Reset.
AUSTRALIA

Response to the Privacy Act Review Report

Reset.Tech Australia
March 2023

Reset.
AUSTRALIA

Contents

About Reset.Tech Australia & this submission

Reset.Tech 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 and strengthen digital markets.

We have organised our response in two sections: responses to selected consultation questions, and a dossier we have compiled on children and young people's privacy harms.

Personal information, de-identification and sensitive information

B. *Should consent be required for the collection, use, disclosure and storage of other tracking data, such as health data, heart rate and sleeping schedule, in addition to precise geolocation tracking data?*

Explicit, opt-in consent should be required to collect, use, disclose or store all biometric data, including tracking data, but consent alone is not sufficient for protection. Ensuring the 'fair and reasonable' test leads to data minimisation, and that impact assessment ensures stronger protections, would also reduce risks.

Both location data and biometric data create unique and serious risks. For example, location data can create significant and unique safety risks where they are handled badly,[1] and is particularly concerning to young people[2] and vulnerable communities— proposal 4.10 to require consents to process this data, is welcome . Biometric data also creates significant and unique risks that warrant additional protection. Unlike many other forms of personal information, biometric data cannot be changed where a breach or other issue arises. Once people's fingerprints or facial recognition data have been compromised, they cannot be changed (simply put, you can't change your fingerprints nor eyes). This is not a hypothetical, and significant breaches involving fingerprint and facial recognition data have and are

[1] For example, we note how location data was allegedly created security risks for users of Uber, see Jo Ling Kent, Chiara Sottile & Michael Cappetta 2016 'Uber Whistleblower Says Employees Used Company Systems to Stalk Exes and Celebs' *NBC News* https://www.nbcnews.com/tech/tech-news/uber-whistleblower-says-employees-used-company-systems-stalk-exes-celebs-n696371

[2] Rys Farthing *et al* 2023 '"It Sets Boundaries Making Your Life Personal and More Comfortable": Understanding Young People's Privacy Needs and Concerns' *Technology & Society Magazine* https://ieeexplore.ieee.org/document/10063169

occurring.[3] 'Tracking' data, such as heart rate and sleep data are a form of biometric data that shares the same risks around permanent compromise. Additionally its unnecessary disclosure could produce substantive harms to Australians, such as health discrimination or economic harms through increased health insurance premiums for example. The stronger protections possible need to be afforded to biometric data, in all its forms.

But explicit, opt-in consent alone is not a sufficient protection. Alongside explicit, opt-in consents, all sensitive personal data, including biometric and geolocation data, should be afforded stronger protections through:

The fair and reasonable test. Data minimisation approaches are central to reducing the risks people face as a result of the collection, use or disclosure of both location and biometric data.Where this data is not strictly necessary, given the unique and significant risks it can create, it should not be collected, used or disclosed in the first instance.

We also emphasise that the 'fair and reasonable' analysis must be considered from the perspective of a reasonable and ordinary person rather than, for example, a 'reasonable data collector'. The Federal Court's analysis from the recent action between the ACCC and Google[4] is relevant to this point.

> *Australian Competition and Consumer Commission v Google LLC* (No 2) [2022] FCA 1476
>
> The ACCC alleged Google misled Australian consumers to obtain their consent to expand the scope of personal information that Google could collect and combine about consumers' internet activity, for use by Google, including for targeted advertising. The Federal Court found the first page of Google's relevant notification to users was not misleading. It also held that consumers, acting reasonably and in their own interests, were adequately informed. The outcome and analysis in this case indicates that 'reasonableness', even in the famously perplexing domain of adtech and targeted advertising, is at risk of a narrow judicial interpretation.

Privacy Impact Assessments for high risk privacy activities, as per proposal 13.1. Any data collection, use, disclosure or disposal of biometric data in all its forms should be defined as a high risk activity subject to an impact assessment. For biometric data in particular, assessments should consider the privacy and broader security risks involved.

---

[3] Such as the leak of over 1 million people's fingerprint data by security firm Suprema. (see vpnResearch Mentor Team 2023 *Data Breach in Biometric Security Platform Affecting Millions of Users* https://www.vpnmentor.com/blog/report-biostar2-leak/). It is worth noting that these security solutions such as biometric readers are available and advertised to Australian clients (see Nedap nd *Biostar integration Seprema* https://www.nedapsecurity.com/technology-partner/suprema/ for example).

[4] *Australian Competition and Consumer Commission v Google LLC* (No 2) [2022] FCA 1476.

Additional protections

What additional requirements should apply to mitigate privacy risks relating to the development and use of facial recognition technology and other biometric information?

