK's data protection legislation applies to children, and is analogous to the the COPC in intent[32]
- Ireland's *Fundamentals*, outlining how the EU's General Data Protection Regime applies to children in Ireland (and, due to the EU's approach to data regulation, is applicable to most platforms in the EU)[33]
- Sweden's *The Rights of Children and Young People On Digital Platforms,* serving as guidance on how Sweden's data protection regulator understands data protection requirements as they apply to children[34]
- The European Commission's BIK+ Strategy.[35]

6.3 Are there cases in which the collection of children's personal information would not be considered fair in any circumstances?

Where data collection, use or disclosure is not in children's best interests, it cannot be considered fair.

We believe that targeted advertising is an example of a data practice that does not function in children's best interests. It creates a context that incentives extensive and unnecessary data collection and involves risky data handling practices, with no upside for children. Given this, it does not function in children's best interests and cannot be considered a fair use of data (see Appendix 4).

6.5 Do you have any specific views on how APP 3 should be applied, or complied with, in relation to the privacy of children?

Compliance with APP3, and a range of other APPs, would be enhanced by expectations that platforms undertake some sort or rigorous assessment activity, such as a Data Protection Impact Assessment, or a Best Interests Impact Assessment.

Impact assessments are required under the *AADC* and expected under the *Fundamentals*, and this approach drives much of the compliance across those Codes. Many of the platforms covered by the COPC will have experience completing these assessments, and it would not be a comparatively radical or excessive ask to require similar assessment activities in Australia.

There is also broad support across civil society for the introduction of data protection impact assessments, with a range of children's organisations supporting the call for impact assessments.[36]

Requiring these assessments, or summaries of these, to be made publicly available would also serve to enhance transparency (as relevant to APP1) and overall trust.

[32]Information Commissioners Office 2020 Age Appropriate Design Code, https://ico.org.uk/ media/for-organisations/ guide-to-data-protection/keydata-protection-themes/ageappropriate-design-a-code-ofpractice-for-online-services-2-1. pdf
[33]Data Protection Commission 2021 The Fundamentals for a ChildOriented Approach to Data Processing, https://www. dataprotection.ie/en/dpcguidance/fundamentalschild-oriented-approach-dataprocessing
[34]The Swedish Authority for Privacy Protection 2021 *The rights of children and young people on digital platforms,* https://www.imy.se/globalassets/ dokument/rapporter/the-rightsof-children-and-young-peopleon-digital-platforms_accessible. pdf
[35]European Commission 2022 European strategy for a better internet for kids (BIK+) | Shaping Europe's digital future, https://digital-strategy. ec.europa.eu/en/policies/ strategy-better-internet-kids
[36]See for example Reseet.Tech Australia 2025 *Children's Privacy Code* https://www.childrensprivacycode.org.au/

Question 9: APP 6 – use or disclosure of personal information

9.4 Do you have any specific views on how APP 6 should be applied or complied with in relation to the privacy of children?

Consideration of children's best interests is also potentially useful when it comes to determining what is a fair or lawful use or disclosure of children's data.

Requirements for rigorous impact assessments would additionally help the realisation of APP6.

Further, there are a couple of current uses of children's data that do not reflect global 'best practice' nor advance children's best interests. These could be remedied under the COPC by requirements to, for example:

- Set privacy settings as 'high' by default for all Australian children, including 16 & 17 year olds. Privacy-by-default advances children's right to privacy, and additionally realises their right to protection from harm via unwanted contact with unknown users. For example, at one stage Meta found, 75% of all 'inappropriate adult-minor contact'—or as it is more commonly called, grooming—on Facebook was a result of their 'People You May Know' friends recommendation system.[37] The PYMK feature did/does not function when accounts are private. A parliamentary question in September 2024 confirmed that the PYMK feature is still turned on for Australian teens.[38] While many larger online platforms now default all children under 18 to private by default, as required in other jurisdictions under similar regulations — including the *AADC*, the *Fundamentals* — this is not an Australian requirement. Indeed, Australian guidelines outline that setting privacy settings to high as a default is only required for those 15 and under on social media services.[39] The COPC is intended to protect children's data right up until the age of 18, and enshrining this within the COPC would ensure that all new platforms, or smaller platforms that currently do not meet this 'standard' voluntarily would be required to in Australia.

- Prohibitions on the default collection of children's geolocation data. Geolocation data is particularly important to young people's right to privacy, but also to their sense of safety. Both the *AADC* and the *Fundamentals* outline prohibitions on the default collection of children's geolocation data, but no such Australian requirement exists. Indeed, Australian guidelines outline that social media services must not broadcast children's live location data.[40] However, not broadcasting location data is not the same as not collecting location data, and creating a trove of kid's location data inevitably creates unnecessary risks around data leaks and breaches, internal misuse and disclosures[41] and inappropriate commercial uses and disclosures.

[37]As made public in *Alexis Spence et al. v. Meta,* U.S. District Court for the Northern District of California, Case No. 3:22-cv-03294 (filed June 6, 2022) p. 11-12, *Growth, Friending + PYMK, and Downstream Integrity Problems.* https://pugetstaffing.filevineapp.com/s/9eb2BZcUfhdTxkxIfV45CJnIivYHhdWcRRuQVwSMz120RVs7ATmxn9r5
[38]Zoe Daniel 2024 *Time to rein in the technology giants* https://zoedaniel.com.au/2024/09/09/time-to-rein-in-the-technology-giants-the-australian-9-sept-2024/
[39]Australian Mobile Telecommunications Association (AMTA), BSA | The Software Alliance (BSA), Communications Alliance Ltd (CA), Consumer Electronics Suppliers Association (CESA), Digital Industry Group Inc. (DIGI) and Interactive Games and Entertainment Association (IGEA) 2023 *Online Safety Codes for Class 1A & 1B* https://onlinesafety.org.au/wp-content/uploads/2023/06/230616_1_SMS-Schedule_REGISTERED-160623.pdf
[40]Australian Mobile Telecommunications Association (AMTA), BSA | The Software Alliance (BSA), Communications Alliance Ltd (CA), Consumer Electronics Suppliers Association (CESA), Digital Industry Group Inc. (DIGI) and Interactive Games and Entertainment Association (IGEA) 2023 *Online Safety Codes for Class 1A & 1B* https://onlinesafety.org.au/wp-content/uploads/2023/06/230616_1_SMS-Schedule_REGISTERED-160623.pdf
[41]Which can have very serious ramifications. See for example, Natasha Lomas 2022 'Instagram fined €405M in EU over children's privacy' *Techcrunch* https://techcrunch.com/2022/09/05/instagram-gdpr-fine-childrens-privacy/

We note that both of these 'uses' are somewhat addressed in the Online Safety Codes, largely the Code addressing Class 1a & 1b material. While these codes are new, they do not offer 'best practice' protections for children's privacy *but they were not they intended to*. When this was raised with the Online Safety Code drafting team during the consultation process, the Code drafters noted that "we consider that this issue is best dealt with through changes to the Privacy Act 1988 (Cth) (currently under review)."[42] That is, they anticipated and expected privacy protections to be dealt with via privacy reform processes, such as the current process. The fact that the Online Safety Codes set lower levels of privacy protections in 2023 as a 'stop-gap' measure is not definitive nor final. Rather it presents an opportunity to address these privacy concerns before they become norms within the Australian digital landscape. There was always an expectation that privacy reforms would 'go back' and address these issues properly (see Figure 6).

					[illegible] advertising and socialisation by commercial interests supported by industry	
41	Australian Child Rights Task Force		Use of GPS location data of children	Privacy of children	At the least, the Codes should reflect a prohibition on the collection of GPS location datas to address risk of misuse or safety breaches.	We consider that this issue is best addressed by the Privacy Act 1988 (Cth) (under review).
42	Australian Child Rights Task Force		Consultation	General	Codes development calls for a transparent and comprehensive examination of	

Figure 6: The Online Safety Code's drafters response to the proposals to, for example, implement improvements around the collection and use of children's GPS location.

Question 10: APP 7 – direct marketing

10.1 Can an APP entity ensure that it creates a 'reasonable expectation' that it may use or disclose children's personal information for the purposes of direct marketing? And if so, how?

We do not believe it is possible for children to hold reasonable expectations about direct marketing given the complexity and scale of information that it would take to understand current practices. 'Direct marketing' covers a wide range of practices, and some are indeed too complex for adults to meaningfully comprehend, let alone children. Given this, we believe that direct marketing should only be allowed using a child's data, where that child has consented to and shared their data directly with an entity for these purposes, and it is in a child's best interest. We note that this is in keeping with proposals in the *Privacy Act Review Report*.[43]

[42]Australian Mobile Telecommunications Association (AMTA), BSA | The Software Alliance (BSA), Communications Alliance Ltd (CA), Consumer Electronics Suppliers Association (CESA), Digital Industry Group Inc. (DIGI) and Interactive Games and Entertainment Association (IGEA) 2022 *Submissions log and industry associations' responses to public consultation feedback* https://onlinesafety.org.au/wp-content/uploads/2022/11/221118_Submissions-log-responses_FINAL.pdf or archived at https://web.archive.org/web/20250424041659/https://onlinesafety.org.au/wp-content/uploads/2022/11/221118_Submissions-log-responses_FINAL.pdf

[43]Proposal 20.5m if implemented, would prohibit direct marketing to a child unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests. See Attorney-General's Department 2022 *Privacy Act Review Report* https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf

Question 11: APP 8 – cross-border disclosure of personal information

11.3 Do you have any specific views on how APP 8 should be applied or complied with in relation to the privacy of children?

The cross-border flow of children's data is widespread within the online space. Large online platforms have worked to onshore EU data, as required by regulations, and to some extent US data (for example, project Clover and project Texas at TikTok[44]), but Australian children's data is stored and processed overseas as part of due course. It is not always clear to us what protections are in place for children's data before it is transferred, nor how children are notified or their specific consent gathered. Because of the opacity of this process, we believe that a precautionary, child-centred approach would involve a presumption of onshoring data processing. We are aware that this would be a significant change.

Further, we believe there is an existing compliance issue with APP8 in general, including for children. This will *also* need addressing, on top of any additional measures of protection provided by the COPC.

Question 14: APP 12 – access to personal information

14.1 What mechanisms are needed to ensure children can easily access their own personal information?

Standard 15 of the UK's *AADC* outlines that platforms should make online tools available to children to enable them to exercise their data rights easily, including the right to request their data. It also outlines expectations for these tools. These might be useful for consideration in the COPC, and include:

1. Requirements to make tools prominent. This would include making sure tools are promoted and visible to children in places that they may see in their user-journey across a platform. They also need to be easily searchable, and have links included in privacy hubs or help centres where platforms offer them.
2. Requirements to make tools age appropriate and easy to use for children. This would include making sure tools use plain language, and are user-tested by Australian children to ensure use of ease.
3. Requirements to make tools specific to the rights they support, for example, calling the feature 'see or download my data' or 'how can I see what data you hold about me' or the likes.
4. Requirements to include mechanisms for tracking progress of requests, in a timely fashion. This would include requirements to for example provide notification of the receipt of a request, as well as updates about the implementation (or not) of the request.

[44]Politico 2023 'TikTok launches 'Project Clover' charm offensive to fend off European bans' *Politico* https://www.politico.eu/article/tiktok-pitches-data-security-plan-to-fend-off-european-bans/

14.4 What timeframe should be considered a 'reasonable period' for responding to a child's access request?

If the presumption is that requests to see or access data will be honoured — barring exceptional circumstances governed by children's best interests — the tools to enable data access will be largely automated. It follows then, that response to requests for access can be rapid and fast.

We note that most large online platforms have tools that:

- Provide immediate or fast (within a day) notification of receipt of the request
- Rapid responses to the access request itself. This is usually in the form of a data downloads accessible within 2 or 3 days of the request

These could be regarded as reasonable periods for average responses, with extensions or exemptions where issues surrounding children's best interests are enlivened.

Question 15: APP 13 – correction of personal information

15.2 What processes or mechanisms should be established to allow children to request corrections of their personal information easily?

As above, Standard 15 of the UK's *AADC* outlines that platforms should make online tools available to children to enable them to exercise their data rights easily, such as the right to request a correction. It also outlines expectations for these tools. These might be useful for consideration in the COPC, and include:

1. Requirements to make tools prominent. This would include making sure tools are promoted and visible to children in places that they may see in their user-journey across a platform. They also need to be easily searchable, and have links included in privacy hubs or help centres where platforms offer them.
2. Requirements to make tools age appropriate and easy to use for children. This would include making sure tools use plain language, and are user-tested by Australian children to ensure use of ease.
3. Requirements to make tools specific to the rights they support, for example, calling the feature 'correct my data' or 'what do I do if some of my data is wrong' or the likes.
4. Requirements to include mechanisms for tracking progress of requests, in a timely fashion. This would include requirements to for example provide notification of the receipt of a request, as well as updates about the implementation (or not) of the request.

There are situations where incorrect data can raise real concerns for children's safety or wellbeing. Given this, it would be helpful if there were requirements for tools and mechanisms to allow children to identify these more worrisome requests. Following this, the COPC could also consider including requirements to ensure entities have in place mechanisms to 'fast track' these more worrisome requests. As an example from a parallel area, the public facing complaints mechanism run by the Office of the eSafety Commissioner asks respondents to simply note if they are distressed when they lodge a request (last time we checked, on a scale of 1-10). A similar, self-identified question such as "does this potential data error make you feel immediately unsafe or unwell" or similar, might help improve the service children experience.

