Reset.
AUSTRALIA

Response to the Senate Economic Reference Committee's Inquiry into International Digital Platforms Operated by Big Tech companies

Reset Australia
Feb 2023

Contents

1. About Reset Australia & this submission

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

This submission has been prepared in response to the Senate Economic Reference Committee's Inquiry into International Digital Platforms Operated by Big Tech companies. It provides an overview of Reset's broader thinking about the issues of regulating international digital platforms in Australia, as well as responding directly to some of the terms of reference of the inquiry.

Specifically, we respond to the Committee's call for evidence around the collection and use of children and young people's data particularly for the purposes of profiling, behavioural advertising, or other uses (Terms of reference 'D') and their questions about online safety in the discussion paper. These responses are in section 3.

2. The need for a comprehensive, effective digital regulatory framework for Australia

Reset Australia welcomes the Committee's Inquiry and its focus on the breadth of potential issues and opportunities that international platforms present to Australian users. Reset Australia has previously outlined five directions for future policy to ensure Australia arrives at an effective, coherent tech regulation framework that informs our response to this inquiry.

2.1 Eliminating risks from systems and processes

Regulation needs to pivot towards targeting risks created across the systems and processes developed by digital services. The aspects of systems and processes, and related risks, that regulation could address includes:

- Algorithms. Including content recommenders systems and ad delivery systems
- Platform design. Including design abuses and dark patterns
- Specific features. Specific features that create risks need to be addressed

It is these sorts of systems and processes that manufacture and amplify risks. However, none of them are inevitable and these risks exist because of choices made by digital platform services. Social media platforms can change and improve their systems, and regulation can incentivise them to do so.

2.2 Expand regulations to address community & societal risks

Existing legislation addresses a collection of individual risks that leave Australians vulnerable to collective risks. Collective risks come in two interconnected forms.

- Community risks, such as those facing indigenous communities, migrant communities, people of colour, women, children and LGBTIQ+ people. These communities often suffer unique and disproportionate harms in the digital world that extend beyond individual risks posed by content. Disinformation and hate speech can affect particular communities in ways that differ from individual harm.
- Societal risks. The scale and reach of social media platforms has the capacity to influence and affect Australian institutions, such as Parliament, the Press and healthcare systems, often with destabilising effects.

Expanding the definitions of harms (and risks) addressed in Australia's regulatory framework would better protect Australian communities and society at large.

2.3 Ensure regulation creates accountability & transparency

There are multiple ways governments can regulate the digital world, but the most effective policies require accountability and transparency from tech platforms themselves. Regulations that identify the core risks as stemming from platforms themselves — and squarely place the burden of responsibility on digital services — should be prioritised.

Regulation can place duties on users in multiple ways, but these are often inappropriate or ineffective:

- Solutions that position individual users (especially children and parents) as key actors in improving safety are often inappropriate and will fail to protect all Australians
- Solutions that pass responsibility on to users (as parents or consumers) to read 'the fine print' or consent to a risky system misrepresents the power asymmetry between users and digital platforms
- Solutions that position individual users (be they 'trolls' or influencers) as the key actors responsible for harm undersells the role of platforms in creating the risky digital environments that enable and encourage toxic actors.

Accountability also requires transparency. Legislators, regulators, researchers and civil society need to have up to date understandings about the specific mechanics of platform's functionalities and outcomes in order to better hold them to account.

2.4 Ensure the regulatory framework is comprehensive

The rapid growth of the technology has seen Australia's issue-by-issue (e.g. 'cyber bullying', 'trolling' etc), sector-by-sector (e.g. 'social media platforms' 'messaging services' etc) regulatory framework struggle to keep pace. Many new and emergent technologies are

missed, and innovative companies straddling the gaps between existing industry definitions are inappropriately regulated.

- A sector-by-sector approach fails to address the vertical integrations and shared functionality of may digital platforms
- An issue-by-issue approach cannot anticipate risks created by innovations and emergent technologies.

These gaps suggest that the current approach is unable to future-proof the regulatory framework, and that as technologies evolve, more and more gaps will emerge. Risk focused, systemic models may be more successful at future proofing themselves.

2.5. Ensure regulation is strong and enforced

Big tech poses big risks and necessitates a robust regulatory response. However, because Australia has to date engaged self- and co-regulatory models by default, our regulatory framework has often failed to reduce risks as rigorously as they otherwise may have.

Future regulation needs to start from the premise that self- and co-regulation will not be sufficient. Reset Australia believes self- and co-regulation have a role to play in the Australian regulatory landscape at large, but that unfortunately the risks posed by the digital environment are:

- High impact, and include significant public health and community safety concerns
- Significant to the community, and the public has an appetite for the certainty of robust regulations
- Unable to be adequately dealt with by lighter touch regulations. Digital platforms have demonstrated a track record of systemic compliance issues, including multiple breaches of existing legislation and a generally anaemic response to self-regulation

This warrants a pivot towards primary and subordinate legislation and regulation for the sector.

Alongside strengthening existing regulation, regulators need to be resourced and enabled to enforce this, and joined up in ways that do not reproduce the issue-by-issue approach hampering current legislative remedies.

3. Response to the Committee's specific terms of reference on children and young people, data and safety

1. The risks Australian children and young people face online in 2023

The Australian government has a long and commendable track record around improving children's online safety. From early legislation in 2015 focussing on cyber-bullying and abuse,, to the inclusion of the multiple content harms and basic safety expectations we see in the *Online Safety Act*, parliament has worked hard. Likewise, the eSafety Commissioner's Safety-By-Design initiatives have provided great global leadership around voluntary measures to help embed children's safety into product design.

We welcome this Committee's expanded focus on exploring '*the collection and processing of children's data, particularly for the purposes of profiling, behavioural advertising, or other uses'*, as well as the focus on online safety noted in the Committee's discussion paper. This expanded focus is much needed.

Broader issues around children's rights—especially privacy and data protection—are currently overlooked in Australia's regulatory framework. Our framework focuses on a narrower understanding of online safety that does not adequately reflect the full scope of the risks children and young people face online. That is, when Australian children and young people engage with the digital world, many of the risks they encounter currently sit outside our regulatory system.

Widely respected research, informed by the lived experiences of young people and the global inHope network of hotlines, identified four types of risks children and young people currently face online:[1]

- Content risks; or risks that emerge from children and young people engaging with or being exposed to potentially harmful content. This would include risks of seeing violent content, sexual content, or content that would be deemed inappropriate such as mis and dis information, dangerous challenges, pro-eating disorder and other age-inappropriate content.