Facial recognition technology, and other uses of biometric data, needs especially careful consideration, and the deployment of risk-based, proactive governance frameworks. The widespread use of this technology drives demand for biometric data collection, use and disclosure, which as discussed above presents significant and unique risks. Given this, the use of technologies that rest on biometric data should be strictly controlled and limited. Biometric data is extremely sensitive and uniquely tethered to its human source. There should be rare cases where it is collected at all, and thoughtfully constructed guardrails where it is harvested, commercialised, and traded.

Proposal 13.2 proposes enhanced risk assessments for this sort of technology, which we welcome. We would recommend that these enhanced assessments consider both privacy and safety concerns associated with these products, *and* the data flows that they create from collection to deletion. Both the products and the data flows need to be subject to strict protections. Proposal 13.1 would require Privacy Impact Assessments for high risk privacy activities. As discussed above, these need to be required for the collection, use, disclosure or disposal of biometric data.

We note that a number of jurisdictions are moving forward with legislative requirements around facial recognition technology and other AI that involves biometric data. This includes the EU and Colombia, Argentina, Brazil, Chile and Uruguay developing frameworks regulating the use of AI.[5] While this is beyond the scope of the *Privacy Act*, it may be worth considering to ensure a comprehensive framework of protections for biometric data and its uses. On a sectoral level, we encourage close reading of the Australian Academy of Science paper, *Data in Professional Sport*.[6] As the authors note, professional sport has long been at the forefront for intense data governance and data subject issues, especially given the pivotal role of biometric data.

---

[5] See for example Argentina *National Plan of Artificial Intelligence* 2020 https://ia-latam.com/wp-content/uploads/2020/09/Plan-Nacional-de-Inteligencia-Artificial.pdf
Uruguay 2021 *Artificial Intelligence Strategy* https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-inteligencia-artificial
Chile 2021 *National Policy on Artificial Intelligence* https://www.minciencia.gob.cl/areas-de-trabajo/inteligencia-artificial/politica-nacional-de-inteligencia-artificial/
Colombia 2021 *Inteligencia Artificial Colombia* https://inteligenciaartificial.gov.co/publicacion/9/
México 2020 *National Mexican Agenda of Artificial Intelligence* https://ia-latam.com/wp-content/uploads/2020/09/Agenda-Mexicana-de-IA-2020.pdf

[6] Australian Academy of Science 2022 *Getting Ahead of the Game: Athlete Data in Professional Sport* www.science.org.au/datainsport

Individual rights

A. *What would the impact of the proposed individual rights be on individuals, businesses and government?*

Rights to access, explanation, objection, erasure, correction, and de-indexation have become mandatory minimum standards for citizens in the European Union and beyond, as other jurisdictions have followed suit from the *General Data Protection Regulation* (GDPR). Australians should be granted equal rights to their European counterparts. We expect the regulatory and compliance burden for companies to be manageable, given that EU standards are widely considered to be the standards towards which even non-EU companies aspire.

For these rights to be meaningful, they must be enforceable. A significant challenge with the maintenance of the GDPR system is timely enforcement. This issue unlocks numerous important resourcing issues well known to those in human rights, access to justice, and civil society more broadly – enforcement bodies need the resources to move cases swiftly and prevent backlog, and civil society needs the appropriate backing to provide advice and support to complainants.

Direct marketing, targeting and trading

A. *What would be the impact of the proposals in relation to direct marketing on individuals, businesses and government?*

Proposals 20.1 and 20.2 are strong steps in the direction of international best-practice data protection. Our feedback relates to whether these amendments are ambitious enough, in the context of high community expectations for privacy and data protection, especially in the aftermath of major data breaches.

Proposals 20.1 and 20.2 should be further galvanised by more limitations at the data collection phase. We agree with the Consumer Policy Research Centre that a 'culture of data minimisation' is the direction that Australian businesses should head. This means that the 20.2 provision should be extended from 'use' to 'collection'. Without influence over the data collection phase, the good efforts of these proposals will not meaningfully improve privacy outcomes.

Proposal 20.2 should be an opt-in provision rather than an opt-out provision. This is in line with the European Commission's experience in similar areas, who moved to an opt-in scheme in 2018 under GDPR. From an individual's perspective, opt-in schemes are the failsafe option.

Opt-out introduces complexity, risk, and compliance dilemmas that are difficult to monitor and expensive to enforce.