To advance children's right to correct their data, any mechanisms offered need to provide children the ability to challenge any decisions made or actions taken that they do not agree with. Any tools developed could outline and guide a child through the process of challenging a decision.

15.4 What timeframe should be considered a 'reasonable period' for responding to a child's correction request?

Requirements calling for a timely response to requests to correct data would be a welcome addition to the COPC. However, multiple types of requests are possible and these may have different requirements. For example:

- Notifications of receipt of requests — which are relatively straight forward and could be automated. We believe a 48 hour timeline for acknowledging receipt of a child's request would be in keeping with existing practice, and that regular (weekly) updates could also be required.
- Response to the correction request itself — this will depend on the complexity or urgency of the request from a child, but an initial starting requirement of one month seems reasonable where cases are not urgent. Platforms should be required to notify children if more than a month is necessary to comply with their request. We note that in consultations we held with young people, they explicitly said one to two weeks, and that one month would leave them feeling 'forgotten' or 'overlooked'. However, we note that these processes can be complicated, and that with notifications along the way, including receipt of request and updates, this could be mitigated.

Outcomes we would like the Code to deliver for children

There are two outcomes we would like to see the COPC deliver for children; a functional right to erasure, and; a presumption against (or prohibition on) use of children's data for targeted advertising purposes. Below, we describe why we feel it is appropriate for the COPC to deliver these outcomes, suggest 'mechanisms' within the COPC that could be deployed to deliver them, and outline where there are comparative expectations in place within global privacy frameworks.

The right to erasure

Why is it appropriate to include a right to erasure?

The COPC would be well placed to ensure children have the right to data erasure.

The right to erasure — or the right to request your data be deleted — is one way to ensure that children and young people have more control and ownership of their data. The right to erasure has been proposed as one way to restore the power imbalance between online service and consumers,[45] and this power imbalance is even more acute between children and (adult run) digital platforms.

It is also a right. The *General Comment on Children's Rights in Relation to the Digital Environment* outlines that children should have the right to delete data when they believe it is unnecessarily stored by private entities:

> "States parties should ensure that children and their parents or caregivers can easily access stored data, rectify data that are inaccurate or outdated and delete data unlawfully or unnecessarily stored by public authorities, private individuals or other bodies, subject to reasonable and lawful limitations. They should further ensure the right of children to withdraw their consent and object to personal data processing where the data controller does not demonstrate legitimate, overriding grounds for the processing. They should also provide information to children, parents and caregivers on such matters, in child-friendly language and accessible formats."[46]

Ensuring this international child rights requirement is met requires offering children some sort of right to erasure, albeit in this instance limited to where they believe collection or use is unnecessary. Combined with the right to object to processing, a general 'right to erasure' and request mechanism would be necessary to advance this right.

There is also strong public support and community expectations for such a presumption. In a poll of 1,500 Australian adults, conducted by YouGov in July 2025, 89% outlined that they would 'strongly agree or agree' with the COPC creating the right for children to request data deletion (See Figure 7).

[45]Attorney General's Department 2022 *Privacy Act Review Report* https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

[46]United Nations Committed on the Rights of the Child 2021 *General comment No. 25 (2021) on children's rights in relation to the digital environment* https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=fT3nx%2FKEyjPie59GG8iHdDugSg7GO4Dn9%2BWkWC%2Fa8TLwKtEAuEF1HM7qW2BzwAImZaR0aN5pTFnoVkzMYkxYKQ%3D%3D, Paragraph 72

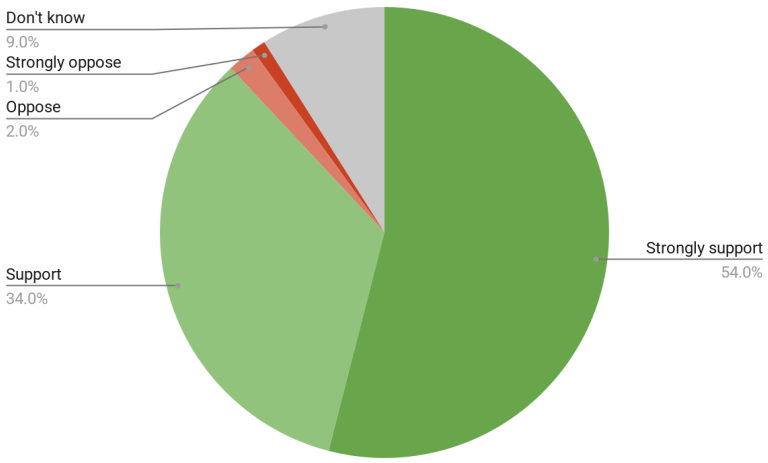


Figure 7: Responses to the question 'Would you support this Code creating a 'right' for children or their parents to request children's data be deleted from online platforms like social media platforms?' (n= 1,500)

How has the right to erasure been implemented for children elsewhere?

This would not be a radical proposition, rather it would help Australian children enjoy rights already widely held by other children internationally. The right to delete is already guaranteed for children and young people (and adults) in a range of other jurisdictions, including:

- In the EU, under GDPR, under articles 15 and 17. It also sets a timeline for one month as a standard for the time to deletion
- In the UK, under the *Data Protection Act* and also codified in the *AADC* standard 15.
- In large parts of the US, such as California, under the *California Consumer Privacy Act*, and Virginia under the *Virginia Consumer Data Protection Act,* Colorado under the *Colorado Privacy Act,* Connecticut under the *Connecticut Data Privacy Act* and Utah under the *Utah Consumer Privacy Act*.

We also note that many large online platforms that the COPC will regulate already offer children the ability to request the complete deletion of their data, and that this is an 'emerging global best practice standard'. This includes Instagram and Facebook,[47] TikTok[48] and Snapchat.[49] Enshrining the right to erasure would ensure that all new platforms, or smaller platforms that currently do not meet this 'standard' would be required to in Australia.

This also suggests that the technical mechanisms needed to ensure this have been developed and deployed by the vast majority of the online platforms that will be covered by the COPC.

[47]Meta 2025 *Delete your Information or Account* https://www.facebook.com/privacy/policy/
[48]TikTok 2025 *Can a User Request to Have their Data Removed?* https://usds.tiktok.com/can-a-user-request-to-have-their-data-removed-and-deleted-from-tiktok
[49]Snapchat 2025 *How do I Clear my Data on Snapchat?* https://help.snapchat.com/hc/en-us/articles/12324650978964-How-do-I-clear-my-data-on-Snapchat

How might this be enacted in the COPC?

Issues around erasure are not limited to a particular APP, rather would offer a remedy or redress where APPs have been violated. For example, if data was collected in a way that as not transparent to a child (violating APP1), or collected in a way that was not strictly necessary for the purposes outlined (APP3), or used or disclosed in a way a child felt was violative (APP6), providing a child or their parents with the right to request deletion would be one way of effecting a remedy.

Noting that we are not 'drafting' experts, but that we could see a way for a simple extension or interpretation of APP 13 to have the effect of requiring platforms to provide remedies for children who request data deletion. APP 13 will require platforms to take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading. If children's perspectives on what is considered 'relevant' or indeed accurate are taken into account as the implied basis for any data deletion request, then an expected remedy — or reasonable step — could be understood to be actioning a child's request to delete their data.

A presumption against the collection, use or disclosure of data for targeted advertising

Why is it appropriate to include a presumption against the collection, use or disclosure of data for advertising purposes?

The COPC would be well placed to prohibit or presume against the collection, use and disclosure of children's personal data for targeted advertising purposes on privacy grounds.

Targeted advertising is a violation of children's right to privacy because of the data handling process it involves. We are aware there are many interconnected discussions occurring about advertising and children, and these are often conflated and lead to conflicting policy 'solutions'. These are discussed in more detail in Appendix 5, but there are large debates about children and commercialisation, and/or children and the potential effects of *harmful* advertising. They are not substantively the same as discussions about the data practice of targeted advertising.

Targeted advertising inherently involves multiple concerning data handling practices, such as:

- The widespread collection of excessive amounts of data about users' behaviour, including that of children.[50] Data minimisation does not appear inherent to this process. It is unclear whether young people meaningfully consent to these practices,[51] and other questions arise around data use, such as necessity, purpose limitation, and transparent notification.
- The use of this data to create an automated profile of a user for the purpose of delivering personalised advertising.[52] These automated profiles are most often created by international

[50]Reset.Tech Australia 2024 *Australians for Sale: Targeted Advertising, Data Brokering and Consumer Manipulation* https://au.reset.tech/news/coming-soon-australians-for-sale-report/
[51]Reset.Tech Australia 2021 *Did we really consent to this?* https://au.reset.tech/news/did-we-really-consent-to-this-terms-and-conditions-young-people-s-data/
[52]See for example Reset.Tech Australia 2021 *Profiling Children for Advertising* https://au.reset.tech/news/profiling-children-for-advertising-facebooks-monetisation-of-young-peoples-personal-data/). Meta, the core example in this report, subsequently claimed to turn off the ability for advertising to reach children through profiling, which was a misleading claim (see Reset.Tech Australia 2021 *Facebook still misusing young people's data* https://au.reset.tech/news/facebook-caught-red-handed-harvesting-teens-data/), a statement they had to correct on record in the US Senate after being presented with this research (available on C-SPAN 2021 *Senate Committee Hearing on Online Protections for*

companies, with no human oversight or 'humans in the loop'.
- Finally, the delivery of an advertisement to a user. Both the content of the ad and the timing of the ad delivery are informed by data profiling, often in concerning ways involving the RTB system.[53]

Because of the privacy risks involved, targeted advertising is a violation of children's right to privacy. This is regardless of the nature of the advertising that is recommended to children. Regulations regarding the *content* of advertising, or requirements to prohibit specific types of advertising content, are best left to broadcasting and communications regulation.

Targeted advertising creates a privacy-risky environment for young people and places them in danger of harm. Privacy harms are real and cognisable, and include psychological harms, relationship harms, autonomy harms and discrimination.

There is also strong public support and community expectations for such a presumption. In a poll of 1,500 Australian adults, conducted by YouGov in July 2025, 86% outlined that they would 'strongly agree or agree' with the COPC presuming against targeted advertising (See Figure 8).

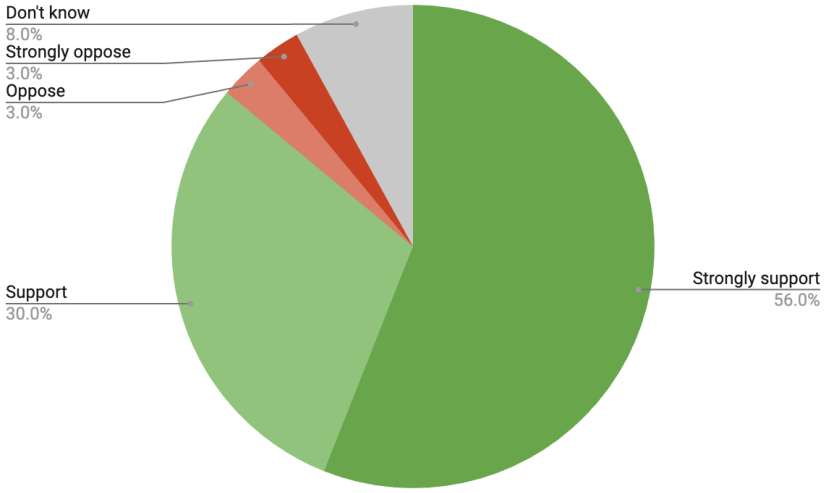


Figure 8: Responses to the question 'Would you support this Code creating a 'rule' that children's data shouldn't be collected or used just to deliver them targeted advertising? (n= 1,500)

How has the presumption against the collection, use or disclosure of data for advertising purposes been implemented for children elsewhere?

Multiple jurisdictions have presumed against the practice in comparable children's data codes, or other regulations. The UK, Ireland and the EU have used data protection laws to create a presumption against targeted advertising by outlining that children should not be profiled (see Figure 4). The EU has dovetailed this with a broader prohibition under the *Digital Services Act* (DSA).

Children https://www.c-span.org/program/senate-committee/senate-hearing-on-online-protections-for-children/605914) or as Sarah Wynn-Williams describes it a "devised cover-up" and a "flat out lie" (in Sarah Wynn-Williams 2025 *Careless People* Macmillan, London)

[53]ICCL 2024 *Australia's Hidden Security Crisis* https://www.iccl.ie/digital-data/australias-hidden-security-crisis/

Feature	Ireland (The *Fundamentals*)	UK (*AADC*)	EU (GDPR & DSA)
Targeted Ads	Very clear presumption that children's data should not be used to deliver targeted advertising.	Discouraged but does not go as far as the Irish approach. Outlines that harmful advertising is prohibited.	Very clear presumption against & prohibition of practice
Profiling	Not allowed unless justified as in children's best interests. Organisations should not profile children, engage in automated decision-making concerning children, or otherwise use their personal data, for advertising/ marketing purposes, unless they can clearly demonstrate how and why it is in the best interests of children to do so.	Targeted advertising must be turned off by default, and must be justified as in children's best interests. Companies need to ensure features that rely on profiling are switched off by default (unless there is a compelling reason to do otherwise).	Not allowed unless justified as in children's best interests
Legal Basis	EU GDPR	UK GDPR & *Data Protection Act*	EU GDPR & DSA

Figure 4: *A simplified overview of how different jurisdictions handle targeted advertising and children*

We also note that many large online platforms that the COPC will regulate already do not use Australian children's data to deliver targeted advertising, and that this is an 'emerging global best practice standard'. This includes platforms such as Instagram, Facebook,[54] and YouTube.[55] These were global service changes announced over time, presumably to ensure compliance with these international regulations. TikTok does not deliver targeted ads to children in Europe, the UK, Brazil, Mexico and Colombia in compliance with domestic regulations, but also limits them across the US, Canada and Latin America.[56] Australian, Asian and African teens appear to remain unprotected on this platform. Presuming against, or prohibiting, targeted advertising to children would lift up standards of protection for Australian children to global best practice. This would include on TikTok, but also on new and smaller platforms that do not offer best-practice protections to Australian children.