- Contact risks: or risks that emerge when children and young people experience, or are targeted by, potentially harmful contact. This contact could include violent or abusive contact such as being harassed or stalked, sexual contact such as grooming and attempts to groom, or contacts that would otherwise be deemed inappropriate such as contact with those attempting to radicalise the young.

- Conduct risks: or risks associated with young people witnessing, participating in or being targeted by harmful conduct. This would include violent conduct, like cyber-bullying, sexual conduct like self generating sexual material, or conduct that is otherwise inappropriate, like joining QAnon style groups.

[1] Sonia Livingstone & Mariya Stoilova 2021 *The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics)* https://doi.org/10.21241/ssoar.71817

- Contract risks, or risks that young people are exploited by commerce. This category would include malicious "contract" risks, such as identity theft and sextortion, but also the 'extended use design' or design abuses that manipulate young people into handing over more data etc.

  Each of these 4 types of risks is exacerbated by the cross-cutting risk of privacy abuses and data exploitation.[2]

Australia's regulatory framework needs rethinking to adequately address the full set of risks children face. Some content and conduct risks are addressed through the *Online Safety Act*, some contact risks are tackled in criminal codes, but commercial risks are largely overlooked and almost all harms are amplified because of inadequate data protections. Table 1 describes how these gaps present in our current regulatory frameworks.

These commercial risks present real threats to the advancement of children's rights. As the UN Committee on the Rights of the Children noted:[3]

> *The digital environment includes businesses that rely financially on processing personal data to target revenue-generating or paid-for content, and such processes intentionally and unintentionally affect the digital experiences of children. Many of those processes involve multiple commercial partners, creating a supply chain of commercial activity and the processing of personal data that may result in violations or abuses of children's rights, including through advertising design features that anticipate and guide a child's actions towards more extreme content, automated notifications that can interrupt sleep or the use of a child's personal information or location to target potentially harmful commercially driven content.*

Given the breadth and dynamics of these risks, the Committee's review is timely.

[2] It may be of interest to the Committee that both contract risks and the cross cutting ability of privacy violations to amplify all types of harm, were added to the framework after extensive consultation in a post-Covid world. The initial framework, developed in 2010, included only the first three Cs. The risks experienced by young people in the digital world are dynamic.

[3] UN Committee on the Rights of the Child 2021 *General comment No. 25 (2021) on children's rights in relation to the digital environment* https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation, paragraph 40

Risk	Current regulatory framework	Gaps in framework
Content — risk of exposure to inappropriate content. For example, risks of exposure to violent content, racist content, pornography, sexualised imagery and mis & disinformation	The *Online Safety Act 2021* is establishing frameworks and Codes around class 1 and 2 materials, as well as developing a Restrictive Access System to limit access to age inappropriate materials like pornography. Violent online material may be addressed by the *Sharing Abhorrent Violent Material Act* 2019	Regulation focuses on individual pieces of content, and overlooks the role of platforms in promoting harmful content to children (via algorithms, for example). Hate speech, mis & disinformation are not adequately addressed in the current framework, but can be harmful
Contact — risks of making inappropriate contact with others. E.g. Risks of exposure to online grooming, stalking & extremist recruitment	A number of online laws exist that address contact risks, from the *Criminal Code Amendment (Protecting Minors Online) Act* 2017 to laws around terrorist recruitment. Some of the *Online Safety Act*'s co-regulatory codes around ensuring user safety may address ways platforms can reduce contact risks, but these are not yet released and will be authored by industry	Existing legislation remedies some harms but does not mitigate risks. While they may criminalise individuals who make inappropriate contact, they do not require platforms to stop recommending adult strangers as 'friends' or 'followers' or prevent platforms enabling adult accounts to message children's accounts for example
Conduct — risks associated with inappropriate behaviour. E.g. bullying, trolling, joining harmful groups (e.g anti-vax)	The *Online Safety Act* includes specific provisions around cyber-bullying for children under 18. This includes taking down content that is deemed cyber bullying, and where the perpetrator is a child, the regulator is able to require apologies	Engagement with harmful communities falls outside the scope of current regulatory frameworks
Contract / Commercial — risks arising from inappropriate commercial activities and contract exploitation. E.g. risks of identity theft, gambling, profiling bias, surveillance advertising, persuasive design	Very limited. Children's data is protected under the *Privacy Act 1988*, which may reduce the risk of identity fraud but does not consider user's metadata as protected data. The Restrictive Access System may restrict gambling (but may miss loot boxes in games).	The use of children's data poses significant risks, and is largely overlooked by Australia's current regulatory framework.

Table 1. The 4Cs of risk for children and young people compared to Australia's current regulatory framework

2. Towards a comprehensive Australian regulatory framework: Privacy, and behaviour advertising as an overlooked online harm

Behavioural advertising (or targeted or personalised advertising) involves the use of people's personal data to target them with specific ads. Children and young people[4] are often subjected to behavioural advertising. Fueled by data-hungry machine learning models,[5] behavioural advertising requires the collecting and processing of children and young people's data on an industrial scale. The best available estimate of the amount of data collected by advertisers about children and young people, by the time they turn 13, is 72 million data points.[6]

A. The prevalence of behavioural advertising

Behavioural advertising, and the excessive collection, retention and sharing of personal data this is associated with, is prevalent and unavoidable for children and young people.

Most of the digital products and services that children and young use have behavioural advertising embedded within them. Australia's current regulatory framework provides no viable alternative for childhood in this digital age, than to receive behaviour advertising. A study of 39 popular children's apps found that 95 percent included at least one form of advertising,[7] and a quick analysis of ten of the most popular apps with Australian teens[8] shows that between 40-70% currently have integrated behavioural advertising. At the time of writing, behavioural advertising is found on YouTube, Instagram, Facebook, Facebook Messenger, Snapchat, TikTok and Twitter. Meta has announced an intention to 'switch off' behavioural advertising during February 2023, although this claim has been made multiple times in the past, including in potentially misleading ways (see Appendix B).

Most of the digital products and services that children and young use track their data to enable behavioural advertising. To meet the data needs of behavioural advertising, the excessive collection, retention and sharing of children's personal data has become the norm across the digital world. For example:

- Analysing the number of trackers in the 'top 10' free children's apps downloaded in Australia shows that the vast majority of apps children use have data trackers installed. In total, 15 apps were cumulatively included in the 'Top 10' downloaded from the Google Play store for Australian children aged 0-5, 6-8 and 9-11 combined. Of these

[4] We use the language of children and young people to describe those under 18 years old

[5] For example, Google claims to have put these powerful AI models into the hands of every advertiser (*See* Jerry Dischler 2018 "Putting machine learning into the hands of every advertiser" *Google: The Keyword* https://support.google.com/google-ads/answer/9065075?hl=en-GB).