For children and young people specifically the prohibition on direct marketing (proposal 20.5) would help to advance their rights and reduce harm and is welcome. Many other jurisdictions in the world have moved to ban this sort of advertising for young people, including Europe through the *Digital Services Act*,[7] Ireland[8] and California.[9] This proposal is a welcome step to achieve international best practice for children. Direct marketing leaves young people vulnerable to economic exploitation. Research has shown that despite young people's privacy concerns, they do not appear to be able to effectively safeguard themselves from the persuasiveness of this advertising.[10] Additional research shows that when teenagers are provided with more information and 'debriefed' about how behavioural advertising works, any initially strong intentions to make purchases are moderated.[11] Research on younger children have also found that "children seem to process targeted online advertising in a noncritical manner"[12] *vis a vis* adults. This leaves young people vulnerable to economic harm. Research we have undertaken suggests young people agree with a prohibition. They outline for example "fundamentally, young people do not want their data used to sell them things, especially without their consent. Young people's data is not company's "private property" - it should be treated as belonging to young people and companies should be considered caretakers of such data."[13]

Direct marketing drives data collection and use practices that violate young people's privacy and creates security risks, but prohibiting marketing alone will not 'turn off' the data collection pipeline for children (as discussed below). A focus on reducing data collection is needed to advance children's right to privacy, alongside the welcome prohibition on direct marketing..

---

[7] European Commission 2022 Digital Services Act https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

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

[9] California 2022 *Age Appropriate Design Code* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273

[10] Specifically, higher levels of targeting using more personalised data generates stronger responses among teens *regardless* of their concerns about privacy. Michel Walrave, Karolien Poels, Marjolijn L. Antheunis, Evert Van den Broeck & Guda van Noort 2018 "Like or dislike? Adolescents' responses to personalised social network site advertising," *Journal of Marketing Communications*, https://doi.org/10.1080/13527266.2016.1182938.

[11] 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.

[12] Eva 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.

[13] See Reset.Tech Australia 2023 *Submission to the Senate Economic Reference Committee's Inquiry into International Platforms submission on behalf of children and young people*

***B**. What would be the impact of the proposals in relation to targeting on individuals, businesses and government?*

The prohibition on targeting children (proposal 20.6) could help to secure young people's right to privacy and security in the digital world. The sheer scale of targeting at the moment is alarming, most of the digital products and services that children and young use track their data to enable behavioural advertising:

- 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.[14]
- The majority of the 'top 10' free children's apps downloaded in Australia contain data trackers. 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, **33% contained Facebook trackers, and 80% contained Google trackers**.[15] (See table 1 in appendix)
- The majority of digital platforms and apps that Australian teenagers use **routinely track data**. Again, exploring ten apps popular with Australian teens[16] shows that 40% of them contain Facebook trackers (or are Facebook), and 70% include Google trackers.[17] (See table 2 in appendix)
- 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**.[18]

OAIC's research into community attitudes to privacy[19] 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'; 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', and; 83% supported the statement 'profiling and

[14] Children and Media Australia 2022 *Apps can track* https://childrenandmedia.org.au/assets/files/news/latest-news/yappcensussummary22fin.pdf
[15] Reset.Tech Australia 2023 *Submission to the Senate Economic Reference Committee's Inquiry into International Platforms*
[16] 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.
[17] Reset.Tech Australia 2023 *Submission to the Senate Economic Reference Committee's Inquiry into International Platforms*
[18] 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
[19] 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

targeted advertising must not occur for children'. This sort of targeting for commercial purposes is clearly not in children's best interests, nor the public's interest.

Requirements to limit the use of some algorithms and some aspects of targeting—as defined in the Privacy Act Review paper—are already in place and protecting children in other parts of the world, including Ireland[20] and California.[21] There is good precedent to limit targeting to instances where it is in children's best interests.

Within the best interests framework, it is important to note that targeting also drives the algorithms and recommender systems children use, from content recommender to search algorithms for example. These can function in children's best interests, ensuring children and young people can access the digital world. Targeting can help advance young people's rights, such as their right to access information from search engines, to play and enjoy leisure pursuits using content recommender systems, or to maintain family or peer relationships. This needs to be considered in evaluating children's best interests when it comes to targeting. Children and young people should not be denied access to the full and rich opportunities of the digital world because beneficial targeting is unnecessarily turned off for them.

But these algorithms can and do regularly promote content, connections or creators that harm children. For example, search algorithms routinely make dangerous challenges available to children,[22] recommender algorithms promote pro-anorexia content and creators,[23] or extremist material to young people,[24] and friend recommender systems regularly recommend adult strangers to children creating grooming risks.[25] They can also be used as part of the 'extended use' design strategy that harms children as described above. The consequences of this can be catastrophic. Recently, a UK Coroner ruled that online content had played more than a minor role in causing the suicide of a 14 year old girl, Molly Russell, after seeing extensive self-harm and suicide content in her recommended (algorithmically promoted) feed. The Coroner concluded that Molly "died from an act of

[20] Data Protection Commission 2021 https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf
[21] California 2022 *Age Appropriate Design Code* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273
[22] Fairplay 2022 *Dared by the Algorithm: Dangerous Challenges are Just a Click Away*
[23] For example, a photo-sharing platform's algorithms routinely promote pro-anorexia content and creators to users, Fairplay 2022 *Designing for Disorder* https://fairplayforkids.org/wp-content/uploads/2022/04/designing_for_disorder.pdf
[24] Ralph Housego & Rys Farthing 2022 'Social Grooming' *AQ Magazine* https://www.jstor.org/stable/27161413
[25] Australian Child Rights Taskforce 2023 *Letter to the eSafety Commissioner* https://childrightstaskforce.org.au/wp-content/uploads/2023/01/Online-Safety-Codes_-ACRT-letter-to-eSafety.pdf

self-harm while suffering from depression and the negative effects of online content".[26] Targeting must not harm a child; this is never in their best interests.