This fact that many online platforms have already turned off targeted advertising for children, and can still deploy advertising without the use of children's data, suggests that the technical mechanisms needed to do so have been developed and are widely in use.

We are aware of concerns from some service delivery organisations that limitations of targeted advertising would prevent them from 'reaching' young people online. Firstly, it is unclear to us the extent to which their current online outreach practices *actually* involve targeted mechanisms, given the number of platforms that have abandoned the practice. It is possible that a prohibition on targeted advertising is being erroneously conflated with a prohibition on online advertising. Secondly, the practice itself is still

[54]Who turned off the ability for advertisers to target children, and the use of 'online engagement' to drive their advertising algorithm in January 2023. See Meta 2023 *Continuing to Create Age-Appropriate Ad Experiences for Teens* https://about.fb.com/news/2023/01/age-appropriate-ads-for-teens/

[55]Google 2025 *Ad-serving protections for teens* https://support.google.com/adspolicy/answer/12205906?hl=en

[56]TikTok 2025 *Protecting minors on TikTok: advertising initiatives* https://ads.tiktok.com/help/article/protecting-minors-on-tiktok-advertising-initiatives

privacy violating, regardless of the content of the ads. Even if targeted advertising is occasionally used to promote 'good ads', it is still a violation of privacy and this overall risk profile would justify prohibiting the use of children's data to fuel this practice.

How might this be enacted in the COPC?

Issues around targeted advertising are broader than those related to direct marketing, which is addressed under APP 7. Rather, targeted advertising intersects with a wider range of APPs. For example:

- APP 1 — may be violated where the practice is not understood or transparent to children
- APP 3 — may be violated where the collection of the data used to drive the targeted ad delivery is not reasonably necessary for the online platform's functioning, and where sensitive information is collected with expressed consent.
- APP 6 — may be violated where entities use, share or disclose personal information for targeted advertising purposes when it was ostensibly collected for other purposes
- APP 8 — may be violated as the RTB system discloses and processes data internationally
- APP 11— may be violated, where reasonable steps are not taken to protect children's information in the RTB system from unauthorised access, modification or disclosure.

The process of targeted advertising involves a 'pipeline 'of data handling practices, including the collection, use and disclosure of data, as well as automated profiling. This means that there are multiple ways a Code could address targeted advertising, and a pipeline-wide approach would be desirable (a data-cycle approach). This could include addressing targeted advertising in though APPs 1, 3, 6, 7, 8 and 11 as outlined above, but it might also be addressed as a stand alone standard or outcome based requirement.

Appendix 1: Technical assessment of 5 Victorian EdTech products, conducted by Human Rights Watch[57]

Technical analysis of five apps and websites procured or recommended for school students by the Victorian Department for Education and Training were found to have a number of privacy breaches, including:

- Eleven third party advertising trackers built into apps or websites that send student's data directly to advertising companies, including Google's DoubleClick and Facebook ad products.
- Ten programmes (SDKs) embedded in products that allow other companies to access student data, including Google and Facebook Advertising products (Google AdMob and Facebook Ads). These give surveillance advertising titans direct access to data about Australian students
- Cookies and tracking pixels that 'track' and follow young people across the internet, after they have logged out of the educational product. These allow advertising companies to track and follow students, and see what they look at and interact with online after class
- Apps that collected student's precise GPS location information. These are unnecessary in an education setting, and create privacy and security risks
- Apps that collected details about the contacts in student's phones, including the profile pictures associated with them. These are unnecessary, and just a bit creepy
- Apps that collect student's unique identifiers (unique codes associated with their device and profiles) and link this data to other data sources, to build 'profiles' about students. These allow private companies to create alarmingly detailed profiles about young people

[57]Han Hye Jung 2022 *How Dare they Peep into my Private Life?* https://www.hrw.org/sites/default/files/media_2022/10/HRW_20220711_Students%20Not%20Products%20Report%20Final-IV-%20Inside%20Pages%20and%20Cover.pdf

EdTech product recommended or procured in Vic	Privacy issues identified
ClickView ClickView is a website primarily directed at secondary and primary school students, and was recommended for use in Victoria. *"ClickView is the leading producer of video content for K-12 and higher education settings. Access compelling, entertaining, curriculum-relevant video content and teacher resources, compile your own video library and leverage interactive testing materials for formative assessment. Trusted by over 5,000 schools and colleges around the world"*	The investigation found this website had **one third party tracker installed sending data about children to commercial advertising companies,** Google Analytics The investigation found that the privacy policies of this website failed to disclose the presence of the Google tracking feature
Minecraft: Education Edit Minecraft: Education Edit is an app primarily directed at students, and was recommended for use in Victoria. *"Minecraft: Education Edition is a classroom version of the hugely popular game Minecraft, specifically created to immerse students in various Minecraft worlds to promote creativity, problem-solving, critical thinking, and collaboration between students."*	The investigation found this app was **collecting student's unique identifiers (unique phone serial codes etc) and engaging in ID bridging**. This means it was identifying individual students and 'linking' their data to enhance profiles The investigation found this app **collecting student's precise location data**, time of current location, last known location, coarse location & WiFi BSSID The investigation found **7 programmes (SDKs) embedded in this product that can allow other companies to access the student data** that Minecraft: Education Edit has, this included Google AdMob and Facebook Ads.
Education Perfect Stile Education is a website primarily directed at students, and was recommended for use in Victoria. *"Spark your students' interest in science with these curriculum-aligned resources to support science teaching and learning"*	The investigation found **11 third party trackers sending data about children to commercial advertising companies**, including Google's advertising products (Google Ad Manager, DoubleClick) and Facebook The investigation also found **1 active cookie tracking students across the internet** (sending data to Google's DoubleClick ad service) The investigation also found **1 active tracking pixel, tracking students across the internet** (Facebook Pixel) The investigation found their privacy policy failed to disclose the presence of the ad trackers, Cookie and tracking pixel
Stile Education Stile Education is a website primarily directed at secondary school students, and was recommended for use in Victoria. *"Stile is a library of online, interactive science lessons for Years 7-10, aligned to the Australian and Victorian Curriculum"*	Stile Education was not found to be collecting nor sharing students data, demonstrating that it is possible to have privacy preserving EdTech products

Cisco WebEx - not an Ed Tech product, but widely in use in schools and included in the HRW report. Included here for completeness. An app that is used to facilitate calls and communication. It is not specifically targeted at students, but was recommended for use in Victoria. *"Cisco Webex is an app for continuous teamwork. Move work forward in secure work spaces where everyone can contribute anytime with messaging, file sharing, white boarding, video meetings, calling, and more. It works on virtually any device, with these top benefits for mobile app users."*	The investigation found this app was **collecting student's unique identifiers (unique phone serial codes etc) and engaging in ID bridging**. This means it was identifying individual students and 'linking' their data to enhance profiles The investigation found this app **collecting student's precise location data**, time of current location, last known location, coarse location & WiFi BSSID The investigation found this app was also **collecting student's contacts' information** (i.e. phone book), including their saved profile photos The investigation found **3 programmes (SDKs) embedded in this product that can allow other companies to access the student data** that Cisco has: Google Firebase Analytics, Crashanalytics and Amplitude The investigation found that Cisco's privacy policy was deceptive, and failed the collection of student's persistent identifiers, and engaging in ID bridging, that they collected location data, student's call logs, student's contacts' information, including their saved photos, the use of embedded SDKs and the identity of third parties receiving users' data

List of third party advertising trackers, Cookies and Tracking Pixels discovered, that harvested and send data directly to advertisers in Vic	**List of programmes embedded in this product that can allow other companies, including advertisers, to access the student data (SDKs) in Vic**
Google Analytics Google Doubleclick Google Tagmanager Facebook.com Facebook.net Hubspot hs-analytics.net Hubspot hsadspixel.net Hubspot hsforms.com Hubspot hubspot.com Mux litix.io Wistia wistia.com Tracking pixel - Facebook Pixel Cookie - sending data to Google's DoubleClick ad service	Facebook Ads Google AdMob Google CrashLytics Google Firebase Analytics Amplitude AppLovin AppsFlyer ironSource Twitter MoPub Unity3d Ads

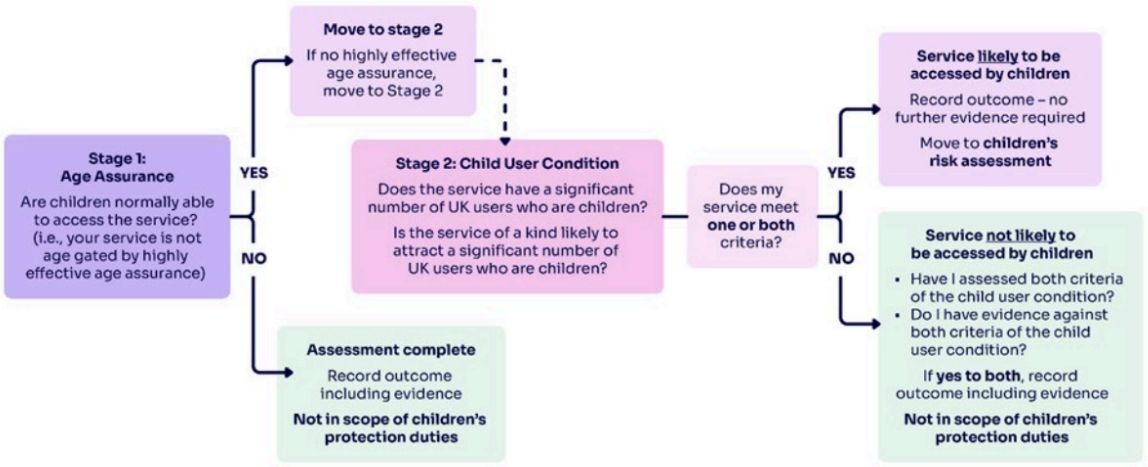
Appendix 2: Age assurance within the Likely to be accessed determination in the UK's *Online Safety Act*

The UK's *Online Safety Act* applies to a much broader range of online services than the COPC, including restricted access services. For this reason, the UK's *Online Safety Act* includes a consideration about age assurance as part of its Likely to be accessed determination. Specifically, if a platform is sufficiently age gated, it 'exempts' the platform from having to implement additional child protection requirements to its service.[58]

Ofcom notes that:

"If children cannot normally access your service or part of it because you have highly effective age assurance and effective access controls in place, you do not need to (proceed in determining if your services is likely to be accessed). You can conclude that the service or that part of it is not likely to be accessed by children."

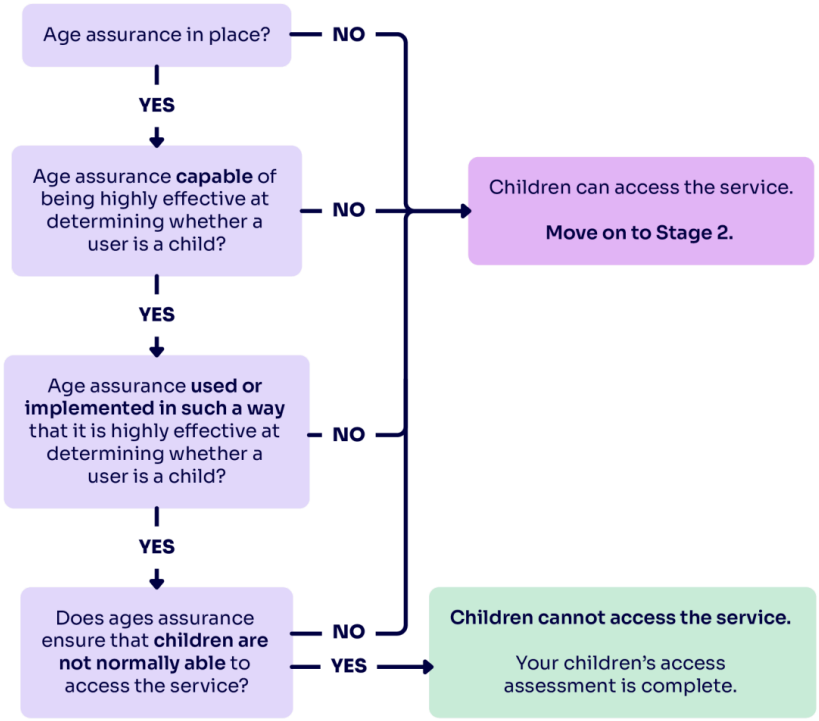
The diagram below notes how age assurance fits into the Children's Access Assessment test created by Ofcom for compliance with the 'Likely to be accessed' standard of the *Online Safety Act*.[59]



The requirements for age assessment are described in greater detail below, noting that age assurance is only necessary where platforms choose to claim exemption, on the basis that their service is not accessible to children.