[6] In Donell Holloway 2019 "Surveillance Capitalism and Children's Data: The Internet of Toys and Things for Children." *Media International Australia, Incorporating Culture and Policy* 170(1), pp. 27-36

[7]Marisa Meyer, Victoria Adkins, Nalingna Yuan, Heidi Weeks, Yung-Ju Chang & Jenny Radesky 2019 "Advertising in Young Children's Apps: A Content Analysis." *Journal of Developmental & Behavioral Pediatrics:* https://pubmed.ncbi.nlm.nih.gov/30371646/#:~:text=DOI%3A-,10.1097/DBP.0000000000000622,-Full%20text%20links.

[8] See Office of the eSafety Commissioner 2021 *The Digital Lives of Aussie Teens* https://www.esafety.gov.au/sites/default/files/2021-02/The%20digital%20lives%20of%20Aussie%20teens.pdf.

apps, 33% had Facebook trackers installed, and 80% had Google trackers installed (see table 2).

- Likewise the majority of digital platforms and apps that Australian teenagers routinely track data. Again, exploring ten apps popular with Australian teens[9] shows that 40% of them have Facebook trackers installed (or are Facebook), and 70% include Google trackers (see table 3).

- A study of EdTech products used in Victoria and New South Wales found that apps and products recommended to school children during the pandemic included cookies, tracking pixels and SDKs that enable data collection and transfer, largely for advertising purposes.[10] (See Appendix B for more details).

This matches global research. An analysis of 959,000 apps on the Google play store in the UK and US found that apps targeting children had the highest number of third-party trackers, collecting and transferring data to other companies;[11] an American analysis of 5,855 children's apps found that the majority had built in data-sharing capacity (Software Development Kits, or SDKs) that facilitated data sharing that breached America's COPPA regulations,[12] and; an American investigation found that two-thirds of apps played by preschool-aged children collected and shared personal data[13] (persistent digital identifiers, which are used to link-IDs in advertising profiles).

[9] See Office of the eSafety Commissioner 2021 *The Digital Lives of Aussie Teens* https://www.esafety.gov.au/sites/default/files/2021-02/The%20digital%20lives%20of%20Aussie%20teens.pdf.
[10] Human Rights Watch 2022 *How Dare They Peep into My Private Life* https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments
[11] Reuben Binns, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert, Nigel Shadbolt 2018 "Third Party Tracking in the Mobile Ecosystem" In *WebSci '18: 10th ACM Conference on Web Science* https://doi.org/10.1145/3201064.3201089
[12] Irwin Reyes , Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez & Serge Egelman 2018 "Won't somebody think of the children?" examining COPPA compliance at scale. *Proceedings on Privacy Enhancing Technologies.* https://doi.org/10.1515/popets-2018-0021
[13] Fangwei Zhao, Serge Egelman, Heide Weeks, Nico Kaciroti, Alison Miller & Jenny Radesky 2020 "Data Collection Practices of Mobile Applications Played by Preschool-Aged Children." *JAMA Pediatr.* https://jamanetwork.com/journals/jamapediatrics/fullarticle/2769689.

Ranking, free apps for kids aged 9-11	Ranking, free apps for kids age 6-8	Ranking, free apps for kids ages 5 & Under	Product	Number of trackers embedded	Number of permissions requested	Facebook trackers present	Google trackers present
1	1	1	YouTube kids	2	12	No	Yes
2	2		Messenger Kids	2	30	Yes	No
3	3		Toca life world: Building a story	3	13	No	Yes
4	4	2	ABC reading eggs: Learn to read	4	11	Yes	Yes
5	6		Spriggy pocket money	7	8	Yes	Yes
6	7	3	VLC for android	0	20	No	No
7	8		Lego builders	0	5	No	No
8	9	4	ABC Kids	5	16	No	Yes
9	10	5	Slither.io	7	7	Yes	Yes
10		6	Little panda's ice cream game	3	3	No	Yes
		7	Class dojo	2	24	No	Yes
		8	Ice cream cone cupcake baking	13	8	No	Yes
		9	Children's doctor dentist	5	5	Yes	Yes
		10	House designer: Fix & flip	1	5	No	Yes
	5		Toca kitchen 2	3	7	No	Yes

Table 2. An analysis of the number of trackers and permission requested by apps,[14] by popularity in Australian downloads from the Google Play store for Android[15]

[14] From Exodus Privacy 2023 *Check an app* https://exodus-privacy.eu.org/en/
[15] Chart ranking on Jan 22, 2023 from Sensor Tower 2023 *Charts and Rankings* https://app.sensortower.com/

Product	Number of trackers embedded	Number of permissions requested	Facebook trackers present	Google trackers present
YouTube	2	39	No	Yes
Instagram	2	46	Yes	No
Facebook	0	64	Not needed	No
Snapchat	3	59	No	Yes
Facebook Messenger	5	68	Yes	Yes
TikTok	5	73	Yes	Yes
Whatsapp	1	62	No	Yes
Twitter	4	49	No	Yes
Discord	2	21	No	Yes
Skype	1	56	No	No

Table 3. An analysis of the number of trackers and permission requested by apps,[16] for ten apps popular with Australian teens[17]

B. The harms of behavioural advertising

This unavoidable behavioural advertising, and the data exploitation underpinning it, harms children and young people in two distinct ways. Firstly, it violates their human right to privacy and secondly, it violates their consumer rights because it is inherently unfair.

Behavioural advertising is a **violation of young people's right to privacy,** and often egregiously so. Children and young people have the right to privacy, including the right to privacy from the excessive collection, retention and sharing of their personal data. Children's right to privacy is enshrined in the *Convention on the Rights of the Child*. Article 16 states that:

> *No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.*

This right to privacy applies in the digital terrain. The Human Rights Council definitively stated that '*children are entitled to human rights and freedoms, as are all individuals. International and regional legal instruments articulate the right to privacy and children's right to privacy*.'[18] Children's right to privacy in the digital world is additionally confirmed by the Committee on the Rights of the Child's *General comment no. 25 on children's rights in*

[16] From Exodus Privacy 2023 *Check an app* https://exodus-privacy.eu.org/en/
[17] See Office of the eSafety Commissioner 2021 *The Digital Lives of Aussie Teens* https://www.esafety.gov.au/sites/default/files/2021-02/The%20digital%20lives%20of%20Aussie%20teens.pdf
[18] Human Rights Council 2021 *Artificial intelligence and privacy, and children's privacy Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci* A/HRC/46/37 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/015/65/PDF/G2101565.pdf?OpenElement

relation to the digital environment also describes States obligations to protect children's privacy in the digital world.[19] The excessive collection, excessive retention and excessive sharing of children and young people's data for behavioural advertising is an unrestrained abuse of market power—it is an arbitrary interference with their right to privacy.