A rights-based approach is needed when evaluating if targeting is in children's best interests, that includes their rights to protection (and not to be harmed), as well as their rights to access information, to plan and enjoy leisure time, and more broadly to the opportunities the digital world can provide.

We note that while proposals 20.5, 20.6 and 20.7 provide a welcome proposition to defend against the use of children's data in commercially exploitative ways. However, while they may turn off behavioural ads from young people's feed, and take young people out of data brokerage services, they may not prevent young people's data from being collected in risky and exploitative ways without additional clarity around data collection using SDKs, cookies and pixels within vertically integrated companies.

Proposal 20.5 will prohibit direct marketing to children, unless the information was provided directly by a child *and* it is in their best interests. On social media, for example, this will mean platforms turn off the delivery of ads using personalised data (but potentially allowing the delivery of ads using contextual information, as some platforms are moving towards in anticipation of European legislation)[27]. Proposal 20.6 will reinforce this by prohibiting targeting a child, and proposal 20.7 will prohibit the trade of personal information of children.

This combination of prohibitions might create a loophole that allows some of the most egregious data harvesting about children to continue, in large, vertically integrated companies. These companies often run platforms themselves, and collect other data directly from children by placing trackers, like cookies, pixels or SDK into other digital products and services. These companies do not disclose (or trade) this data, indeed it is not in their commercial best interests to disclose it. If these platforms simply turn off their ad delivery systems, they may avoid all of the prohibitions outlined in these proposals while still collecting reams of personal information about young people.

While this data collection might not be fair nor reasonable, we would argue that it never has been and yet has still continued en masse. it might be worth considering an explicit prohibition on the collection of children's data using cookies, pixels or SDKs unless it is necessary to deliver the service. Clarifications around if proposal 20.6—prohibitions around targeting children—includes the collection of children's data through cookies, tracking pixels or data harvesting SDKs should be considered.

Beyond the *Privacy Act* review, the scope of harmful data harvesting about children is so significant that it warrants a multi-pronged approach. We note that the Children and Media

[26] BBC 2022 'Molly Russell inquest: Father makes social media plea' *BBC* https://www.bbc.co.uk/news/uk-england-london-63073489
[27] Meta 2023 *Continuing to Create Age-Appropriate Ad Experiences for Teens* https://about.fb.com/news/2023/01/age-appropriate-ads-for-teens/

Australia have proposed adding privacy considerations to the National Classification System to determine the suitability of content for their children. This is worth considering.

***C**. What would be the impact of the proposals in relation to sale of personal information on individuals, businesses and government?*

More clarification is needed for how Proposals 20.1 and 20.2 will reduce privacy and competition harms in vertically integrated companies. In these corporate structures, businesses will collect extensive amounts of data and trade within themselves. Given the intense integration of data across the large platforms and services, we caution that the 'Trading' category captures these internal activities within large corporate structures and avoids creating an accidental and vast loophole.

We also note the consent requirement in Proposal 20.4: it is crucial that 'consent' under a future *Privacy Act* does not fall captive to what noted advocate Dr Johnny Ryan labels as a 'thin veneer of compliance theatre'. We encourage, firstly, the use of the stricter GDPR definition of consent rather than the version from the *Australian Privacy Principles*. Additionally, we encourage an end to the cookie banner 'consent spam' that has flourished under the GDPR framework, which causes user inconvenience and confusion. We advocate for a more user friendly regime where, for instance, settings can be saved at the browser level and applied across digital services.

There must also be serious consequences for businesses who breach the consent requirement. In the UK, the Information Commissioner's Office confirmed that a key standards-setting body for digital advertising, the IAB, relied on non-compliant transparency and consent frameworks.[28] This significant finding was undermined by the ICO's failure to take action, despite strong arguments that the IAB was responsible for the largest-ever data breach in the UK.[29]

[28] Information Commissioner's Office 2019 'Update report into adtech and real time bidding' https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf

[29] Johnny Ryan 2020 'The ICO's failure to act on RTB, the largest data breach ever recorded in the UK' Brave,

Children and young people

While the Review consultations did not specifically ask about children and young people, we note that a number of the proposals address their privacy concerns in ways that we wanted to support and comment on that were not addressed above.

