Reset·Tech
AUSTRALIA

The Children's Online Privacy Code and targeted advertising

Reset.Tech Australia
June 2025
Policy briefing

Summary

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?

Contents

Reset.Tech Australia is an independent, non-partisan policy research lab committed to driving public policy advocacy, research and civic engagement to strengthen our democracy in the context of technology. We are the Australian affiliate of Reset, a global initiative working to counter digital threats to democracy.

Introduction

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).*[1]

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.[2] 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,[3] 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.[4] 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

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

[2] 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/

[3] 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/

[4] 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)

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 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.[5]

Targeted advertising sits at the core of the business model of surveillance capitalism,[6] 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.

[5] ICCL 2024 *Australia's Hidden Security Crisis* https://www.iccl.ie/digital-data/australias-hidden-security-crisis/
[6] 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

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.[7] When it comes to children specifically, debates exist around the role of advertising in promoting on materialism,[8] causing economic harms such as excessive spending,[9] and contributing to climate change.[10] 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,[11] junk food,[12] gambling,[13] indoor tanning,[14] 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. It is a systems focussed approach, drawing attention to how data is inappropriately collected, used and disclosed to drive advertising delivery.

[7] 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
[8] 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
[9] Juliet B. Schor 2004 *Born to buy* Scribner, London
[10] Global Action Plan 2022 *Big Tech's Dirty Secret* https://www.globalactionplan.org.uk/files/big_tech_report.pdf
[11] 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
[12] 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
[13] 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
[14] Jenny Radesky, Yolanda Reid Chassiakos, Nusheen Ameenuddin and Dipesh Navsar 2020 'Digital Advertising to Children' *Pediatrics* https://doi.org/10.1542/peds.2020-1681

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 World* 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.'[15]

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.'[16]

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.'[17]
- 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.'[18]
- 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.'[19]

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.

---

[15] 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 42

[16] 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

[17] 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

[18] 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

[19]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

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[20] 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'[21] 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.[22] 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[23] (a type of distress), and feeling that these ads are invasive and 'up in their faces' (a disruption to their digital tranquility).[24] 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.'[25] 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.[26] 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.'[27] 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

[20] Danielle Citron & Daniel Solove 2021 'Privacy Harms' *Boston University Law Review*, 837 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222
[21] Danielle Citron & Daniel Solove 2021 'Privacy Harms' *Boston University Law Review*, 837 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222, pp 841
[22] 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
[23] Reset.Tech Australia & the CREATE Foundation 2025 *Consultation with young people about the Children's Online Privacy Code and the right to access, correct or delete data* forthcoming
[24] 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
[25] Danielle Citron & Daniel Solove 2021 'Privacy Harms' *Boston University Law Review*, 837 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222, pp. 831
[26] See Sarah Wyn-Williams 2025 *Careless People* Macmillan, London
[27] Danielle Citron & Daniel Solove 2021 'Privacy Harms' *Boston University Law Review*, 837 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222, pp. 845

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:

> *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.*[28]

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.[29] 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.[30] 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[31].

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

---

[28] 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

[29] 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.

[30] 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

[31] 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.

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*.'[32]

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 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*.'[33]

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.*'[34]

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.[35] 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:

---

[32] 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

[33] 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.

[34] 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.

[35] 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

> *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.*[36]

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:

> *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.*[37]

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.*[38]

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.[39] Parental consent is also necessary if the child is under the age of 13.

The UK's GDPR 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

---

[36] 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
[37] European Commission 2022 *Digital Services Act* https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng
[38] 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/
[39] 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/

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).

Feature	**Ireland (DPC Fundamentals)**	**UK (Age Appropriate Design Code)**	**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	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.[40]

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.[41]

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.

[40] CPRC 2023 *Not a Fair Trade* https://cprc.org.au/report/not-a-fair-trade-consumer-views-on-how-businesses-use-their-data/
[41] CPRC 2024 *Singled Out* https://cprc.org.au/report/singled-out

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

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.

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.[42] 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.[43] The same is true for parents. The discussion noted that many of the organisations at the 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.[44]

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,[45] and
- The capacity for lying and cover-ups within this sector.[46]

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

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

[43] 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

[44] 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/

[45] 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

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

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.[47]

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.

[47] 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

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.