[58]Ofcom 2025 *Children's Access Assessment* https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/childrens-access-assessments-guidance.pdf?v=395679

[59]Ofcom 2025 *Children's Access Assessment* https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/childrens-access-assessments-guidance.pdf?v=395679



We do not believe this approach is necessary in the COPC.

Appendix 3: Notes from a policy roundtable on the 'Likely to be accessed' standard and the COPC[60]

Summary

The Children's Online Privacy Code ('the Code') will establish a set of guidelines to improve children's privacy and will apply to social media services, relevant electronic services and designated internet services *where they are likely to be accessed by children* ('LTBA'). This briefing paper explores a discussion held by 13 experts from academia and civil society in July 2025 around how the 'likely to be accessed' standard might be operationalised in the Code.

It recommends that:

- The development of the LTBA standard should take a child rights based approach, and ensure that as much as possible, coverage matches the online services that children and young people use
- Any 'thresholds' included would consider children's rights as a priority and risks to their privacy if not met. Some existing understandings of 'likely' might create an expectation of a simple numeric threshold, and therefore not offer appropriate protections for rights
- The understanding of what 'use by a child' is should be expanded beyond the obvious situation where a child has actively chosen to use a service. Where a service uses a child's data, children should also be considered users of a service
- Frameworks for LTBA determinations could draw from the UK's *AADC* and Irish *Fundamentals*, and the evidence standards outlined in these jurisdictions.

The discussion outlined that:

- A US style 'actual knowledge test' disincentivises platforms from knowing the ages of their users, and opens up loopholes to avoid compliance
- The UK has two different types of LTBA-style determinations in operation:
    - The LTBA determination under the *AADC*: Platforms need to determine if their service is intended for use by children, or if not, if they are still accessed by or likely to attract children
    - The Children's Access Determination under the UK O*nline Safety Act*: Platforms need to determine if their service is accessible to children (i.e. if they prevent child access). If not, they must then consider if their platform is accessed by or is the type of service likely to attract children
- A LTBA standard in Australia could consider if a platform is directed at or intended for children, or if it is likely to be accessed based on whether there is evidence that either children use the service or it is the type of service likely to attract children. Australian data about these propositions is already available, and civil society could play a strong role in enhancing and scrutinising this data
- Children's rights are an important consideration to centre in these discussions. A well defined LTBA assessment can help advance children's rights, and consideration of children's rights could help to define any thresholds within a LTBA standard
- Discussion around thresholds needs to consider children's rights and risks to their rights to privacy. The concept of 'likely' has many potential interpretations available through existing law and jurisprudence, including some that might favour a simple numeric count of child-users in determining LTBA. This a risk-blind approach could overlook significant challenges posed to children's rights. There might be value in describing or quantifying these risks, to ensure these principles are still considered in any numeric calculations

[60]Reset.Tech Australia 2025 *Likely to be Accessed in the Children's Online Privacy Code* see https://au.reset.tech/work for publication in late early August 2025.

- There are two potential use-cases for the Code; one where children use a service, and the other where a service 'uses' a child. In both instances, children's right to privacy applies and should be protected. This might involve expanding the understanding of what 'use by a child' means, beyond the obvious situation where a child logs in and registers for an account. Where a service uses a child's data, children could also be considered users of a service
- There are some existing guidelines about what LTBA determinations could look like, derived from the UK's *AADC* and Irish *Fundamentals*, that might be applicable in the Australian context as well

Introduction to the policy roundtable on the 'Likely to be accessed' standard and the COPC

In late 2024, Parliament passed the *Privacy and Other Legislation Amendment Act 2024*. The bill set out to amend the *Privacy Act 1988 ('Privacy Act')* by, among other privacy-enhancing reforms, making provisions for the Office of the Australian Information Commissioner to draft a Children's Online Privacy Code ('the Code'). The Code will specify how online services accessed by children need to comply with the Australian Privacy Principles (the 'APPs'), and may also impose additional requirements provided they are not inconsistent with the APPs.

The Code will build on the definitions created by the *Online Safety Act* and apply to:

- Social Media Services
- Relevant electronic services (such as online multiplayer games and messaging apps) and
- Designated internet services (such as general entertainment, news or educational content services)

… *where they are likely to be accessed by children*. It will exclude health care providers and may cover additional classes of entities as determined by the Privacy Commissioner.

The 'Likely to be accessed' standard ('LTBA') has been widely used internationally. It is the standard for determination in:

- The UK's *Age Appropriate Design Code* (*'AADC'*) where it applies to "relevant information society services which are likely to be accessed by children"[61]
- The Irish *Fundamentals to a child-oriented approach to data processing*, (*'Fundamentals'*) which covers services directed at, intended for, or likely to be accessed by children[62]
- Some US State laws, such as the California *Age Appropriate Design Code*[63]
- The UK's *Online Safety Act*, which places additional safety requirements on platforms likely to be accessed, and outlines what a 'children's access assessment' looks like[64]

Most of the online platforms and services that will fall under the coverage of the Code will have experience in completing 'LTBA' assessments. This will help in providing evidence that is useful for the Australian context.

---

[61]UK Information Commissioner's Office *Age Appropriate Design Code* 2020 https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/,

[62]Ireland, Data Protection Commission 2021 *FundamentatIs for a Child Oriented Approach to Data Protection* https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf,

[63]California 2021 *The California Age-Appropriate Design Code Act* https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB2273&showamends=false

[64]Noting that given the differing nature of this law, and its broader application, the children's access assessment will differ from privacy focussed codes UK *Online Safety Act* 2023 https://www.legislation.gov.uk/ukpga/2023/50

Realising children's best interest requires a precautionary approach to the LTBA standard. If the aim of the Code is to enhance children's privacy, this requires maximising coverage which generally favours low thresholds for inclusion in the Code.

This policy briefing reflects discussions from a roundtable of 13 experts from academia and civil society held in July 2025. The group examined the concept of 'likely to be accessed' and how it might be applied in the context of the Children's Online Privacy Code. The event was conducted under the Chatham House Rule, meaning this briefing presents a summary of the discussion, without attributing specific comments. It began with three short provocations, outlined below, followed by a broader discussion and recommendations.

1. The US' 'actual knowledge' approaches to designation

The US' 1998 *Child Online Privacy Protection Act* ('*COPPA*')[65] aims to protect the data of children under 13, by requiring verifiable parental consent for its collection and processing, among other things.

It uses a different test for platforms to determine if a platform processes the data of under 13 year olds, and has to therefore comply with *COPPA*. There are two considerations for platforms to decide whether *COPPA* applies to them:

- A service has to be directed towards or targeted at children under 13, such as Sesame Street
- A service has to have actual knowledge of an under 13 year old accessing them

The 'actual knowledge' standard is designed to capture platforms that are general purpose, where adults may also use them or where they may not be targeted to under 13 year olds, but where 13 year olds may also be using them.

The 'actual knowledge' standard is different to a constructive knowledge standard, and in practice disincentivizes platforms from knowing the ages of their users.

This creates a loophole. If a platform sets a minimum age requirement of 13, and does no further investigations into the ages of users on their platforms and are not required to, they can claim to not knowingly process the data of children under 13. Therefore, they do not have to comply with *COPPA*. This often differs from advertising materials produced by platforms, which suggests they can reach under 13 year olds, but this is not the type of information *COPPA*'s standard requires.

There are parallels learnings to be made, given the *Online Safety Amendment (Social Media Minimum Age) Act 2024.* The implementation of the Act may lead to the presumption that data about children under 16 will not be processed by social media platforms, so the COPC need not apply to them. This will simply not be the case, as data about 16 & 17 year olds will still be collected, and 13 - 15 year olds might still use platforms without registering for an account. 'Actual knowledge' standards or claims that 'these platforms are no longer directed at children because of the minimum age requirements' are not sound.

An alternative to an 'actual knowledge standard' is a 'LTBA standard', where platforms are required to comply with privacy projections *where they are likely to be accessed by children.* This is starting to close the loopholes created by an actual knowledge standard, and therefore help bring more platforms in scope of privacy protections for children.

There are a number of types of evidence that could be useful in this regard:

[65]For the text of *COPPA*, see https://www.govinfo.gov/content/pkg/USCODE-2011-title15/html/USCODE-2011-title15-chap91.htm

- Research and survey evidence, and news reports, about children using platforms. It is harder for platforms to avoid research that younger children are using their platforms, when there is a LTBA standard involved
- Internal marketing and advertising materials created by platforms, which often point to an ability to 'target' younger children. This suggests that platforms know more about their user profiles, and their ages, than they are publicly suggesting. Again, this could come under scope as evidence under a LTBA standard

2. The UK's approach to 'Likely to be Accessed'

What are the obligations under the UK's AADC?

The UK's *AADC* applies to "information society services (ISS) likely to be accessed by children". It is explicitly designed to cover services that are both:

- Intended for and target children, and;
- Those not specifically targeted at children, but are nonetheless likely to be used by children.

The AADC places an obligation on platforms to undertake a LTBA determination, and if they are deemed LTBA, then they must apply the standards of the Code. The UK's Information Commissioner's Office (ICO) outlines that:

> *"If the nature, content or presentation of your service makes you think that children will want to use it, then you should conform to the standards in this code. If you have an existing service and children form a substantive and identifiable user group, the 'likely to be accessed by' definition will apply. Given the breadth of application, the ICO recognises that it will be possible to conform to this code in a risk-based and proportionate manner.*
>
> *If you decide that your service is not likely to be accessed by children and that you are therefore not going to implement the code then you should document and support your reasons for your decision. You may wish to refer to market research, current evidence on user behaviour, the user base of similar or existing services and service types and testing of access restriction measures.*
>
> *If you initially judge that the service is not likely to be accessed by children, but evidence later emerges that a significant number of children are in fact accessing your service, you will need to conform to the standards in this code or review your access restrictions if you do not think it is appropriate for children to use your service."*[66]

What are the 'tests' under the AADC?

In determining if a platform is likely to be accessed by children then, platforms need to consider if they are targeted to or directed at children, or if their service is likely to be accessed by a "significant number of children". A "significant number of children" means that the number of children accessing a service is material or non-trivial, meaning that children form a "substantive and identifiable user group" of a platform. This includes consideration of the number of people using the service; the number of the users who are likely to be children; and the data processing risks the service poses to children.

[66]ICO 2025 *Likely to be accessed' by children – FAQs, list of factors and case studies* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/

In assessing whether a platform is likely to attract a significant number of users, ICO guidance recommends a range of types of evidence that could be considered, from internal research, marketing materials or external research about platform users.

What are the obligations under the UK's *Online Safety Act?*

The UK's *Online Safety Act (UK OSA*) imposes a legal obligation on regulated online service providers to assess whether platforms are likely to be accessed by children under the age of 18. This requirement forms the basis of the child safety duties set out under Part 3 of the Act, which applies to all user-to-user and search services offering functionality that enables interaction between users.

Under the *UK OSA*, service providers must determine whether their platform falls within the scope of the child safety duties by carrying out a "suitable and sufficient" Children's Access Assessment.[67] If a provider fails to conduct a suitable and sufficient assessment, or conducts one inadequately, Ofcom — the designated regulator — will treat them as if the duties apply. Ofcom has enforcement powers to issue confirmation decisions and sanctions for non-compliance.

What are the 'tests' under the UK *OSA*?

The Children's Access Assessment considers whether it is possible for a child to normally access all or part of the service.[68] The *UK OSA* permits providers to conclude that children cannot access the service if they use 'highly effective' age verification or estimation techniques. Ofcom has defined these as technically accurate, robust, reliable and fair, including methods such as photo ID matching, facial age estimation, reusable digital ID services etc, but excluding self-declaration of age.

If the platform does *not* use highly effective age assurance, so that children can still access the service in principle, the next step is to determine whether the platform satisfies the child-user condition. This can be met in two ways:

- There is a significant number of children who are actual users of the service (or part of it); or
- The service is of a kind likely to attract a significant number of users who are children.

'Significant' for both these purposes is defined as significant in proportion to the total number of UK users. However, Ofcom have noted that a relatively small number of child-users may count as significant if the associated risk of harm is high. Ofcom has clarified that only age assurance data can reliably support a claim about the proportion of child-users.

Only if neither criterion is met can the provider conclude that the service does not fall within the scope of the act. Services must keep record of their assessments and are required to review them annually, or sooner if any substantial change is made to the service or there is a significant increase in child-users.

Alignment between the UK's *AADC* & *OSA*

Ofcom's approach aligns with the ICO's *AADC* (now called the Children's Code), which similarly requires platforms to consider whether they are likely to be accessed by children. Ofcom and the ICO have signed

[67]UK, Online Safety Act 2023 https://www.legislation.gov.uk/ukpga/2023/50/section/35/enacted
[68]Ofcom 2025 *Children's access assessments*
https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/childrens-access-assessments-guidance.pdf?v=395679

a Memorandum of Understanding[69] committing to information-sharing and coordinated regulatory oversight. While the Children's Code is focused on data privacy, the OSA is viewed as more stringent, with complex compliance obligations and stronger enforcement mechanisms.

Together these overlapping frameworks signal a clear direction, that children's safety duties are non-negotiable, and platforms must proactively assess and demonstrate how they meet these requirements.

3. What evidence is there for a LTBA assessment in Australia?

What could a 'LTBA' standard consider in Australia?

Building on the UK experience in the *AADC* and Irish experience under the *Fundamentals*, there is a version of the LTBA standard that is broad and widely used. Under this formulation, platforms would be considered likely to be accessed where they are:

1. *Likely to be accessed because they are directed to or intended for children, or*
2. *Likely to be accessed as demonstrated by either:*
    a. *Evidence that children's use of the service is more than de minimis or;*
    b. *It is the type of service that is likely to attract children.*

What data might be available? What could civil society do?