A. *Proposal 16.1 and 16.2: Age of a child and age of presumption of consent*

We welcome the proposal that the age at which someone is defined as a child is 18 years old (proposal 16.1). This is in keeping with Australia's commitments under the UN Convention on the Rights of the Child.[30]

This is a strong and necessary bulwark against the attempt to reduce privacy protections for 16 and 17 year olds currently proposed by industry in the drafting of the Online Safety Codes.[31] Here, industry is proposing not providing privacy-by-default protections, and geolocation data protections, to young people aged 16 and 17 by introducing the concept of a 'young Australian child' (aged under 16) versus an 'Australian child' (aged under 18).[32] Reducing protections for 16 & 17 year olds is not in keeping with international norms, and we welcome the clarification via the *Privacy Act* review that is not in keeping with the intent of the Attorney General.

Proposal 16.2 recommends keeping the presumption of the age of capacity at 15 years old (noting that there may be some confusion about whether it is 15 and over as described in the OAIC's guidance,[33] or over 15 as described in the *Privacy Act* review paper). A blanket age is arbitrary and may interfere with young people's right to access the digital world. In this context the exemptions for preventative and counselling services are very welcome, but they may not secure young people's right to access for other reasons; such as leisure or socialisation. In principle, requirements for parental consent should not arbitrarily remove capable young people from the digital world.

More importantly, requirements for parental consent may fail to materially protect children for two reasons. Firstly, because too often parents have no meaningful option but to consent. For example, where parents are asked to consent to EdTech products in the classroom that include data trackers, 'declining' is not a viable option if they wish their child to have an education.[34] Secondly where services exploit data or cause harm through data processing, having a parental click 'I agree' is of material benefit to children. Parental consent does not affect children's rights to privacy nor protection from harm,[35] and is not an especially helpful response to the issue. It is unhelpful, because parental consent is not the same as 'parental

[30] UN General Assembly 1989 *Convention on the Rights of the Child* https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child
[31] Industry Associations 2023 Revised Online Safety Codes https://onlinesafety.org.au/
[32] Reset.Tech Australia 2023 *Response to the Revised Online Safety Codes* LINK
[33] Office of the Australian Information Commissioner. *Children and Young People* https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/children-and-young-people
[34] See for example Frida Alim, Nate Cardozo, Gennie Gebhart, Karen Gullo, and Amul Kalia 2017 Spying on Students: School-Issued Devices And Student Privacy https://www.eff.org/files/2017/04/13/student-privacy-report.pdf
[35] Jelena Gligorijević 2019 'Children's Privacy: The Role of Parental Control and Consent' *Human Rights Law Review* https://doi.org/10.1093/hrlr/ngz004

control' or 'parental oversight',[36] and does not necessarily mean that young people will receive greater support from their parents. Parental consent simply places additional burdens onto parents to accept or reject privacy risks, when they are not best placed to manage these risks.

With this in mind, the focus must remain on stronger protections for all children under 18 when it comes to the way their data is collected, used and disclosed. This includes requiring reforms to systems and process used platforms to mitigate against harms in the first instance, and requiring transparency and accountability to this through risk assessments and independent audits, etc. Some of these measures are proposed—or potentially proposed via the Online Privacy Codes—in the review, and these may be a more effective focus.

There should be no confusion about the difference between 'age at which young people are entitled to stronger protection' and 'age at which young people are entitled to the presumption of capacity'. These are not binary decisions and requiring additional protections does not mean requiring additional parental consents. Young people's best interests dictate that these different requirements be considered independently.

B. *Proposal 16.3: Requiring clear and transparent privacy policies and collection notices*

Requiring privacy policies and collection notices to be clear and accessible to young users is welcome. Only 7% of young people feel confident that they have understood the 'terms and conditions' that they agree to online, and only 4% of young people say they always read the privacy policies and collection notices presented to them.[37] Young people are not at fault here; 9 out of 10 apps popular with young people in Australia require a tertiary degree to understand, and take on average 1 hour and 46 minutes to read.[38] They also contain a number of manipulative dark patterns, designed to 'trick young people' into agreeing to additional unnecessary data collection.[39] Clear and transparent, age appropriate, privacy policies and collection notices will go some way to remedying this situation.