The privacy violations involved in the behavioural advertising process are often egregious in scope and magnitude. For example, data harvested about young people is routinely shared without adequate safeguards in the 'Real Time Bidding' process (RTB). RTB see masses of seemingly unconnected data points linked to creating a vast, extremely personalised profile about each user,[20] using unique IDs like Mobile Advertising ID or handset's device IDs. These profiles contain identifiers that share all sorts of personal information about specific users, from their exact GPS locations to health concerns like STDs, religion and income.[21] These profiles are then arbitrarily shared with hundreds of adTech companies. For example, Google broadcasts these details about each users thousands of times a day to 968 different adTech companies,[22] in order for them to 'bid' to place a targeted ad in a user's feed. Young people's data is not immune from this process. While age markers for children may not be included in profiles, children's personal data—such as their GPS location data, health concerns, religion and family income—are routinely fed in the RTB machine.[23] This exposes thousands of data points about children to hundreds, if not thousands, of companies each day. The legal basis for processing data in the RTB process is contested in Europe and the UK.[24]

Privacy violations can also be exacerbated by poor data handling practices. An analysis of 186 popular children' game apps in Australia found that over half (59%) contained 'concerning code' that potentially enabled privacy and security risks.[25]

Secondly, **behavioural advertising could be considered unfair when deployed on children and young people**. We argue that it is unfair because; young people can be uniquely vulnerable to the practice by nature of their age; it is used in ways that target especially vulnerable young people, and; because it violates the morals and principles of the majority of the Australian population. This is an unconscionable practice.

Research suggests that younger children can struggle to distinguish between advertising and non-advertising content, a capability that appears to emerge only at age 12.[26] This challenge is exacerbated by digital advertising techniques,[27] with research suggesting that six year olds may only recognise a quarter of ads presented online even where they include an

---

[19] UN Committee on the Rights of the Child 2021 *General comment No. 25 (2021) on children's rights in relation to the digital environment* https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

[20] Global Action Plan 2019 *Kids for Sale* https://www.globalactionplan.org.uk/files/kids_for_sale.pdf

[21] See for example IAB Tech Lab 2018 *Audience Taxonomy* https://www.dropbox.com/sh/7xo77grl2mnb6b6/AAAlszXoQ_zM2kUSsSRqKJSqa?dl=0&preview=7.+Industry+template+of+intimate+categories+to+profile+people+(Appendix+E).xlsx

[22] Irish Council for Civil Liberties 2019 *Real Time Bidding* https://www.iccl.ie/what-is-real-time-bidding/

[23] Global Action Plan 2019 *Kids for Sale* https://www.globalactionplan.org.uk/files/kids_for_sale.pdf

[24] Michael Veale & Frederik Zuiderveen Borgesius 2022 'Adtech and Real-Time Bidding under European Data Protection Law' *German Law Journal* doi:10.1017/glj.2022.18

[25] Children and Media Australia 2022 *Apps can track* https://childrenandmedia.org.au/assets/files/news/latest-news/yappcensussummary22fin.pdf

[26] Angela Campbell 2016 *Rethinking Children's Advertising Policies for the Digital Age*, 29 Loy. Consumer Law Review https://ssrn.com/abstract=2911892

[27] Laura Owen, Charlie Lewis, Susan Auty, Moniek Buijzen 2012 'Is children's understanding of non–traditional advertising comparable to their understanding of television advertising?' *Journal Public Policy Mark.* doi.org/10.1509/jppm.09.003; and Angela Campbell 2016 *Rethinking Children's Advertising Policies for the Digital Age*, 29 Loy. Consumer Law Review https://ssrn.com/abstract=2911892

obvious cue such as a price.[28] Behavioural advertising is more problematic again for the young, with research suggesting that young people are less able to develop informed purchasing intentions when exposed to behavioural advertising. For example, when young people are provided with textual "debriefing", i.e. an explanation of how behavioural advertising works, initially high purchase intentions decrease.[29] That is, when teenagers are provided with accurate information about the mechanics of targeting, they moderate their purchase intentions accordingly. This vulnerability is more pronounced for younger children. Experimental research explored how younger children (aged 9-13 years old) are affected by targeted advertising, finding that they are not driven to higher purchase intentions because they experience targeted ads as more relevant, but because targeted ads affect how much children "like" being advertised to *because they do not recognize they are being targeted*. The researchers conclude "thus, children seem to process targeted online advertising in a noncritical manner"[30] *vis a vis* adults.

Research has also shown that higher levels of targeting, involving more personalised use of data, generate stronger responses in teenagers regardless of their concerns about privacy—[31] that is, teenagers are unable to turn their concerns about their privacy into effective safeguarding strategies from behavioural advertising.

In addition to these concerns about the unfairness of the practice for all young people, we are deeply concerned about the way behavioural advertising can be used to, and indeed is promoted for its ability to, target additional vulnerable young people. For example, Facebook outlined to Australian advertisers that their behavioural advertising system is able to target young people when they are feeling "insecure," "worthless," or "need a confidence boost."[32] And research has shown that Facebook does not exercise care nor caution with this "vulnerability" targeting. Tests of Facebook's Australian advertising systems demonstrated that Facebook would allow advertisements that promoted "Cocktail recipes from what you can steal in your parents liquor cabinet" to young people Facebook identified as interested in alcohol, or offer weight loss ads to young women interested in extreme weight loss, for example.[33]

Questions need to be raised about the fairness—and conscionability of—a practice that leaves young people less able to effectively moderate their purchasing intentions, and can be deployed in ways to specifically exploit particularly vulnerable young people.

This is particularly troubling given that behavioural advertising, and the associated data exploitation, violates the morals and principles of the majority of the Australian community.

