The Australian Privacy Principles & the Rights of Children and Young People

A briefing note

Reset.Tech Australia
April 2025

Summary

This briefing paper is prepared in advance of a workshop on the development of the Children's Online Privacy Code (the Code). It documents some connections between the Australian Privacy Principles (APPs), children's rights and young people's perspectives, with a view to enriching a conversation about what the Code could and should address to improve children's privacy. It covers:

APP	Considerations for children
1. Open & transparent management of personal information	Informing children of their rights on the online world and providing them with processes to seek remedies
2. Anonymity & pseudonymity	Empowering children to navigate the online world without identifying their real names to companies and internet providers, allowing them to take some charge of their privacy
3. Collection of solicited information	Ensuring providers do not over-collect, or unfairly or unlawfully collect, children's personal information
4. Dealing with unsolicited information	Ensuring providers responsibly dispose of personal information they should not have collected
5. Notification of the collection of information	Informing children when, and under what conditions, their personal information is collected, which supports autonomy and agency
6. Use or disclosure of personal information	Setting obligations for how providers use children's information, and how they disclose this information to others, which reflects their rights to privacy and protection from digital harms
7. Direct marketing	Providing guardrails for how and when providers can market to a child, and protecting children from commercial exploitation
8. Cross-border disclosures	Requiring a provider ensures overseas recipients of children's personal information do not breach the APPs, reflecting the transnational nature of children's rights
9. Government identifiers	Preventing providers from adopting, using, or disclosing government identifiers such as passport numbers (exceptions apply), helping to protect children's identity
10. Quality of personal information	Ensuring providers maintain children's personal information to be accurate, complete, up-to-date, and relevantly used and disclosed, maintain correct and up-to-date information on children. There are additional expectations to only use and disclose relevant information and to prevent prejudice and unfair outcomes based on faulty data
11. Security of personal information	Requiring providers to take steps to protect children's personal information from unauthorised acts of access or interference, or loss, which helps to protect them from breaches and digital harms like ID theft, scams, etc
12. Access to personal information	Empowering children to access their own personal information
13. Correction of personal information	Providing ways for children to correct their own personal information

Contents

Reset.Tech Australia is an independent, non-partisan policy research lab committed to driving public policy advocacy, research and civic engagement to strengthen our democracy within the context of technology. We are the Australian affiliate of Reset.Tech, a global initiative working to counter digital threats to democracy. We are grateful to the Internet Society Foundation for their support for this work.

Introduction

"Can the government make a baseline about how our data can be protected?" — Young Person[1]

The *Privacy Act 1988* arises as a regular example of Australia's privacy deficiencies and outdated data protection environment. While this position is hardly contestable among privacy advocates, it is important that the dialogue around privacy reforms in Australia takes place with a clear view of how the Act currently operates and where privacy and data rights currently 'live' in the environment.

It was introduced to give effect to Australia's agreement to implement the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,*[2] and Australia's obligations under Article 17 of the *International Covenant on Civil and Political Rights*,[3] but has largely been static since. Given that over 35 years have passed since the Act was introduced and that it was drafted before the arrival of internet technology, reform of the Act and its operation are well overdue.

The critical parts of the Act are the Australian Privacy Principles (APPs), nestled in Schedule 1 of the legislation (see Figure 1). Where the Act empowers the Office of the Australian Information Commissioner (OAIC) and enlivens a range of functions and activities relating to privacy oversight and enforcement, the APPs provide the detail on what Australians' privacy protections are, and what organisations in scope of the Act need to do to realise them.

Late last year, the *Privacy and Other Legislation Amendment Act 2024* was passed. 'Tranche 1' of the privacy reforms—as they have become known—may have fallen short of the 'bullseye' many advocates desired.[4] However, they offer signs of how a more muscular privacy regime could operate in the future. Especially for children. The Amendment Act introduced a mandate for the OAIC to develop a Children's Online Privacy Code (the Code).

The Code will ensure that the objectives of the APPs reach into children's online worlds, and when it comes into force, will operate in tandem with the APPs.The two instruments should be mutually reinforcing. In other words, to shape the development of the Code in children's best interests, we need to reflect on the APPs. This report takes an initial step to consider what that project of integration and adaptation needs to look like.

Who does the *Privacy Act* and the Code apply to?

The *Privacy Act* is not universal in application. Its provisions are intended to regulate how Australian Government agencies and organisations with an annual turnover of more than $3 million handle the personal information of individuals. These are called 'regulated entities' in the Act (or sometimes just providers or platforms in this document for short).

While the exact details of the Children's Privacy Code are being drafted, it is intended to cover:

- Social media companies, designated internet services and relevant electronic services as defined under the *Online Safety Act*, that are likely to be accessed by children' (excluding health care providers), and
- All entities already regulated by the APPs, under the *Privacy Act*.