Evidence of children's use of a service — or in the formulation described above, part 2a — can come in many forms, and determining a threshold could require considerations of a range of evidence. The UK Information Commissioner's Office (ICO) *Likely to be Accessed Guidance*[70] provides a comprehensive starting place that would be applicable to Australian contexts, including:

- Data that platforms have about the number of users aged under 18 on their services in Australia. This will be largely internal, and we would be reliant on platforms to self-report this. As requirements for age assurance increase under the *Online Safety Act* and its Codes, we would expect this evidence to be increasing in volume and improving in accuracy.
- Research — internal or external from academics, market research, news stories etc — that suggests that Australian young people are using a service. This might include, for example, the annual survey undertaken by the Office of the eSafety Commissioner, the *Keeping Kids Safe Online* series,[71] but there could be an additional role for civil society in developing ongoing research in this area. We note here that evidence of effective age-gating aimed at 'keeping out' under 18 year olds could be submitted as evidence that a platform is not likely to be accessed by children, but that this would not be required by or apply to all services,
- Information used or created for advertising purposes, such as data available in the Real-Time Bidding system or other advertising codes that suggest users are children. This data is not routinely available to civil society, but has become so in the past as a result of whistleblowers and leaks.[72]

[69]UK Information Commissioner's Office 2024 *A Joint Statement by Ofcom and the Information Commissioner's Office on Collaboration on the Regulation of Online Services*
https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/05/a-joint-statement-by-ofcom-and-the-information-commissioner-s-office-on-collaboration-on-the-regulation-of-online-services/#:~:text=We%20have%20published%20a%20joint%20statement%20with%20Ofcom,interest%20to%20achieve%20a%20coherent%20approach%20to%20regulation.
[70]UK Information Commissioner's Office 2020 *Likely to be accessed by children*
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/
[71]Office of the eSafety Commissioner 2025 *The online experiences of children in Australia*
https://www.esafety.gov.au/research/the-online-experiences-of-children-in-australia
[72]See for example, the Xandr files leak documented in Reset.Tech Australia 2023 *Australians for Sale*
https://au.reset.tech/uploads/Reset.Tech-Report-Australians-for-Sale-2023.pdf

- Information received about complaints about child-users, or complaints from child-users. This will be largely internal, and we would be reliant on platforms to self-report. However, there may be value in organisations or entities that receive or engage with complaints from children directly to record details about the number of complaints received about each platform, to share with the OAIC for the purposes of informing a LTBA determination.

Evidence that the service is likely to attract children — or in the formulation above, part 2b — can also come in many forms, and could include considerations of the following examples;

- Use of the types of content, design features or activities which are likely to be attractive to children. Internal and external research can be useful in describing what this sort of content, features and activities are. There could be an additional role for civil society in developing ongoing research in this area.
- Whether children are known to access similar services. There could be an additional role for civil society in developing ongoing research in this area, to identify which services are similar and accessed by children.
- The business model of the company.
- If the company markets itself as having child-users.

Given the extensive use of the 'Likely to be accessed' standard internationally, it would be valuable to include as evidence in the Australian context, 'a previous determination that a service or part of a service is 'Likely to be accessed" in a similar determination as conducted in the UK under the *AADC* or *Online Safety Act*, or Ireland under the *Fundamentals*.

If the aim is to drive up privacy standards, and ensure compliance with proposed reasonable steps, measures to improve transparency — for regulators and the 'public' — and auditing this evidence should also be considered in the Code. Again, civil society could play a role in reviewing and auditing evidence produced as part of LTBA assessments, noting that this would be a new role civil society would need to be supported to take on.

Could we just set a numeric bar?

This raises a question about if we should have a straightforward numeric formula, i.e. if a platform has X many Australian children users, it is 'likely to be accessed'. While this idea has some appeal, it is rendered slightly unnecessary because the *Privacy and Other Legislation Amendment Act 2024* initially applies only to high-risk classes of entities. The *Act* did not seem to intend for there to be a high-bar for a numeric significance test precisely because it was designed for services that have high levels of privacy-risks inherently; social media, relevant electronic services and designated internet services, and other risky services as determined by the Privacy Commissioner.

Additionally, the guidance around the UK's *AADC* outlines that significant use from children does not require a large number of children to be using a service, nor that they must form a substantial proportion of users. It simply means that child-users must be more than a de minimis group.[73] Determining what is significant requires exploration of both the numbers of child-users *and* the risks posed to their data that this Code is intended to redress.[74]

[73]TaylorWessing 2024 *Likely to be accessed* https://www.taylorwessing.com/en/global-data-hub/2024/february---childrens-data/likely-to-be-accessed-by-children

[74]As a further caution against the notion of using a numeric measure of significance alone; the population of Australian children aged under 18 is small. There are around 5.7m children aged 0-17 (UNICEF 2023 *How Many Children are there in Australia?* https://data.unicef.org/how-many/how-many-children-under-18-are-there-in-australia/) which works out around 335,000 children in each year of age if evenly divided. This means numerically low levels of use could still represent a sizable portion of Australia's age cohorts. For example, it would still be possible for a platform to reach half Australian 16 & 17 year olds (which would be huge market penetration), while failing to reach a 0.5m threshold.

What about age-assurance? How will platforms know that a user is a child?

Pre-existing mechanisms and knowledge that platforms already hold should be sufficient to determine who might be a child-user for the purposes of the Code, such as self-reported date-of-birth data provided at registration, other pre-existing age assurance mechanisms (that are increasing in use already) and data about user behaviour that they already process. Compliance with other regulations internationally is increasingly driving a need for more effective age assurance measures; the Code will benefit from this, but it does not need to contribute to this.

This raises the common question 'but how do platforms know if the data belongs to a child'? We believe there is a relatively straight forward solution to this, learning from the Irish *Fundamentals*:

- For platforms that are directed to or intended for children, platforms should simply assume all user data is children's data and apply the requirements in the Code. (Barring obvious exceptions, for example where they allow parents or teachers to hold a linked account, or parents' credit card data).
- For platforms that are general use, and have adult and child-users, where a user has self-identified as a child, or the platform suspects they are a child through any other already in place age assurance mechanism, the platform should *assume* that data is children's data.

The principles within the Code, and broader privacy-by-design settings, should apply to platforms where this is the case. This raises the question about 'what to do about children who fib about their age online and pretend to be over 18?, and how we specifically protect their data or accounts':

- Where a user has identified that they are an adult but a platform has *any conflicting data* that raises suspicions that they are a child, the platform should err on the side of caution and treat that data as children's data. There are no 'downsides' to having additional privacy protections applied if in doubt. Suspicions about 'adults who might actually be children' can be, and are already, derived from existing forms of age assurance such as analysis of their online behaviour or other age assurance mechanisms. Where a platform genuinely has no reason to suspect a user is a child, they can treat the data as adult data.

We are aware that a few children-who-fib may go unprotected as a result of being undetected, in which case, they will have the same levels of privacy protection as they currently do, while still benefitting from overall principles based protection applied to platforms overall. This will be an ever diminishing number of children, as requirements for age assurance from other regulations — both Australian and international — drive age detection across many platforms.

There is no perfect solution for this, but perfect need not be the enemy of the good and proportionality is key. There are many problems in the online world for children and this Code cannot and will not fix all of them, nor could it be reasonably expected to.

Discussion from a policy roundtable on the 'Likely to be accessed' standard and the COPC

The discussion focused on 4 key themes.

The importance of children's rights

A well defined LTBA assessment can help advance children's rights. Children's rights exist in the online environment, meaning that they are entitled to protections across the digital world, wherever they are or

wherever they are 'likely to go' online. If we start from the perspective of the Code enhancing children's rights to privacy, then a broad coverage from a LTBA assessment is desirable.

This child-centric approach is demonstrated in the UK's *AADC*. One of the 'wins' of this Code was that default moved from 'needing to demonstrate that children are the primary users of an app to ensure regulatory standards apply' to 'making sure that a service is protective of children, even if children aren't targeted as the primary users of a service'. That is, protections were extended to travel across the digital world to include the services children use, not just the services they are 'expected' to use.

Civil society organisations could have a role to play in both confirming and shaping this understanding, by documenting where children are or are likely to go online, but also by exploring other factors such as where risks to their rights exist online.

Thresholds cannot be numeric alone

When thinking through a LTBA determination, it's important to remember that 'likely' has many potential interpretations available through existing law and jurisprudence (see addendum below). This is worth considering while discussions about thresholds within a LTBA determination are ongoing.

Unless there is clarity, there could be a situation where a court or regulator chooses to create a numeric threshold alone. Given this possibility, it might be useful to document considerations around 'risks' to children's privacy, how to measure these, and how these could be weighted within a LTBA determination. This might lead to some sort of actuarial approach — or 'real options' — to correct for the shortfalls of a numeric threshold, but this takes us further away from a principle based approach.

However, if an issue was taken to court around a LTBA determination, existing interpretations of the concept of 'likelihood' would be relevant, but not necessarily binding. Requiring compliance with Convention on the Rights of the Child could be considered, especially where there is any ambiguity. In short, any attempts to develop a numeric threshold would need to consider risks to children's rights as well, and this would ideally be considered in guidance from the OIAC.

What counts as a 'user'?

The Code applies to all children under 18, but there are two distinct use-cases within that scope; one where children use a service, and; another where a service 'uses' a child (or more specifically, their data).

In the latter case, defining a child as a user of a service might not align with lay definitions of a service user. Put plainly, there are plenty of digital products that collect, use or disclose children's data or images, where children do not actively login and register for an account, and this challenges the plain language understanding of a 'user of a platform'.

A broader understanding of the word 'user' was surfaced by interrogating products like childcare apps. With these products, the user that 'signs on to the service' is most often a parent, but they are still designed for and intended to facilitate the collection, use and disclosure of significant amounts of children's data, such as images of children. Under a broader formulation of a 'user', these sorts of products are more likely to meet the LTBA test in the same way, if they are included in scope. For example, a child care app would be considered targeted at or directed to children (because they are designed to share photos of children), and additionally, they may be considered the type of service that is likely to attract child 'users'.

While the final scope of the Code is as yet undetermined, there is an argument for including these apps if a 'user' is considered more broadly to include 'data subject'. This would encourage a broader principles based approach to protection, rather than a narrow form of use.

What could we borrow from other jurisdictions?

There was a discussion about the guidance that will have been produced in other jurisdictions, and an understanding that we should learn from these in the Australian context.

There are learnings that could be taken from:

- Guidance from the UK around the *AADC*[75]
- Section 3.1 of the Irish *Fundamentals*[76]
- Guidance around the 'Children's Access Assessments' under the UK's *Online Safety Act*, noting that this will be different in substance to the Australian Code[77]

There was an understanding that this guidance could be used as a spring board for Australia, to give us initial models of a LTBA determination for consideration. They can be further enhanced by additional research and an active consideration of children's rights, including the views and experience of children and young people themselves.

Recommendations from a policy roundtable on the 'Likely to be accessed' standard and the COPC

- The development of the LTBA standard should take a child rights based approach, and ensure that as much as possible, coverage matches the online services that children and young people use
- Any thresholds included would also need to consider children's rights and risks to their privacy. Some existing understandings of 'likely' might create an expectation of a simple numeric threshold, but these would need to be balanced against rights considerations
- The understanding of what is 'use by a child' could be expanded beyond the obvious situation where a child has actively chosen to use a service. Where a service uses a child's data, children could also be considered users of a service
- Frameworks for LTBA determinations could draw from the UK's *AADC* and Irish *Fundamentals*, and the evidence standards outlined in these jurisdictions.

Australian jurisprudence on 'likely' (Addendum)

A long and settled line of authority in Australian jurisprudence, particularly in the context of the *Competition and Consumer Act 2010* (Cth), has firmly established that "likely" does not mean "more probable than not" (that is, a probability greater than 50%). Instead, the settled judicial interpretation is that "likely" denotes a "real chance or possibility" that is substantive and not merely "fanciful or remote".[78]

---

[75]ICO 2025 *Likely to be accessed' by children – FAQs, list of factors and case studies* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/

[76](Irish) Data Protection Commission 2021 *Fundamentals for a Child Oriented Approach to Data Processing* https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf

[77]Ofcom 2025 *Children's access assessments* https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/childrens-access-assessments-guidance.pdf?v=395679

[78]*ACCC v Metcash Trading Ltd*, 2011 and Ian Wylie 2012 'What is "likely" in the Competition and Consumer Act 2010?' *Competition and Consumer Law Journal*, *20*, 28

This interpretation has been consistently applied across diverse legal domains. The Australian Law Reform Commission (ALRC), for instance, has suggested that "likely" in the context of causing harm should mean "a real possibility, a possibility that cannot sensibly be ignored having regard to the nature and gravity of the feared harm in the particular case")[79]. Adopting this "real chance" test for the Code sets a threshold that is substantive but appropriately low, consistent with the protective objects of the enabling legislation.

Under the "real chance" test, the OAIC would not be required to prove that children constitute a majority, or even a substantial minority, of a service's user base. The evidentiary burden would be to demonstrate, on the balance of probabilities, that there is a non-trivial possibility that children access the service. This aligns with the legislative intent to place a proactive obligation on platforms to consider the possibility of child access based on a realistic assessment of their service's appeal and context, rather than allowing them to shelter behind a narrow definition of their intended adult audience.