---

[28] Moondore Ali, Mark Blades, Caroline Oates, Fran Blumberg 2009 'Young children's ability to recognize advertisements in web page designs' British Journal Developmental Psychology doi: 10.1348/026151008x388378

[29] Brahim Zarouali , Koen Ponnet, Michel Walrave, Karolien Poels 2017 ""Do you like cookies?" Adolescents' skeptical processing of retargeted Facebook-ads and the moderating role of privacy concern and a textual debriefing" *Computers in Human Behavior* http://dx.doi.org/10.1016/j.chb.2016.11.050.

[30] Eva A. van Reijmersdal, Esther Rozendaal, Nadia Smink, Guda van Noort & Moniek Buijzen 2017 'Processes and effects of targeted online advertising among children' *International Journal of Advertising* https://doi-org.ezproxy-b.deakin.edu.au/10.1080/02650487.2016.1196904.

[31] Michel Walrave, Karolien Poels, Marjolijn L. Antheunis, Evert Van den Broeck & Guda van Noort 2018 'Like or dislike? Adolescents' responses to personalized social network site advertising,' *Journal of Marketing Communications*, https://doi.org/10.1080/13527266.2016.1182938.

[32] Darren Davidson 2017 "Facebook targets 'insecure' young people" *The Australian* https://theaustralian.com.au/business/media/digital/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6.

[33] Reset 2021 *Profiling Children for Advertising: Facebook's Monetisation of Young People's Personal Data* https://au.reset.tech/uploads/resettechaustralia_profiling-children-for-advertising-1.pdf.

The OAIC's research into community attitudes to privacy[34] found that 84% of Australians agreed or strongly agreed with the principle that 'children should have the right to grow up without being profiled and targeted'. Likewise, 87% agreed or strongly agreed that this right also applied to EdTech; 'technology in schools and for education should only collect the minimum personal information necessary for the service.' Both of these principles are routinely violated. In the same survey, potential protections for children were discussed, and 83% supported the statement 'profiling and targeted advertising must not occur for children'.

Internal research from Instagram reveals that young people may be unhappy with it as well. Young people identify "inappropriate advertisements targeted to vulnerable groups" as one way in which "Instagram harms their mental health," suggesting that "teens called out ad targeting on Instagram as feeding insecurities, especially around weight and body image."[35] Moreover, the research suggests that young people want to be able to "opt out of advertising categories that are personally triggering, such as skinny teas and lollipops or waist-trainers."[36] In short, behavioural advertising is a product feature young people have asked Instagram to turn off.

C. The case for regulatory action

Young people and parents are not able to effectively safeguard against these unavoidable harms because much of the practice is deceptive. This further reduces the ability of the 'consumer choice' model to safeguard children, because it deprives young people and parents the ability to choose the best product for them.

There is often no meaningful process for consumers to give or deny permission for behavioural advertising. Research has shown that consumers have little knowledge about how this practice affects and operates on them.[37] Many companies rely ethically, and legally where required, on problematic notice and consent processes with complex privacy policies used to justify processing children's data for behavioural advertising. The problems of privacy policies are well known, but these extend to products frequently used by young people. An Australian study of the privacy policies of 10 popular apps and products used by young people found that nine of them required a college level degree to understand and on average they each take one hour and 45 minutes to read.[38]

This lack of awareness is demonstrable among young people. A poll of 506 teenagers in 2022 found that many young Australians are not sure what data is collected about them; 41.9% suggested that they did not know the amounts nor types of data that digital platforms and apps were collecting about them, 22% felt they were 'in the middle' for knowledge and only 36% felt they were aware about the amount and types of data that was collected about them.[39] Earlier polling in 2021 of 400 16 & 17 year olds found that:[40]

---

[34] OAIC 2020 *Australian Community Attitudes to Privacy 2020* https://www.oaic.gov.au/__data/assets/pdf_file/0015/2373/australian-community-attitudes-to-privacy-survey-2020.pdf

[35] Teen Mental Health Deep Dive, p. 28, 39, Published by The Wall Street Journal September 29, 2021, https://digitalwellbeing.org/wp-content/uploads/2021/10/Facebook-Files-Teen-Mental-Health-Deep-Dive.pdf.

[36] Teen Mental Health Deep Dive, p. 28, 39, Published by The Wall Street Journal September 29, 2021, https://digitalwellbeing.org/wp-content/uploads/2021/10/Facebook-Files-Teen-Mental-Health-Deep-Dive.pdf.

[37] Chang-Dae Ham 2017 "Exploring how consumers cope with online behavioral advertising," *International Journal of Advertising*, https://doi.org/10.1080/02650487.2016.1239878.

[38] Reset 2021 *Did We Really Consent to This?* https://au.reset.tech/uploads/l01_resettechaustralia_policymemo_t_c_report_final-july.pdf.

[39] See submission from Young people from the Y, NSW, also being made to this inquiry

[40] Reset 2021 *Did We Really Consent to This?* https://au.reset.tech/uploads/l01_resettechaustralia_policymemo_t_c_report_final-july.pdf.

- Only 7% of young people are confident they understood everything they agreed to in privacy policies, 21% are quite confident, 41% are only a little bit confident and 20% of young people say they don't understand any of it. The other 10% didn't know.
- Only 4% of young people always read the privacy policies, 13% read them most of the time, 38% read them some of the time while 45% of young people never read them.

Parents are not necessarily more aware, particularly at times when they are vulnerable themselves. For example, an Australian survey about how new mother's use pregnancy apps[41] found that while 29% said they were 'a little' or 'very concerned' about the privacy implications of these apps, 27% said that they were not at all concerned and 35% said that they were not concerned because "the app they used did not involve them uploading personal data or images". (9% that they were not sure). However, these apps routinely create sensitive profiles from data uploaded, from babies' dates of birth, birthweights, ultrasound photos, health details like medical appointments etc.

This lack of awareness may be a consequence of active obfuscation on behalf of major platforms. An analysis of the privacy policies and practices of 10 apps popular with Australian young people noted that eight of them deployed dark patterns, which actively attempted to "trick" young people into agreeing to sharing more personal data than is necessary.[42] Dark patterns are frequently deployed in children's apps too. For example, kids games often ask children to share their location or phone books, or encourage them to "share their top score," which requires linking the app to other accounts or sharing it with contacts.[43] It is not always explicitly clear that this will allow additional data collection and transfer.

This active obfuscation is often exacerbated by potentially misleading statements by digital platforms. As appendix B highlights, when questioned about behavioural advertising and children across 2021 and 2022, Meta issued a range of opaque potentially misleading replies.

Given that parents and teens disapprove of the practice, it is unclear whether they would continue to use the same digital service and products, or use them in the same way, if behavioural advertising was more accurately represented to them. The OAIC found that 84% of adult consumers suggested that privacy is an important consideration when choosing a digital product.[44] This makes behavioural advertising potentially unfair when deployed on young people.