But again, consent alone cannot justify data exploitation or causing harm through data processing. Firstly, whether young people understand the collection notices or not, young people often have no meaningful alternative but to click 'I accept'. Digital platforms and online services are integral to the experience of growing up in 2023, and many young people do not have a meaningful choice but to take part. As young people explained as part of an academic panel recently, "we have no choice but to use them", and "there really isn't any other way".[40]

---

[36] Simone van der Hof & Sanne Ouburg 2021 *Methods for Obtaining Parental Consent and Maintaining Children Rights*
https://euconsent.eu/download/methods-for-obtaining-parental-consent-and-maintaining-children-rights/

[37] 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/

[38] 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/

[39] 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/

[40] Kate Mandell & Rys Farthing 2023 *Digital Child Seminar: Privacy and the 'trade off' of growing up digital in Australia*
Centre for the Digital Child, March 23rd online

Secondly, presenting understandable policies and collection notices does not mean that platforms and services will not violate young people's rights. Even where clear and transparent terms are offered, children and young people should be asked to 'click to agree' to harm. As young people described this "at the very least we need to know the risks" through understandable collection notices and privacy policies, but what they were potentially more interested in was "what are the ways to lessen the risks".[41]

While welcome, the emphasis must remain on requiring reforms to systems and process used platforms to mitigate against harms in the first instance.

C. *Proposal 16.4: The introduction of the Best Interests principle in the fair and reasonable test*

We welcome the introduction of children's best interests into the consideration of whether a collection, use or disclosure is fair and reasonable in the circumstances. This has the potential to address a number of privacy violations that young people currently experience that may not be immediately addressed in the *Review* or proposed Code, such as the use of data to develop or refine extended use designs.

Extended use designs are not in children's best interests, and they can be especially vulnerable to these design features that attempt to keep young people 'hooked' on a digital product. These include push notification designed to pull young people back into an app,[42] endless scroll, content recommender algorithms that are "optimized for addiction"[43] (i.e., "trained" to maximize the amount of time young people spend watching videos)[44] to removing video time markers[45] or other features that might remind young people to log off and take a break.[46] Extended use designs can harm children. In rare cases, this extends to a medical addiction, called Internet gaming disorder,[47] but more commonly, extended use

[41] Kate Mandell & Rys Farthing 2023 *Digital Child Seminar: Privacy and the 'trade off' of growing up digital in Australia* Centre for the Digital Child, March 23rd online

[42] De Montfort University 2022 *DMU research suggests 10-year-olds lose sleep to check social media* https://www.dmu.ac.uk/research/research-news/2022/dmu-research-suggests-10-year-olds-lose-sleep-to-check-social-media.aspx#:~:text=Research%20support-,DMU%20research%20suggests%2010%2Dyear%2Dolds%20lose%20sleep%20to%20check,up%20to%20use%20social%20media

[43] Allison Zakon 2022 'Optimized for addiction: Extending product liability concepts to defectively designed social media algorithms and overcoming the communications decency act' *Wisconsin Law Review* (5) https://ssrn.com/abstract=3682048

[44] Kevin Roose 2019 'The Making of a YouTube Radical' *New York Times*

[45] Louise Matsakis 2019 'On TikTok, There Is No Time' *Wired*

[46] For example, Instagram allows users to set daily time limits to prevent overuse. Consumer's used to be able to self define their daily limit, including setting limits at 10 or 15 min. Earlier this year, Meta set a new 'limit' to these daily limits. Consumers can only now set a daily limit of 30 minutes or more (See Natash Lomas 2022 'Instagram quietly limits 'daily time limit' option' *TechCrunch*)

[47] As defined in DSM5 onwards (See American Psychiatric Association 2013 *Diagnostic and Statistical Manual of Mental Disorders. 5th edn*. American Psychiatric Publishing Arlington). See also Cecilie Andreassen 2015 'Online social network site addiction: A comprehensive review' *Current Addiction Reports* doi:10.1007/s40429-015-0056-9, who explores the potential for social networking sites to be addictive

design causes constant relationship harm. Intrafamily conflict around screen time is rife,[48] and many teachers report conflict in the classroom over the use of digital devices.[49] These can also cause physical harm, because they cost young people sleep.[50] Extended use designs and many other issues are not explicitly covered by the *Privacy Act* review and do not necessarily need to be. Rather we describe them as an example of the capacity of introducing children's 'best interests' principle into the fair and reasonable test.

Additionally, it is important to engage children and young people in the development of guidance around what the best interests principle means in practice. In our research with young people around online privacy and regulation, young people put it plainly; they wanted their personal information "only collected and used in ways that advance their best interests, but this needs specifics about what it means. Young people need to decide what young people's best interests are."[51] The OIAC should undertake meaningful deliberations with young people about what the 'best interests' principle means in practice, with regards to the fair and reasonable test.