The following table consolidates the application of the "real chance" test across various legal contexts, providing an authoritative basis for its adoption in the Code's guidelines.

Term/ Phrase	**Source/ Context**	**Leading Case/Authority**	**Judicial Definition**	**Implied Probability**
Likely	Competition and Consumer Act 2010 (Cth) (s. 50 - mergers)	*ACCC v Metcash Trading Ltd* FCAFC 151	A real chance or possibility; something that is not remote or fanciful.	Substantially less than 50%
Likely	Statutory tort for invasion of privacy (ALRC proposal)	ALRC Discussion Paper 80 (2014)	A real possibility, a possibility that cannot sensibly be ignored having regard to the nature and gravity of the feared harm.	Less than probable; context-dependent on harm
Reasonably Likely	Commonwealth Ombudsman (Defence/VET Student Loans)	Citing *Dept. of Agriculture v Binnie* VR 836	A chance which is real — not fanciful or remote. A chance described as 'reasonable' is one that is 'sufficient' or 'worth noting'.	Less definite than probable
Likely to result in	Victoria Legal Aid Guidelines (sentencing)	VLA Handbook	The actual penalty the person would expect, based on all circumstances.	An expectation, not a mathematic al probability

[79]Australian Law Reform Commission, 2014 *Serious Invasions of Privacy in the Digital Era* (DP 80), p. 1

Appendix 4: Notes from a policy roundtable on targeted advertising and the COPC[80]

Summary of the roundtable on targeted advertising and the COPC

The Children's Online Privacy Code ('the Code') is widely expected to address a range of privacy issues for children, including targeted advertising. This briefing paper explores a discussion held by 21 experts from academia and civil society in June 2025 around how the Code might address targeted advertising.

It recommends that:

- The Code addresses the 'data processes' involved in targeted advertising. This includes data collection, use, and disclosure, along with other aspects inherent to targeted advertising that cuts across multiple Australian Privacy Principles (APPs).
- The Code offers a strong remedy, such as prohibiting or presuming against the collection, use or disclosure of data to enable targeted advertising.
- Strong requirements for transparency — including regulator transparency and public transparency — be implemented within the Code itself.

The discussion outlined that:

- Targeted advertising is a violation of children's rights because of the data handling process it involves. The Children's Online Privacy Code would be well placed to prohibit this practice on privacy grounds.
- Targeted advertising creates a risk environment for young people and places them in danger of harm. Even if this process is occasionally used to promote positive advertising, this overall risk profile would justify prohibiting the use of children's data to fuel this practice in the Code.
- Multiple jurisdictions have presumed against the practice in comparable children's data codes. The UK, Ireland and the EU have used data protection laws to create a presumption against targeted advertising by outlining that children should not be profiled. The EU has dovetailed this with a broader prohibition under the *Digital Services Act*.
- A major mismatch exists between how the digital economy currently functions and what Australians deserve and want. Extensive research shows that Australians are uncomfortable with the practices of targeted advertising.
- The process of targeted advertising involves a pipeline of data handling practices, including the collection, use and disclosure of data, as well as automated profiling. This means that there are multiple ways a Code could address targeted advertising, and a pipeline-wide approach would be desirable.
- There is a broader need for transparency and accountability within the Code. Without this, non-compliance or malicious-compliance could become commonplace.
- Ultimately, this is a question of 'the business model'; can protecting children's privacy create a way to lift children out of the current rights-violative approach?

[80]Reset.Tech Australia 2025 *Targeted advertising and the Children's Online Privacy Code* https://au.reset.tech/news/targeted-advertising-the-children-s-online-privacy-code/

Introduction for the roundtable on targeted advertising and the COPC

In late 2024, Parliament passed the *Privacy and Other Legislation Amendment Act 2024*. The bill set out to amend the *Privacy Act 1988 ('Privacy Act')* by, among other privacy-enhancing reforms, making provisions for the Office of the Australian Information Commissioner to draft a Children's Online Privacy Code ('the Code'). The Code will specify how online services accessed by children need to comply with the Australian Privacy Principles (the 'APPs'), and may also impose additional requirements provided they are not inconsistent with the APPs.

The Code is expected to address a range of concerns regarding children's privacy in an online world, including the collection, use and disclosure of children's data for targeted advertising purposes. This briefing paper explores how the Code might address targeted advertising practices.

Issues around targeted advertising are often conflated with concerns around advertising in general or with issues around the content of advertising. As section 1 of this report outlines, these are valid concerns, but they are not the same as those raised by *targeted* advertising specifically. Although Australian law does not define targeted advertising, many model definitions exist internationally, and a useful working definition can be developed from proposals from the Attorney General's Department:

> *Targeting – capture the collection, use or disclosure of information which relates to an individual including personal information, deidentified information, and unidentified information (internet history/tracking etc.) for tailoring services, content, information, advertisements or offers provided to or withheld from an individual (either on their own, or as a member of some group or class).*[81]

Targeted advertising is the use of this data heavy *process* to deliver advertising. It is sometimes referred to as behavioural advertising or stalker advertising, and involves more than just delivering personalised ads to children. As a process, it involves multiple concerning data handling practices, such as:

- The widespread collection of excessive amounts of data about users' behaviour, including that of children.[82] Data minimisation does not appear inherent to this process. Companies collect and analyse granular information; from how long users hover over a video before swiping on, to whether they downloaded a mental health app last week. It is unclear whether young people meaningfully consent to these practices,[83] and other questions arise around data use, such as necessity, purpose limitation, and transparent notification.
- The use of this data to create an automated profile of a user for the purpose of delivering personalised advertising.[84] These automated profiles are most often created by international companies, with no human oversight or 'humans in the loop'.
- Finally, the delivery of an advertisement to a user. Both the content of the ad and the timing of the ad delivery are informed by data profiling, often in concerning ways. The Real-Time Bidding (RTB) process — the technical system that allows automated placement of ads in

[81] Attorney General's Department 2022 *Privacy Act Review Report* https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

[82] Reset.Tech Australia 2024 *Australians for Sale: Targeted Advertising, Data Brokering and Consumer Manipulation* https://au.reset.tech/news/coming-soon-australians-for-sale-report/

[83] Reset.Tech Australia 2021 *Did we really consent to this?* https://au.reset.tech/news/did-we-really-consent-to-this-terms-and-conditions-young-people-s-data/

[84] See for example Reset.Tech Australia 2021 *Profiling Children for Advertising* https://au.reset.tech/news/profiling-children-for-advertising-facebooks-monetisation-of-young-peoples-personal-data/). Meta, the core example in this report, subsequently claimed to turn off the ability for advertising to reach children through profiling, which was a misleading claim (see Reset.Tech Australia 2021 *Facebook still misusing young people's data* https://au.reset.tech/news/facebook-caught-red-handed-harvesting-teens-data/), a statement they had to correct on record in the US Senate after being presented with this research (available on C-SPAN 2021 *Senate Committee Hearing on Online Protections for Children* https://www.c-span.org/program/senate-committee/senate-hearing-on-online-protections-for-children/605914) or as Sarah Wynn-Williams describes it a "devised cover-up" and a "flat out lie" (in Sarah Wynn-Williams 2025 *Careless People* Macmillan, London)

children's feeds — raises significant concerns about data disclosures. For example, anyone with access to the RTB system can see live profile data at an alarming rate, such as the live location data of an Australian, which is broadcast on average 449 times per day.[85]

Targeted advertising sits at the core of the business model of surveillance capitalism,[86] and most large online platforms.

Issues around targeted advertising are broader than those related to direct marketing, which is addressed under APP 7. Rather, targeted advertising intersects with a wider range of APPs. For example:

- APP 1 — concerning the transparency and openness of the process. APP 1 requires companies to be open and transparent about how they collect and use personal information.
- APP 3 — relating to the way children's data is collected. APP 3.3 outlines that that information collected must be reasonably necessary for the company's functions, and that sensitive information can only be collected with consent.
- APP 6 — governing how data is used. APP 6.1 outlines that a company may only use or disclose personal information for the same purpose as they collected it.
- APP 8 — addressing cross-border flows of information. APP 8 requires companies to ensure that before transferring data overseas, steps are taken to ensure overseas data handlers comply with the APPs.
- APP 11— regarding the security of personal information. APP 11.1 requires companies to take reasonable steps to protect the information from misuse, interference and loss, as well as from unauthorised access, modification or disclosure.

This policy briefing reflects discussions from a roundtable of 21 experts from academia and civil society held in June 2025. The group examined the implications of targeted advertising and how the Children's Online Privacy Code might be able to address this. The event was conducted under the Chatham House Rule, meaning this briefing presents a summary of the discussion, without attributing specific comments. It began with three short provocations, outlined below, followed by a broader discussion and recommendations.

1. Targeted advertising as a privacy violation and harm

Different debates about advertising and young people

The relationship between children and advertising is often considered problematic in a number of ways. However, not all of these problems stem from *targeted* advertising, nor do all find a remedy in privacy policy. This problem landscape is often confused and conflated, so for the purposes of clarity, we present below a short tripartite typology of this landscape. In reality, these landscapes are interconnected and the boundaries between them are not distinct, however they can still be separated into three conceptual areas:

1. Concerns about the effects of advertising overall on children. These debates draw on an old and rich field of media effects studies, which aim to explore what the impact of media consumption is on individuals.[87] When it comes to children specifically, debates exist around the role of advertising in

[85]ICCL 2024 *Australia's Hidden Security Crisis* https://www.iccl.ie/digital-data/australias-hidden-security-crisis/
[86]See Donnell Holloway 2019 'Surveillance capitalism and children's data: the Internet of toys and things for children' *Media International Australia*, *170*(1), pp. 27-36. https://doi.org/10.1177/1329878X19828205
[87]See for example, Patti M. Valkenburg, Jochen Peter, and Joseph Walther 2016 'Media Effects: Theory and Research' *Annual Review of Psychology Research* https://doi.org/10.1146/annurev-psych-122414-033608

promoting on materialism,[88] causing economic harms such as excessive spending,[89] and contributing to climate change.[90] This is a debate about the value or harm of advertising as a societal phenomenon. The solutions to these broader issues largely sit outside the scope of privacy and data protection policy.

2. Harms from specific advertising (or framed in positively, ethical advertisements and placements). Concerns exist about potential harms associated with the content of particular advertising, such as ads for alcohol,[91] junk food,[92] gambling,[93] indoor tanning,[94] etc. There are also debates about the placement of advertising, such as age-appropriate ads during major sporting events or within 'watersheds' periods. These are important discussions about the advertising content and children's exposure to them, and are often addressed through advertising standards and codes and broadcast laws.

3. The process of targeting ads to children. This discussion — explored below — concerns the impact of targeted advertising as a data-heavy process on children. It is content neutral. That is, it is not necessarily concerned with the content of the ads, nor with their effect on consumers, but focuses on the privacy rights of children. As a metaphor to help differentiate between these debates, this discussion is about what happens to data "behind the screens", rather than what appears on the screens (i.e. which ads are broadcast), or what happens to the viewer after seeing an ad (i.e. media effects). It is a systems focussed approach, drawing attention to how data is inappropriately collected, used and disclosed to drive advertising delivery.

Targeted advertising as a rights violation

The process of targeting ads to children is a violation of their privacy rights as expressed under numerous international instruments. Advancing children's rights in Australia requires prohibiting targeted advertising.

Article 16 of the *Convention on the Rights of the Child* ensures children the right to privacy, outlining that 'no child shall be subjected to arbitrary or unlawful interference with his or her privacy.' The *General Comment on Children's Rights in Relation to the Digital Environment* is the codicil to the Convention that explains how children's rights translate to the digital world. It outlines that realising children's right to privacy requires that 'States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling.'[95]

[88]Usha Lenka Vandana 2014 'A Review on the Role of Media in Increasing Materialism among Children' *Procedia - Social and Behavioral Sciences* https://doi.org/10.1016/j.sbspro.2014.04.212
[89]Juliet B. Schor 2004 *Born to buy* Scribner, London
[90]Global Action Plan 2022 *Big Tech's Dirty Secret* https://www.globalactionplan.org.uk/files/big_tech_report.pdf
[91]Susan Martin, Leslie Snyder, Mark Hamilton, Fran Fleming-Milici, Michael Slater, Alan Stacy, Meng-Jinn Chen and Joel Grube 2006 'Alcohol Advertising and Youth' *Alcohol Clinical and Experimental Research* https://doi.org/10.1111/j.1530-0277.2002.tb02620.x
[92]Bridget Kelly, Rebecca Bosward, Becky Freeman 2021 'Australian Children's Exposure to, and Engagement With, Web-Based Marketing of Food and Drink Brands' *Journal of Medical Internet Researc*h https://doi.org/10.2196/28144
[93]Hannah Pitt, Samantha Thomas, Amy Bestman, Melissa Stoneham and Mike Daube 2016 "'It's just everywhere!" Children and parents discuss the marketing of sports wagering in Australia' *Australian and New Zealand Journal of Public Health* https://doi.org/10.1111/1753-6405.12564
[94]Jenny Radesky, Yolanda Reid Chassiakos, Nusheen Ameenuddin and Dipesh Navsar 2020 'Digital Advertising to Children' *Pediatrics* https://doi.org/10.1542/peds.2020-1681
[95]United Nations Committed on the Rights of the Child 2021 *General comment No. 25 (2021) on children's rights in relation to the digital environment* https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=fT3nx%2FKEyjPie59GG8iHdDugSg7GO4Dn9%2BWkWC%2Fa8TLwKtEAuEF1HM7qW2BzwAImZaR0aN5pTFnoVkzMYkxYKQ%3D%3D, Para 42

UNICEF has also noted the distinction between advertising and targeted advertising, stating that the latter violates children's rights: 'Many data collection practices happen without children's knowledge, consent (and without effective control). The result is that children's privacy is repeatedly breached.'[96]

There are many aspects of the process of targeted advertising that make it inherently incompatible with children's rights to privacy, such as:

- The arbitrary nature through which digital companies engage in surveillance, without effective oversight or due diligence. The *General Comment* notes that 'Digital practices, such as automated data processing, profiling, behavioural targeting, (etc…) are becoming routine. Such practices may lead to arbitrary or unlawful interference with children's right to privacy.'[97]
- The lack of consent and autonomy it offers young people. The *General Comment* notes that 'Any digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy and should not be conducted routinely, indiscriminately or without the child's knowledge, nor should it take place without the right to object to such surveillance.'[98]
- The absence of data minimisation involved in the process. The *General Comment* notes that 'in commercial settings and educational and care settings, and consideration should always be given to the least privacy-intrusive means available to fulfil the desired purpose.'[99]

No matter the ad, no matter the time of day it appears, nor the impact on the consumer, targeted advertising is a violation of children's rights because of the process it involves. The Children's Online Privacy Code would be well placed to prohibit this practice on privacy grounds.