It appears that the only effective form of protection for children and young people from the harms of behavioural advertising will come from effective legislation to change the behaviours of digital platforms themselves.

Many countries have moved towards legislation that prohibits behavioural advertising for young people. For example, the Irish Data Protection Commission made clear that as a use of personal data that was not in children's best interests, it would not comply with their 2021

[41] Deborah Lupton & Sarah Pedersen 2016 'An Australian survey of women's use of pregnancy and parenting apps' *Women and birth* https://doi.org/10.1016/j.wombi.2016.01.008
[42] Reset 2021 *Did We Really Consent to This?* https://au.reset.tech/uploads/l01_resettechaustralia_policymemo_t_c_report_final-july.pdf.
[43] Science Daily 2018 "Advertising in kids' apps more prevalent than parents may realize" https://www.sciencedaily.com/releases/2018/10/181030091452.htm.
[44] OAIC 2020 *Australian Community Attitudes to Privacy 2020* https://www.oaic.gov.au/__data/assets/pdf_file/0015/2373/australian-community-attitudes-to-privacy-survey-2020.pdf

guidance.[45] Europe has doubled down on this, with the EU wide *Digital Services Act* 2022[46] prohibiting targeting children with behavioural advertising.

3. Towards an effective Australian regulatory framework: The failure of self and co-regulation to protect children and young people

The issues paper published by the committee also calls for evidence about the effectiveness of the current legislative framework in protecting children and preventing online harm. As described above, the current framework is 'patchy' and does not comprehensively address all of the risks children and young people face online, especially privacy risks. But it also does not always address risks *effectively*.

For example, the reliance on self- and co-regulation routinely fails to protect children and young people. The draft Online Safety Codes, which the eSafety Commissioner has asked to be revised and resubmitted,[47] demonstrate perfectly how co-regulation fails to deliver online safety and privacy for children and young people. The eSafety Commissioner may ultimately reject even the revised versions, but this reinforces the fact that co-regulation as an approach systematically fails children.

Comparing the initial industry drafted Codes with regulator drafted Codes that address similar issues in other jurisdictions, the weakness of co-regulation becomes apparent. Below we compare Australia's industry-drafted Online Safety Code with three Codes drafted by regulators and legislators—the UK's *Age Appropriate Design Code* (UK 2020), Ireland's *Fundamentals for a Child Oriented Approach to Data Processing* (Ireland 2021), and California's *Age Appropriate Design Code* (California 2022)—to highlight the systemic weakness of the approach.[48]

A. The age at which young people's accounts default to private

Every time a young person creates a new account on a platform which has profiles, (or 'accounts' or 'handles'), that platform has a choice. The default settings for that child's account can be set to the most private, or they can default to public. It is a stark choice. Children's best interests are better served with private accounts that maximise safety and

---

[45] 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

[46] EU 2022 *Digital Services Act* https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

[47] Office of the eSafety Commissioner 2023 *Online industry asked to address eSafety's Concerns with the Safety Codes* https://www.esafety.gov.au/newsroom/media-releases/online-industry-asked-address-esafetys-concerns-draft-codes-0

[48] The proposed final versions of these Codes are not publicly available. But here we discuss two examples of demonstrable weaknesses in the Australian Codes vis-a-vis regulator drafted Codes, which we believe still exist in the final version. Reset and others raising these three issues with the industry drafters through a required consultation process. The industry drafters stated that "in response to feedback, the Code provisions concerning privacy settings on children's accounts have been amended to apply to children under 16", for example. This suggests these three issues persist in the final version currently under consideration, alongside many others (see Online Safety Codes 2022 *Submissions log and industry associations'1 responses to public consultation feedback* https://onlinesafety.org.au/wp-content/uploads/2022/11/221118_Submissions-log-responses_FINAL.pdf)

privacy; whereas commercial interests are better served with public accounts that maximise engagement and therefore profit. Young people can, of course, change these settings but everytime a child opens an account, a platform has an opportunity to nudge them towards privacy and safety, or not.

These nudges are important for children's privacy and safety. Meta themselves have outlined the value of private accounts, stating:

> *Wherever we can, we want to stop young people from hearing from adults they don't know or don't want to hear from. We believe private accounts are the best way to prevent this from happening.*[49]

Accordingly, the proposed Online Safety Codes include proposals about defaulting children's accounts to private. They propose a 'minimum age' under which children's accounts must default to private. When we compare the minimum ages proposed by industry draft Codes compared to regulator drafted Codes, we can see that the industry drafted proposals leave Australian 16 and 17 year olds comparatively unprotected.

AGE UNDER WHICH YOUNG PEOPLE'S ACCOUNTS MUST 'DEFAULT TO PRIVATE'[50]

	Who 'wrote' the rules?	On social media	On online games
UK	Regulators/ legislators[51]	18	18
Ireland	Regulators	18	18
California	Legislators	18	18
Australia	Industry	16[52]	16

This should not be understood as a one-off accident. International experimental research has demonstrated that in jurisdictions where regulators and legislators have written the rules, 16 and 17 year olds are routinely protected, but where rules written by regulators and legislators do not exist, teenagers are unprotected.[53] The draft Codes in Australia propose the exact same low standards present in jurisdictions where 'no regulations' exist at all. Co-regulation did not attempt to raise the floor of protections one iota.

---

[49] Meta 2021 'Giving young people a safer, more private experience on Instagram' https://about.fb.com/news/2021/07/instagram-safe-and-private-for-young-people/

[50] Meaning they must be set to a private account, or otherwise the have the highest privacy settings turned on in default mode

[51] The UK's *Age Appropriate Design Code* was written by the regulator (the ICO) and subsequently passed by parliament

[52] According to the draft Code for Social Media services made available, they must "have default settings that are designed to prevent (children) from unwanted contact from (strangers), including settings which prevent the location of the child being shared with other accounts by default", but there is no specific mention of defaulting children's accounts to private. The response from the industry drafters to this point was to confirm that it would be 16 (see Online Safety Codes 2022 *Submissions log and industry associations'1 responses to public consultation feedback* https://onlinesafety.org.au/wp-content/uploads/2022/11/221118_Submissions-log-responses_FINAL.pdf)

[53] See Fairplay 2022 *Discrimination by Design* https://fairplayforkids.org/wp-content/uploads/2022/07/design-discriminations.pdf

Indeed, some social media platforms themselves have made clear that this is a deliberate choice. Newly published documents leaked from the whistleblower Francis Haugen suggest that Meta have carefully considered and limited this trade off. A document called '*Should we default teens into privacy settings'* ultimately recommends against defaulting to private settings because 'data projections show a strong potential for loss of valuable interactions in DMs (direct messages)'.[54] When Meta finally introduced a minimum age under which they would default young people's accounts to private, in anticipation of the UK's Age Appropriate Design Code in 2020, they announced:

> *starting this week, everyone who is under 16 years old (or under 18 in certain countries) will be defaulted into a private account when they join Instagram*[55]

Australian teenagers may be less protected than teenagers in "certain countries" because we allow industry to draft their own Codes via co-regulation.