D. *Proposal 16.5: A Children's Online Privacy Code*

We would like to particularly welcome proposal 16.5, introducing a Children's Online Privacy Code. Reset.Tech, alongside many partners in the children's rights space, has been calling for such a code[52] to address the exploitative and harmful use of children's data. The exploitative processing of data is both a privacy violation in itself, and often leaves young people vulnerable to other harms, such as safety risks where they location data is exposed, to commercial risks where they are served manipulative behavioural advertising.[53]

[48] Sarah Domoff, Aubrey Borgen, Sunny Jung Kim, Jennifer Emond 2021 'Prevalence and predictors of children's persistent screen time requests: A national sample of parents' Human Behavior and Emerging Tech doi.org/10.1002/hbe2.322

[49] Abigail Hess 2019 'Research continually shows how distracting cell phones are—so some schools want to ban them' *CNBC*

[50] See De Montfort University 2022 as above

[51] Rys Farthing *et al* 2023 '"It Sets Boundaries Making Your Life Personal and More Comfortable": Understanding Young People's Privacy Needs and Concerns' *Technology & Society Magazine* https://ieeexplore.ieee.org/document/10063169

[52] For more information about this coalition see https://www.childrensdatacode.org.au/

[53] Reset.Tech Australia 2023 *Submission to the Senate Economic Reference Committee's Inquiry into International Platforms*

The UK implemented an Age Appropriate Design Code in 2020[54], followed by Ireland,[55] France,[56] the Netherlands,[57] Sweden,[58] and more recently California[59] among others.[60] These Codes have increased privacy protections for young people in these jurisdictions, which has left Australian children with less privacy comparatively.[61]

An Online Privacy Code is a welcome move to address some of the systemic harms young people face in the online world. This is one way to ensure the necessary focus on reforming systems and process used platforms, to prevent harm to children in the first instance.

D.i. Code developers

We note that the Code developer is yet to be appointed, and would strongly urge the government to appoint the OAIC to undertake this task, in accordance with proposal 5.1. Co-regulation, or allowing industry to draft their own codes, does not work to secure young people's interests. Where this has been tried in Australia around online safety, it led to demonstrably weaker proposals around children's safety[62] which were (at least) initially rejected by the regulator. This should not be understood as a 'one-off' incident. The mis and disinformation code authored by industry has also required subsequent intervention from the ACMA to strengthen[63], and in the EU too voluntary codes have ultimately had to be subsumed within the *Digital Services Act* because they failed to deliver change.[64] Where industry authors codes, weaker protections are offered and regulators inevitably have to step up. The issue is that children continue to be harmed during this unnecessary delay.

---

[54] *Age Appropriate Design Code* 2020
https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/
[55] Data Protection Commission 2021
https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf
[56] CNIL 2021 https://www.cnil.fr/fr/les-droits-numeriques-des-mineurs;
[57] Ministry of the Interior and Kingdom Relations 2021
https://codevoorkinderrechten.nl/wp-content/uploads/2021/07/Code-voor-Kinderrechten-Wordversie_EN.pdf
[58] The Swedish Authority for Privacy Protection 2021
https://www.imy.se/globalassets/dokument/rapporter/the-rights-of-children-and-young-people-on-digital-platforms_accessible.pdf
[59] California 2022 *Age Appropriate Design Code*
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273
[60] European Commission 2022 *Better Internet for Kids+ Strategy*
https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids
[61] Fairplay 2022 *Global Platforms Partial Protections*
https://fairplayforkids.org/wp-content/uploads/2022/07/design-discriminations.pdf
[62] Reset.Tech Australia 2022 *How outdated approaches to regulation harm children*
https://au.reset.tech/news/how-outdated-approaches-to-regulation-harm-children-and-young-people-and-why-australia-urgently-needs-to-pivot/
[63] Office of the Minister for Communications 2023 *New ACMA powers to combat harmful online misinformation and disinformation*
https://minister.infrastructure.gov.au/rowland/media-release/new-acma-powers-combat-harmful-online-misinformation-and-disinformation#:~:text=The%20Albanese%20Government%20will%20legislate,misinformation%20and%20disinformation%20in%20Australia.
[64] For example, obligations under the self-regulatory *Code of Practice on Disinformation* (2018) were found to be inadequate, and replaced by obligations within the *Digital Services Act*.

Co-regulation is uniquely unpopular when it comes to children's online privacy, and may have the effect of eroding public trust in the Codes. In a poll of Australian adults, 76% said they would prefer an independent regulator like the Information Commission to draft the 'rules' around children's privacy online.[65] Ten percent said they would prefer parliament to write the rules, with only 5% indicating that they thought Social Media companies should be involved in drafting the rules. We asked if this would affect trust – 71% of respondents said they would not trust social media companies to write the 'rules'. Likewise, when we polled young people themselves, 46% said they would prefer an independent regulator draft the rules, and 27% said they'd prefer parliament do so. 52% said they would not trust social media companies to write the rules.[66]

D.ii. Contents of the code

We support the focus on outlining how children's best interests can and should be realised through the contents of the Code. To ensure a Code creates the reforms to platform's systems and process reforms that are so urgently needed, systemic requirements like risk assessments must be part of the Code, alongside side requirements for specific rules like not collecting unnecessary geolocation data.