Targeted advertising as a 'harm'

For those less familiar with a rights-based approach, who may feel more comfortable with a harm- or health-focussed approach to calling for a prohibition, Citron & Solove[100] developed a typology of 'privacy harms' that are cognisable to courts and regulators. The process of targeting advertising at children creates risks around these privacy harms:

- **Psychological harm**: which 'involve(s) a range of negative mental responses, such as anxiety, anguish, concern, irritation, disruption, or aggravation'[101] are generally broken up into two types by regulators; emotional distress and disturbance. Distress involves feeling pain or unpleasantness, while disturbance involves disruption to tranquility and peace of mind.[102] Targeted advertising causes both distress and disruption to tranquility. For example, young people talk about feeling shocked at how targeted some ads are, and worried about whether their phones are listening to them[103] (a type of

[96]Carly Nyst 2019 *Children and Digital Marketing: Rights, risks and opportunities* UNICEF https://www.unicef.org/childrightsandbusiness/media/256/file/Discussion-Paper-Digital-Marketing.pdf
[97]United Nations Committed on the Rights of the Child 2021 *General comment No. 25 (2021) on children's rights in relation to the digital environment* https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=fT3nx%2FKEyjPie59GG8iHdDugSg7GO4Dn9%2BWkWC%2Fa8TLwKtEAuEF1HM7qW2BzwAlmZaR0aN5pTFnoVkzMYkxYKQ%3D%3D, Para 68
[98]United Nations Committed on the Rights of the Child 2021 *General comment No. 25 (2021) on children's rights in relation to the digital environment* https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=fT3nx%2FKEyjPie59GG8iHdDugSg7GO4Dn9%2BWkWC%2Fa8TLwKtEAuEF1HM7qW2BzwAlmZaR0aN5pTFnoVkzMYkxYKQ%3D%3D, Para 75
[99]United Nations Committed on the Rights of the Child 2021 *General comment No. 25 (2021) on children's rights in relation to the digital environment* https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=fT3nx%2FKEyjPie59GG8iHdDugSg7GO4Dn9%2BWkWC%2Fa8TLwKtEAuEF1HM7qW2BzwAlmZaR0aN5pTFnoVkzMYkxYKQ%3D%3D, Para 75
[100]Danielle Citron & Daniel Solove 2021 'Privacy Harms' *Boston University Law Review*, 837 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222
[101]Danielle Citron & Daniel Solove 2021 'Privacy Harms' *Boston University Law Review*, 837 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222, pp 841
[102]Danielle Citron & Daniel Solove 2021 'Privacy Harms' *Boston University Law Review*, 837 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222, pp 841-44
[103]Reset.Tech Australia & the CREATE Foundation 2025 *Consultation with young people about the*

distress), and feeling that these ads are invasive and 'up in their faces' (a disruption to their digital tranquility).[104] There is no need to 'prove' a causal relation to mental health diagnoses to talk about the psychological harms of targeted advertising; interferences with peace of mind and feeling upset can be characterised as a cognisable psychological harm for regulators.

- **Physical harm**, or significant harms that 'result in bodily injury or death.'[105] The process of targeting young people who may be particularly vulnerable, such as being able to target teens interested in weight loss or feeling depressed, creates real risk for physical harm.[106] What might be a benign product for one young person can, if targeted unsafely, create risks for others. For example, workout content can be great for most young people, but if deliberately targeted to those with body dysmorphia, it can cause harm.
- **Relationship harm** occurs when relationships 'that are important for one's health, well-being, life activities, and functioning in society' are damaged, including inter-family conflict. If parents and children are bickering or arguing about the impact or purchase of products, services or game upgrades prompted to them via targeting, this constitutes relationship harm.
- **Economic harm,** or harms involving monetary losses or a loss in the value of something. Targeted advertising allows the precise delivery of scam ads, which affect young people.
- **Discrimination**, or acts and practices that entrench inequality and disadvantage people based on protected characteristics. Targeted advertising reaches young people based on behavioural data that is often correlated with demographics and protected characteristics. This can produce discriminatory effects. For example, ads for university open days will reach different young people than ads for military recruitment' a process that will be algorithmically refined until it becomes more and more effective.
- **Autonomy harm,** which 'involve(s) restricting, undermining, inhibiting, or unduly influencing people's choices.'[107] Autonomy harms prevent people from making choices that realise their preferences, trick them or deny them the freedom to decide for themselves. The persistent and selective nature of targeted advertising ensures an unbalanced presentation of consumer information. This affects autonomy.
- **Reputational harm** is where an 'individual's reputation and standing in the community' has been injured. There are fewer examples connecting reputational harms and targeted advertising for children, but they do exist in the digital world. For example, when someone hacks a child's account and assumes their identity for example, this can cause reputational harm.

Targeted advertising creates a risk environment for young people and places them in danger of harm. Even if this process is occasionally used to promote positive advertising, the balance of this risk would justify a prohibition on using children's data to fuel this practice in the Children's Online Privacy Code.

2.How other jurisdictions deal with targeted advertising and children

How Ireland handles targeted advertising and children

The Irish *Fundamentals for a Child-Oriented Approach to Data Protection* ('the Fundamentals') is clear in stating that there is a presumption against using children's data to deliver targeted advertising. It notes:

Children's Online Privacy Code and the right to access, correct or delete data forthcoming

[104]See for example, Rys Farthing, Katya Koren Ošljak, Teki Akuetteh, Kadian Camacho, Genevieve Smith-Nunes & Jun Zhao, J. 2024 'Online Privacy, Young People, and Datafication: Different Perceptions About Online Privacy' *Social Media + Society*, *10*(4). https://doi.org/10.1177/20563051241298042 or Reset.Tech Australia 2024 *Young People and Online Privacy* https://au.reset.tech/uploads/For-Print-Final-report.pdf

[105]Danielle Citron & Daniel Solove 2021 'Privacy Harms' *Boston University Law Review*, 837 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222, pp. 831

[106]See Sarah Wyn-Williams 2025 *Careless People* Macmillan, London

[107]Danielle Citron & Daniel Solove 2021 'Privacy Harms' *Boston University Law Review*, 837 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222, pp. 845

> *Organisations should not profile children, engage in automated decision-making concerning children, or otherwise use their personal data, for advertising/marketing purposes, unless they can clearly demonstrate how and why it is in the best interests of children to do so.*[108]

The *Fundamentals* adopts a zero interference approach in relation to the best interests of the child.

The authors of the *Fundamentals* — the Data Protection Commission ('DPC') — make it very clear that they do not consider it in the best interests of children to be shown advertisements for games, services, products or content where such advertisements are based on profiling.[109] Accordingly, a high burden of proof is placed on organisations to demonstrate how processing children's personal data for the purposes of profiling and/or automated decision making for advertising is in children's best interests. The DPC therefore considers that there will be a very limited range of circumstances in which the profiling of children and/or the use of automated decision-making concerning them are legitimate and lawful activities under the *General Data Protection Regulation* (GDPR). One example of a possible exception is the use of such measures to protect a child's welfare.

This position builds on a European Data Protection Board stipulation — based on the GDPR — that solely automated decision-making, including profiling, which produces legal or similar effects should not be used for children.[110] The *Fundamentals* addresses the process of automated profiling inherent in targeted advertising and outlines that this should not occur.

If an organisation decides to profile and/or engage in automated decision-making about children for any purpose, it must first carry out a data protection impact assessment (DPIA) to assess whether the processing will result in a high risk to the rights and freedoms of children. The best interests of the child must be a critically considered factor in conducting a DPIA involving children's personal data[111].

The *Fundamentals* also notes that there is a difference between targeted advertising and other forms of direct marketing. This allows for the possibility that some direct marketing may be in the legitimate interests of a business and also in the best interests of a child, such as where a child aged 16 or over has signed up to receive ads and deals directly. However even in such cases, the Irish 'Code' still places the onus of responsibility on the company: '*Should organisations decide to conduct electronic direct marketing activities towards children, they should be able to demonstrate how this is in the best interests of the child, irrespective of any business model or commercial interests of the organisation*.'[112]

Examples of situations where direct marketing may be used to positively promote the best interests of children include direct marketing for counselling or support services; educational, health and social

---

[108]Data Protection Commission 2021 *Fundamentals for a Child Oriented Approach to Data Protection* https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf, pg 57

[109]Data Protection Commission 2021 *Fundamentals for a Child Oriented Approach to Data Protection* https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf, pg 57.

[110]European Commission 2016 *General Data Protection Regulation* https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng. Recital 71 states that '"solely automated decision-making […] with legal or similarly significant effects […] should not concern a child'. Exceptions to this rule should remain under limited circumstances, such as where it is necessary "to protect their welfare". From the Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679: 'There may nevertheless be some circumstances in which it is necessary for controllers to carry out solely automated decision-making, including profiling, with legal or similarly significant effects in relation to children, for example to protect their welfare. EDPB 2018 *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* https://ec.europa.eu/newsroom/article29/items/612053/en

[111]Data Protection Commission 2021 *Fundamentals for a Child Oriented Approach to Data Protection* https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf, pg 7.

[112]Data Protection Commission 2021 *Fundamentals for a Child Oriented Approach to Data Protection* https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf, pg 54

services; and advocacy and representative organisations. Otherwise, there is generally a presumption that such marketing is not in children's best interests.

Interestingly, the DPC also offers reflections on a harm-based approach to advertising. It notes '*Many parents object to the idea of children being targeted with, for example, fast food advertisements on online sites. However such contextual advertising needs to be regulated through advertising standards rather than the GDPR as these advertisements aren't tailored based on personal data*.'[113]

How the EU handle targeted advertising and children

Ireland is part of the European Union, so the Irish Code draws heavily from the EU's GDPR. However, it's worth noting a few other developments that will apply across Europe as well.

Recital 38 of the GDPR states that children's data warrants special protection, positioning children as potentially more vulnerable to risks and less aware of their rights. Recital 71 GDPR provides that children should not be subject to decision-making based solely on automated processing, including profiling, which encompasses commercial profiling for advertising purposes.

Further, in their 2013 Opinion on Apps on Smart Devices, the European Data Protection Board (EDPB) — or more correctly, their predecessor, the Article 29 Working Party — stipulated that, in the best interests of the child, companies '*should not process children's personal data for behavioural advertising purposes, neither directly nor indirectly, as this will be outside the scope of a child's understanding and therefore exceed the boundaries of lawful processing.*'[114]

The EDPB has reiterated this principle in its guidelines on automated individual decision-making and profiling and states that organisations should, in general, avoid profiling children for marketing purposes, due to their particular vulnerability and susceptibility to behavioural advertising.[115] This is especially relevant in the contexts of online games and other information society services that use profiling to identify users who can be encouraged to spend more money. The Council of Europe has also expressed similar views, stating:

> *Profiling of children should be prohibited by law. In exceptional circumstances, states may lift this restriction when it is in the best interests of the child or if there is an overriding public interest, on the condition that appropriate safeguards are provided for by law.*[116]

Incidentally, it's worth noting that the EU's *Digital Services Act* (DSA) goes one step further for clarity, outlining an unambiguous presumption against targeted advertising to individuals aged under 18. The DSA is not rooted in data protection law, but is a broader regulatory instrument, however Recital 71 reinforces the GDPR and states:

---

[113]Data Protection Commission 2021 *Fundamentals for a Child Oriented Approach to Data Protection* https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf, pg 4. Domestic advertising standards and laws also exist, and could be reformed to address harmful content in advertising, for example the Australian Consumer Law addresses some aspects of advertising and the AANA has a Children's Advertising Code.

[114]As referenced in the Data Protection Commission 2021 *Fundamentals for a Child Oriented Approach to Data Protection* https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf, pg 50 and also in the *BEUC's Comments on the EDPB's Guidelines on the Targeting of Social Media Users* https://www.beuc.eu/sites/default/files/publications/beuc-x-2020-098_beucs_comments_on_the_edpb_guidelines_on_the_targeting_of_social_media_users.pdf pg. 3.