B. Collection of children and young people's precise geolocation data

Children's location data is extremely sensitive and inappropriate disclosure can create safety risks. Accordingly, the proposed Online Safety Codes include proposals about how to handle children and young people's precise geographic location. Again, when we compare the safety measures proposed by industry draft Codes compared to regulator drafted Codes, we can see that the industry drafted proposals are significantly weaker.

In Australia, the proposal is to not *broadcast* children's location. In jurisdictions where codes have been drafted by regulators and legislators, they propose the stronger step of not *collecting* children's locations in the first instance. Preventing services from broadcasting precise locations is a significantly weaker step than preventing them collecting location data, because it overlooks the risks presented from:

- Data security flaws. Collecting troves of location data creates inevitable security risks from malicious hacking to a lack of internal controls about which staff, if any, should be able to access children's GPS locations. The scale of the recent Optus[56] and Medicare[57] breaches, and the gravity of the harms enabled by now-convicted abuser Alexander Jones' ongoing access to the Victorian DHSS' vulnerable children's database[58] suggest that these are not pedantic considerations. Security issues can affect many children and cause immense harm.

---

[54] Instagram UX Research nd *Should we default teens into privacy settings* https://www.documentcloud.org/documents/23322914-copy-of-should-we-default-teens-into-privacy-settings__sanitized_opt

[55] Meta 2021 'Giving young people a safer, more private experience on Instagram' https://about.fb.com/news/2021/07/instagram-safe-and-private-for-young-people/

[56] David Spears 2022, 'Federal government to unveil new security measures following massive Optus data breach' *ABC News* https://www.abc.net.au/news/2022-09-25/new-security-measures-to-be-unveiled-following-optus-data-breach/101472364

[57] See Sashwat Awasthi & Lewis Jackson 2022 'Australia's Medibank says data of 4 mln customers accessed by hacker' *Reuters* https://www.reuters.com/business/healthcare-pharmaceuticals/australian-health-insurer-medibank-says-all-customers-personal-data-compromised-2022-10-25/

[58] Sarah Curnow & Josie Taylor 2021 'About a boy' *ABC News* https://www.abc.net.au/news/2021-04-18/did-alex-jones-use-dhhs-database-crissp-to-groom-a-teenager/13301262

- Errors and missteps from services. For example, a simple failure of process saw Instagram make children's contact details publicly available if they simply opened business accounts.[59] Children's precise location data is not immune to failures of process, even if digital services agree in principle to not broadcast locations, mistakes happen.

- Commercial harm arising from this data. Not *broadcasting* GPS data does not prevent online service providers using and selling this data for commercial exploitation, such as behavioural advertising. We note again, that while Europe is moving to ban targeted advertising to children, this Code appears to have been drafted in ways that deliberately enable this ongoing practice in Australia. Again, this is out of step with emerging global protections.

PROTECTIONS FOR CHILDREN'S PRECISE LOCATION (GPS LOCATION)			
Who 'wrote' the rules?		**On social media**	**On online games**
UK	Regulators/ legislators	Must not collect by default	Must not collect by default
Ireland	Regulators	Must not collect by default	Must not collect by default
California	Legislators	Must not collect by default	Must not collect by default
Australia	Industry	Must not broadcast by default	Must not broadcast by default

Australian children's precise location data will continue to be collected at scale and pose safety risks, because we allow industry to draft their own rules. In a letter to the eSafety Commissioner,[60] the Australian Child Rights Taskforce asks two questions about the Codes:

> *Firstly*, d*o these [Codes] improve safety standards for Australian children from the current position, and secondly*, *do they match the standards enjoyed by children elsewhere in the world where their safety has been considered.*

They go on to state '*we do not believe that either question can be answered in the affirmative*'. Codes that neither improve safety from the existing status quo, nor reach minimum international standards are not 'strong' Codes.

The capacity of co-regulation to improve children's safety was made crystal clear by industry, in their response to Reset.Tech's submission to consultation around these proposed Codes. In responding to our concerns about collecting children's GPS data, the industry authors stated "we consider that this issue is best dealt with through changes to the Privacy Act 1988 (Cth) (currently under review)." The lack of ambition to voluntarily improve children's safety demonstrated in their reply is stunning. They make clear they are prepared to offer children lower levels of protection—when it comes to their GPS data—until the Attorney General

[59] Natasha Lomas 2022 'Instagram fined €405M in EU over children's privacy' *Techcrunch* https://techcrunch.com/2022/09/05/instagram-gdpr-fine-childrens-privacy/
[60] ACRT 2023 *Letter Regarding the Online Safety Codes* https://childrightstaskforce.org.au/resources/member-news-and-publications/

makes them improve practice. Where industry is unwilling to voluntarily improve practice, self and co-regulation will always fail children.

4. What can be done to enhance children's rights in the digital environment

The issues paper published by the committee also asks what more could be done to enhance online safety for children and young people in Australia. Reset's broader position about the general direction of travel is outlined above, but more specific recommendations are below.

Recommendation 1: Remedy the failures of self and co-regulatory mechanisms for digital platforms and services, by not registering any new co-regulatory Codes and progressively replacing existing self- and co-regulatory Codes. This includes Codes around children and young people's online safety and privacy.