While the contents of the Code is yet to be developed, we would like to offer in advance all the materials and research we have gathered in this space, including polling data and extensively qualitative data from young Australians about what they believe a privacy code for the digital world should address, as well as content ideas from civil society that we would be delighted to share. For example, one group of young people we worked with in Western Sydney to develop a youth-authored version of a privacy code, developed 14 key principles.

[65] Reset.Tech Australia 2022 *How outdated approaches to regulation harm children* https://au.reset.tech/news/how-outdated-approaches-to-regulation-harm-children-and-young-people-and-why-australia-urgently-needs-to-pivot/

[66] Reset.Tech Australia 2022 *How outdated approaches to regulation harm children* https://au.reset.tech/news/how-outdated-approaches-to-regulation-harm-children-and-young-people-and-why-australia-urgently-needs-to-pivot/

Young people's ideas for privacy principles in the online world

To realise young people's best interests young people's their personal information should:

1. Must be only collected and used in ways that advance their best interests
2. Be collected and used only when it is needed. No one should be able to collect data that they do not strictly need, including GPS data and "cookies". Don't collect or use these unless they are needed
3. Be collected and used only when young people have clearly been asked:
    - Agreeing to confusing privacy policies, or out of date policies, is not enough. Fine print isn't okay, it's got to be clear
    - Young people should be asked about all the types of information that is going to be collected, and all the ways it is going to be used. A single 'yes' or 'no thanks' button isn't good
4. Personal information should not be used in any ways other than what young people were clearly asked about
5. Young people should not be pushed or tricked into agreeing to data collection, for example:
    - Dark patterns - don't make the 'yes' button bigger than the 'no thanks' button
    - Rename "cookies" as "data grabbers"
6. Be collected, used and stored in safe and secure ways
7. Be kept for as long as is it needed only
8. Not be sold or traded to other companies
9. Young people should have the right to request it be deleted
10. Companies that collect and use young people's data should be accountable to them. If something goes wrong, it should be the company's responsibility to provide help and support and fix it
11. Not be used in ways that can harm, including in algorithms that make apps addictive or encourage harmful content in 'for you' feeds
12. Companies should have to be transparent about what information they are collecting, and who they are sharing or selling it to. This means being clear with each individual
13. Young people should be supported and educated about privacy, their rights and risks
14. Don't have advertising turned on by default for young people. Young people should be able to opt-in to advertising overall, and also be able to choose if they want their data used to personalise these ads or not.

We want to see all young people under 18 protected, as this is their rights. But we would also encourage you to think about protections right up until the age of 25, to ensure extra safety and privacy for young people as they transition into adulthood.

D.iii. Enforcement of the code

Ensuring that the Online Privacy Code for Children creates real change for young people requires strong enforcement. We note that the OAIC would need to be adequately resourced to ensure this. The OAIC received comparatively low levels of funding, which may reduce their capacity to effectively enforce the Code.

Approximate funding per person, in AUD, of different Information Commissioners[67]	
$1.11pp	Office of the Australian Information Commissioner. Australia Based on an annual budget $28,487,000 for 2021-22, Australian population of 25,739,256 in 2021
$1.96pp	Information Commissioner's Office, UK Based on an annual budget £70,625,526 for 2021-22, UK population of 67,081,000 in 2020
$6.04pp	Data Protection Commission, Ireland Based on an annual budget €19,128,000 for 2021-22, Irish population of 5,011,500 in 2021 (Ireland also has EU wide data protection functions)

Enforcements of similar Codes in the UK and Ireland have been active and involved active and early use of investigative powers and audits,[68] and within two years had six ongoing investigations and were issuing fines for practices around children's data.[69] This experience suggests that Codes will not simply come to life through voluntary adoption by industry; the OAIC needs a muscular response that requires strong powers and adequate resources.

[67] Reset.Tech Australis 2022 *The Future of Digital Regulations in Australia* https://au.reset.tech/uploads/the-future-of-digital-regulations-in-australia.pdf
[68] Such as those undertaken with the gaming industry to develop specific guidelines, see ICO 2023 *New guidance to industry issued for game developers on protecting children* https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/02/new-guidance-to-industry-issued-for-game-developers-on-protecting-children/
[69] ICO 2022 I*CO could impose multi-million pound fine on TikTok for failing to protect children's privacy* https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-could-impose-multi-million-pound-fine-on-tiktok-for-failing-to-protect-children-s-privacy/

Appendix

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 1. An analysis of the number of trackers and permission requested by apps,[70] by popularity in Australian downloads from the Google Play store for Android[71]

[70] From Exodus Privacy 2023 *Check an app* https://exodus-privacy.eu.org/en/
[71] 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 2. An analysis of the number of trackers and permission requested by apps,[72] for ten apps popular with Australian teens.[73]

[72] From Exodus Privacy 2023 *Check an app* https://exodus-privacy.eu.org/en/
[73] 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