[115]EDPB 2018 *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* https://ec.europa.eu/newsroom/article29/items/612053/en

[116]Council of Europe 2021 *Children's data protection in an education setting - Guidelines (2021)* https://edoc.coe.int/en/children-and-the-internet/9620-childrens-data-protection-in-an-education-setting-guidelines.html, Para 7.6.2

> *Providers of online platforms should not present advertisements based on profiling using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor.*[117]

How the UK handles targeted advertising

Under the UK's *Age Appropriate Design Code* automatic profiling of children — such as the profiling that drives targeted advertising — should be turned off by default:

> *You should always provide a privacy setting for behavioural advertising which is used to fund a service, but is not part of the core service that the child wishes to access. Although there may be some limited examples of services where behavioural advertising is part of the core service (e.g. a voucher or 'money off' service), we think these will be exceptional. In most cases the funding model will be distinct from the core service and so should be subject to a privacy setting that is 'off' by default.*[118]

That is, it's still possible to *collect* data but not to *use the profiles that are created from this data* to target advertising, unless kids 'turn targeted advertising on' (or explicitly consent).

For profiling facilitated by cookies, for the purposes of targeted advertising, valid consent must be 'opt in', This means that allowing profiling 'by default' is not an option.[119] Parental consent is also necessary if the child is under the age of 13.

The UK GDPR (supplemented by the *Data Protection Act)* states that profiling anyone, including children, requires a DPIA and the fulfilment of certain measures, like human oversight and explicit consent. It stops short of the EU's recitals stating that profiling should not concern a child at all but it makes it abundantly clear it should not be 'a norm'. As a result, most large online services will have turned it off in the UK.

The UK *Age Appropriate Design Code* also includes the best interests of the child as a fundamental standard.

The Code offers a harm-centric approach to advertising as well, in Standard 5 which addresses detrimental uses of data. It notes that children's personal information should not be processed in ways that conflict with relevant marketing and behavioural advertising codes and standards which include rules prohibiting the marketing of certain products to children, such as high fat salt and sugar foods and alcohol. Like the Irish *Fundamentals*, here the UK's Code defers to advertising standards and communications regulations to address advertising content.

So, three different jurisdictions have all created a presumption against targeted advertising by outlining that children should not be profiled, sometimes dovetailed with an outright prohibition, or a belt-and-braces approach that says 'also definitely don't profile them to deliver harmful ads' (see Figure 1).

[117] European Commission 2022 *Digital Services Act* https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng
[118]Information Commissioner's Office 2020 *Age Appropriate Design Code* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/
[119]Information Commissioner's Office 2020 *Age Appropriate Design Code* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/

Feature	Ireland (DPC — Fundamentals)	UK (ICO — AADC)	EU (GDPR & DSA)
Targeted Ads	Very clear presumption that children's data should not be used to deliver targeted advertising.	Discouraged but does not go as far as the Irish approach. Outlines that harmful advertising is prohibited.	Very clear presumption against & prohibition of practice
Profiling	Not allowed unless justified as in children's best interests. Organisations should not profile children, engage in automated decision-making concerning children, or otherwise use their personal data, for advertising/marketing purposes, unless they can clearly demonstrate how and why it is in the best interests of children to do so.	Targeted advertising must be turned off by default, and must be justified as in children's best interests. Companies need to ensure features that rely on profiling are switched off by default (unless there is a compelling reason to do otherwise).	Not allowed unless justified as in children's best interests
Legal Basis	EU GDPR	UK GDPR & *Data Protection Act*	EU GDPR & DSA

Figure 1: A simplified overview of how different jurisdictions handle targeted advertising and children

3. Public opinion about targeted advertising

There is a serious mismatch between what industry tells us Australians want when it comes to targeted advertising and what Australians actually want. More businesses are using people's data in more ways than ever before, but there is often a suggestion that Australians don't mind. However, research suggests that they do. Australians are not comfortable with many of the data handling practices currently in use.

For example, research conducted with adults (before the Latitude and MediSecure privacy breaches), found that:

- 74% of Australians are not okay with companies sharing or selling their personal information to other companies.
- 64% find it unfair that companies require them to supply more personal information than what is necessary to deliver the product or service.
- 90% expect businesses to really step-up and protect them from their information being used in ways that leave them worse-off.
- Less than 10% of Australians are not comfortable with how targeted advertising is currently implemented in Australia.
- 46% are not comfortable with any kind of targeted advertising
- Among those consumers who are comfortable with targeted advertising, most wanted to see significant changes. For example:
    - 23% only want to see ads based on their current search for a product or service.
    - 31% want the option to opt-out.
    - 25% only want to see targeted ads when they have opted in.[120]

[120]CPRC 2023 *Not a Fair Trade* https://cprc.org.au/report/not-a-fair-trade-consumer-views-on-how-businesses-use-their-data/

There is a high level of discomfort around the amount of data being collected and the way it is being used, and this discomfort increases when data is used for advertising purposes.

There is also an awareness among consumers about how little control they have over their personal data. Further research with adults found that:

- 72% believe they have little to no control over the information collected by businesses with which they have no direct interaction.
- 71% believe they possess little to no control over businesses sharing their personal information with other entities.[121]

Far from being 'unconcerned', Australians want better protections and there are different models available to do this. One model might be to opt in to targeted advertising, another might be to provide opt-out options (less strong), but an alternative might be to introduce presumptions against the practice.

Part of the issue in gauging public opinion around these practices is the opaqueness of the practice itself, and the lack of awareness about how the process works. For example, consumers aren't aware of, nor understand, the workings of data brokers or how profiling happens. It can be difficult for people to understand what these practices are and what these terms mean. More importantly, it should not be up to consumers to become experts in understanding these practices in order to feel safe online or in control of their choices.

This opaqueness is reinforced by complex terms of service and impenetrable privacy policies that use vague language about how data can be collected, used or disclosed — and the way data can influence which products that are made accessible to people (and sometimes, with dynamic pricing even the prices advertised to them).

And this is for adults. We know there is a major mismatch between how the digital economy currently works and what Australians deserve, and this mismatch is especially pronounced when it comes to targeted advertising. If we were to ask parents and carers about their comfort level when it comes to children, we would only expect the discomfort to increase. Children deserve the benefits of a digital economy that is fair and safe, not exploitative; not just today but into the future as well.

Discussion from the roundtable on targeted advertising and the COPC

The discussion focused on four key themes.

1. **Targeted advertising as a process, rather than the instant of ad delivery**

There was discussion around the *process* that targeted advertising involves, including a pipeline of data handling practices. This includes:

- Data collection from multiple means and sources
- Data use and disclosure for profiling, and then
- The use of this profile and other data for the final instance of ad delivery.

The discussion outlined how a focus on this pipeline (or process), alongside the data use at the moment in time when an ad is served to a young person, was necessary.

[121]CPRC 2024 *Singled Out* https://cprc.org.au/report/singled-out

Existing APPs cover various aspects of this pipeline; from APPs about openness and transparency, which should make data collection transparent, to APPs addressing data collection and data use, which should limit the ways in which this data is collected, used or shared, and APPs around cross-border transfers, which should govern how this process happens on international platforms.

There was discussion around whether the current APPs, and privacy framework, adequately address targeted advertising and whether the issues are regulatory gaps or regulatory compliance. A Code presents an opportunity to address both.

2. Addressing a 'process' in the Code creates multiple opportunities and pathways to remedy

The nature of this process presents multiple opportunities for a Code to address the data cycle, and we see this in international approaches. For example:

- The UK*'s Age Appropriate Design Code* focused on the use of the data for profiling for commercial purposes. It says that while companies can collect data, they cannot use it to target advertisements to children or profile them. The collection of data requires transparency, language appropriate for children, safeguards, DPIAs etc, but the data collection part of the process is allowed to an extent.
- The Irish *Fundamentals* also use profiling as the mechanism to presume against the practice but outline more clearly that the limited extent to which data collection for these purposes would be allowable (see section 2 above for more detail).

We can also see variations in the approach to data collection evident in the EU and UK's handling of cookies. Cookies exist solely to collect data to enrich profiling. The EU and UK have regulations against the indiscriminate use of cookies — non-essential cookies must be turned off by default — but we do not have similar requirements in Australia. This highlights how different online experiences are shaped by legislation, including children's online experiences.

There was discussion around the paucity of attention given to the 'data collection' part of the pipeline. Specifically, whether regulators could determine if data was collected for targeted advertising purposes, or for a different (but related) purpose such as personalising a user's experience using AI. Concern was raised that data collection necessary for targeted advertising might simply be 'wrapped up' in the personalisation necessary to make AI work; it's the same data, the same process, but for a different end product.[122] If data collected for personalisation is not considered part of the targeted advertising pipeline, ads could then be targeted to consumers based on other aspects of their personalised experience creating large loopholes.

Focusing on all the aspects of the pipeline seemed necessary to remedy this. The UK's *Age Appropriate Design Code* outlines that data collection and use for 'providing a more personalised experience' is not justification enough when it comes to children's data. Safeguards and protections such as requirements for purpose limitation help to prevent functional loopholes. The Irish *Fundamentals* also addresses each part of the pipeline to arrive at a presumption against targeted advertising.

Regulatory remedy is required because young people have no 'self-defence' mechanisms available to them to avoid the privacy harms associated with targeted advertising. While there is a great deal of research into the steps young people sadly have to take to avoid other types of online harms, commercial harms like targeted advertising are not within their control. There are simply no evasive tactics they can deploy.[123] The same is true for parents. The discussion noted that many of the organisations at the

[122]See for example, Tama Leaver, Suzanne Srdarov 2025 *Children and Generative Artificial Intelligence (GenAI) in Australia: The Big Challenges* https://digitalchild.org.au/artificialintelligence/

[123]See for example, a discussion around children's limited resilience and consent models at Lisa Archbold, Damian Clifford, Moira Paterson, Megan Richardson and Normann Witzleb 2021 'Adtech and Children's Data Rights' *UNSW Law Journal* https://doi.org/10.53637/PJPS3138

roundtable were frequently asked what parents could do to limit the risks of privacy harms, but the answers do not lie in individualised approaches or remedies. A regulatory remedy is necessary.

There was also discussion around whether a prohibition on the collection of data for targeted advertising was a better approach, or whether the collection of data central to the creation of advertising profiles such as Mobile Advertising IDs or any pseudonymised identifier, could be prohibited. This would be complex, and concerns were raised about non-compliance or malicious compliance. Instead, a proactive approach focused on broader prohibitions with transparency was discussed.

3. The need for transparency and accountability

The discussion returned to the question of 'but how will a regulator know' what purpose data was collected for. This highlighted the need for pro-active obligations on platforms to disclose which data they collect, how they use it and why, in order for any remedy to be meaningful.[124]

Such transparency would also help introduce a preventative approach to privacy harms; by showing upfront what is going to happen to data and entering into a discussion with regulators about data practices, rather than waiting for a significant issue to occur and having to react to it.

The possibilities of independent audits and transparency reports were raised as processes that could improve transparency, especially in light of the following:

- The scale of the fines that industry currently wears with seemingly little impact,[125] and
- The capacity for misleading information and a lack of transparency within the sector.[126]

This also raised questions about meaningful enforcement and the need for powers that extend beyond fines to remedies such as data deletion and algorithm destruction. The FTC case against Weight Watchers was mentioned as an example, where regulators alleged that Weigh Watchers had improperly collected children's data and as part of the settlement had to delete both the data and any AI algorithms they had built and trained on that data.[127]

4. A question of business model

The scale of the privacy risks and rights violations discussed raised broader questions about the business model. If a family is bickering with their children owing to their overuse of platforms — prompted by a business model that relies on profiling and targeted advertising — then fully confronting targeted advertising requires confronting the business model.

There were questions raised, and some excitement, about what that might look like, especially given that the current business model has been particularly difficult from a child rights perspective and was rolled out with limited accountability.

An effective prohibition of the process of targeting — including the data cycle — could effectively lift children out of this business model, creating a profoundly different experience for them. This raised a salient point, about the capacity of the Code to create a different digital world for children and young people, where the business model doesn't impact them in the same way.

---

[124]A parallel discussion on how transparency might work within an online safety framework might offer potential insights. See for example Reset.tech Australia 2024 *Achieving Digital Platform Public Transparency in Australia* https://au.reset.tech/news/achieving-digital-platform-public-transparency-in-australia/

[125]See for example, Chandni Gupta 2023 *Made to Manipulate: The impact of deceptive online design practices on wellbeing and strategies to mitigate harm* https://cprc.org.au/report/made-to-manipulate-report

[126]See for example, Sarah Wyn-Williams 2025 *Careless People* Macmillan, London

[127]While the FTC's website is down, see Electronic Privacy Information Centre 2022 *U.S. Regulators Order Algorithm and Data Deletion in Settlement* https://epic.org/u-s-regulators-order-algorithm-and-data-deletion-in-settlement-with-weight-watchers/

Recommendations from the roundtable on targeted advertising and the COPC

The discussion and contributions outlined a number of recommendations for the development of the Children's Online Privacy Code, including:

- Addressing the 'data process' involved in targeted advertising, including data collection, use, and disclosure, as well as other related elements under the APPs such as cross-border data transfer and openness and transparency. The process of targeting advertising spans a number of APPs, and each aspect of the process needs remedy.

- A strong approach, whether prohibiting or presuming against the collection, use or disclosure of data to enable targeted advertising. The Irish Fundamentals, stemming from the EU approach, provide potential models for how this might be developed.

- Strong requirements for transparency, including regulator transparency and public transparency, be implemented within the Code itself.