- Any Online Safety Codes drafted by industry need to be rejected. Stronger more robust 'codes' (industry standards) should be instead drafted by the eSafety Commissioner.
    - This is a possibility, but the decision rests with the Office of the eSafety Commission as they negotiate with the industry drafters on the proposed Codes. As the co-regulatory process is fundamentally flawed, we believe Australian children will be best served if the eSafety Commissioner drafts industry standards.
- An in-principle commitment for all new regulations to be written by regulators or legislators should be explored.
- The proposed Online Privacy Code for children, recommended as part of the review of the *Privacy Act* should be drafted by the OAIC. This requires adopting recommendation 5.1 in the Privacy Act Review[61] that extends the powers of the Information Commissioner to draft Privacy Codes ('industry standards') directly, where it is in the public interest and where it is unlikely that an appropriate industry representative can be found.
    - We believe that recommendation 5.1 in the Privacy Act review needs minor amendment to make sure that standards can be drafted directly by the Information commissioner where it is directly in the public interest *or* it is unlikely that an appropriate industry standard representative can be found.
- In the longer term, all existing self- and co-regulatory mechanisms in operation should be considered for gradual replacement with regulator drafted standards. As each code comes up for its scheduled review, it would be timely to evaluate if a regulator drafted code would be more effective in improving the digital landscape for Australians.
- Relevant regulatory bodies would need to be resourced adequately in order to achieve this.

Recommendation 2: Introduce a specific standard protecting children and young people's privacy, rooted in children's rights and their best interests, addressing privacy concerns, behavioural advertising and broader design abuses affecting children. The code must apply to all services likely to be accessed by children and young people.

[61] Attorney General's Office 2023 *Privacy Act Review* https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

- This is a key recommendation 16.5 in the Privacy Act Review, and should be implemented.
    - We would like to see this proposal extended to include requirements to undertake risk assessments and duties to mitigate against identified risks. This has the capacity to transform the digital environment for the better. Without requirements for risk assessments, or explicit duties of care, digital platforms would simply be required to react to mandates from the 'Code authors' (be they ideally OAIC, or potentially industry itself). This is in keeping with international requirements, and would extend any potential Privacy Code into an upstream, systems and processes focussed piece of regulation.
    - Risk assessments could also require algorithmic impact assessments, requiring companies to identify and mitigate any risks their algorithms—which use children's data—create. Algorithms can create significant risks for young people, and Australian institutions.[62]
- A number of jurisdictions around the world have introduced specific regulator or legislator drafted Codes and frameworks (in Australia, standards) that reflect children's rights, specifically the 'best interests principle' to improve children's online safety and privacy. These include the UK's *Age appropriate design code*,[63] Ireland's *Fundamentals for a child oriented approach to data protection*,[64] Sweden's *Barns och ungas rättigheter på digitala plattformar*[65], the Netherlands' *Code voor kinderrechten*,[66] France's *Les droits numériques des mineurs*,[67] and California *Age Appropriate Design Code*.[68] Many other jurisdictions are actively considering this, including the EU and New Mexico, Maryland and other US states. These codes have been successful in driving up standards of safety for children and young people.[69]
- These codes apply to all digital services and products children and young people use, to ensure that protections travel with them from social media, to online games to EdTech and AdTech platforms.
- Reset.Tech Australia has worked with a coalition of children's organisations across Australia who are supportive of this sort of standard, and documented strong support from civil society[70] and from children and young people.[71]
- Such a standard would also help ensure Australia meets its obligations under the Convention on the Rights of the Child to better protect children from online commercial exploitation. The Committee on the Rights of the Child's *General*

---

[62] Reset.Tech Australia 2022 'Social Grooming' *AQ Magazine* https://www.jstor.org/stable/27161413
[63] Information Commissioners Office 2020 Age Appripriate Design Code https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/
[64] 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
[65] Barnombudmannen 2020 Barns och ungas rättigheter på digitala plattformar https://www.imy.se/globalassets/dokument/ovrigt/barn-och-ungas-rattigheter-pa-digitala-plattformar.pdf
[66]Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2021 *Code voor kinderrechten*, https://codevoorkinderrechten.nl/wp-content/uploads/2021/03/20210311_Code-voor-Kinderrechten_v1-1.pdf
[67] CNIL 2020 *Les droits numériques des mineurs* https://www.cnil.fr/fr/les-droits-numeriques-des-mineurs
[68] California 2022 *Age Appropriate Design Code Act* https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB2273&showamends=false
[69] Information Commissioner's Office 2022 "Children are better protected online in 2022 than they were in 2021" - ICO marks anniversary of Children's code https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/children-are-better-protected-online-in-2022-than-they-were-in-2021/
[70] See for example https://www.childrensdatacode.org.au/
[71] Reset.Tech Australia 2021 *Keep it to a limit* https://au.reset.tech/uploads/resettechaustralia_policymemo_pollingreport_final-oct.pdf

comment no. 25 on children's rights in relation to the digital environment[72] outlines our obligations:

- *… 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.* (paragraph 42)
- *States parties should take legislative, administrative and other measures to ensure that children's privacy is respected and protected by all organizations and in all environments that process their data. Legislation should include strong safeguards, transparency, independent oversight and access to remedy. States parties should require the integration of privacy-by-design into digital products and services that affect children. They should regularly review privacy and data protection legislation and ensure that procedures and practices prevent deliberate infringements or accidental breaches of children's privacy.* (paragraph 70)
- *In addition to developing legislation and policies, States parties should require all businesses that affect children's rights in relation to the digital environment to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services. That includes businesses that target children, have children as end users or otherwise affect children. They should require such businesses to maintain high standards of transparency and accountability and encourage them to take measures to innovate in the best interests of the child. They should also require the provision of age-appropriate explanations to children, or to parents and caregivers for very young children, of their terms of service.* (paragraph 39)

Recommendation 3: Prohibit collecting and using children's data to enable behavioural advertising to children. This would bring Australia into alignment with Europe.

- The EU's *Digital Services A*ct includes a ban on using children's data for profiling children for the purposes of advertising. This protects children from the harmful business model, restoring their human rights to privacy and consumer right to fair practices. It is unclear if there is a moral case to allow Australian children to be harmed while their European peers are protected.
- This is partly covered by recommendation 20.5, 20.6 and 20.7 in the Privacy Act Review to prohibit direct marketing to a child unless the personal information used for the direct marketing was collected directly from the child and the direct marketing is in the child's best interests, prohibit targeting of a child except where that is in their best interests, and prohibit trading in personal information of children. We believe this needs to be clarified to:
    - Make it exceedingly clear that commercial advertising is not in children's best interests and

[72] UN Committee on the Rights of the Child 2021 *General comment No. 25 (2021) on children's rights in relation to the digital environment*
https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation

- Extended to cover the privacy-invasive data harvesting pipeline. A prohibition on delivering marketing or targeting to children, and a prohibition in trading data, will not stop the pipeline of data collection that underpins most of the digital world. Because of the significant vertical integrations of these international platforms, they can and will continue to collect data even if they do not target ads to children or trade it with third parties. Prohibitions on *collecting* data involved in the behavioural advertising model must also be specified.