[1]Quote from a young person, unpublished focus group data
[2]Organisation for Economic Cooperation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* https://www.oecd.org/en/publications/2002/02/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of- personal-data_g1gh255f.html
[3]UN General Assembly 1966 *International Covenant on Civil and Political Rights* https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
[4]That were proposed in, for example, the *Privacy Act Review Report* Office of the Attorney General 2023 *Privacy Act Review Report* https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

Privacy and children's rights

"Privacy is vital to children's agency, dignity and safety and for the exercise of their rights — it is also central to the realisation of children's rights as a whole. Children's personal data are processed to offer educational, health and other benefits to them."[5]

This report attempts to sketch out what the key considerations around the APPs might be from a child rights perspective, and includes the voices of children and young people themselves where possible. Some sections are long, where the connections and interdependencies are better known or better researched. Some sections are short, reflecting spaces where the intersection of APPs and children's rights has been less clearly identified. Some will be clear and others will require extrapolation from connected conversations. The contours of these connections speak to the need to reflect on the APPs from a child rights perspective more clearly as the Code is being drafted, and in general, as the debate about digital regulations and young people moves ahead.

The debate about regulating children and the online world continues in Australia; from the *Online Safety Amendment (Social Media Minimum Age) Act 2024* placing new restrictions on children's ability to lawfully access social media accounts under the age of 16, to mobile phone bans in public schools.[6] Alongside this debate about regulating for children's safety outcomes — which appears to be largely focussed on limiting access— sits a regulatory opportunity within the Children's Online Privacy Code. It seeks to protect children by safeguarding the way the digital world uses them (or their data, specifically), rather than the way they use the digital world. By addressing privacy, and the use and misuse of children's data, the Code has the capacity to make a systemic intervention to change the way online platforms and services operate while ensuring children's access is protected.

The debate about restrictions does not limit the impact of the Code, in fact it emphasises the Code's rights-enhancing capacity. The Code will regulate where the limited bans end; from online gaming services, to YouTube and video streamers, to 16 & 17 year olds on social media platforms, to covered apps on phones used just outside of the school gates. But more importantly, it has the capacity to 'limit the machine' rather than limit the users. This is the type of systemic, upstream reform that children's advocates have been rallying behind for years.

The Code has implications for the advancement of children's rights across the country. The digital world is now a key site where young people's rights can be advanced or violated. As the United Nations Committee on the Rights of the Child (the UN Committee) describes in its *General Comment No.25 (2021) on children's rights in relation to the digital environment (*the General Comment)*,* "the rights of every child must be respected, protected and fulfilled in the digital environment."[7]

The protection of children's privacy in particular, via laws and regulations such as this Code is an essential duty of the state in advancing children's rights. The UN General comment makes clear that "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."[8] We welcome this Code as one small step towards this goal.

[5]Paragraph 67, 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
[6]Marilyn Campbell & Elizabeth Edwards 2024 'We looked at all the recent evidence on mobile phone bans in schools – this is what we found' *The Conversation* https://theconversation.com/we-looked-at-all-the-recent-evidence-on-mobile-phone-bans-in-schools-this-is-what-we-found-224848
[7]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
[8]Paragraph 70, 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

We offer this report not as the 'final say' on children's rights and the APP. We offer this as a note to explore what is known, and document what is not currently known, to start the conversation between the child rights canon and the Australian privacy framework, to enhance the Code development process.

	Concept	Content	Category
1	Open and transparent management of personal information	Binds regulated entities to the APPs as a whole. Ensures privacy policies are clear, current, and comprehensive	Rights as a data subject
2	Anonymity and pseudonymity	Facilitates people to provide their information in an anonymous or pseudonymous way (with exceptions)	
3	Collection of solicited personal information	Sets the parameters for permissible information collection, with enhanced responsibilities when sensitive information is involved	
4	Dealing with unsolicited personal information	Provides responsible handling practices when APP regulated entities receive unsolicited information	
5	Notification of the collection of personal information	Outlines when and in what circumstances an APP entity must notify individuals about collecting their information, such as through collection notices. Enhanced responsibilities when sensitive information is involved	
6	Use or disclosure of personal information	Sets the parameters for permissible use and disclosure of personal and sensitive information	Handling personal information
7	Direct marketing	Provides the conditions for permissible direct marketing practices involving use or disclosure of personal information	
8	Cross-border disclosure of personal information	Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas	
9	Adoption, use or disclosure of government related identifiers	Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual	
10	Quality of personal information	Obliges APP regulated entities to take reasonable steps to ensure the personal information it collects, uses, and discloses is accurate, up to date and complete (noting use and disclosure must also be relevant to the collection purpose)	Information integrity and security
11	Security of personal information	Sets out a comprehensive set of expectations for guarding personal information against misuse, interference and loss. Further expectations for preventing unauthorised access, modification or disclosure	
12	Access to personal information	Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity	
13	Correction of personal information	Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals	

Figure 1 - Summary of the Australian Privacy Principles (APPs)[9]

[9]Adapted from OAIC 2025 *Australian privacy principles quick reference* https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference

Methods

This briefing paper draws together two sources of information, to attempt to connect where the Australian Privacy Principles (the 'APPs') and children's rights connect:

- Desk research around the international child rights guidance and most specifically the United Nations Convention on the Rights of the Child[10] (the Convention) and the General Comment No. 25 (2021) on Children's Rights in relation to the Digital Environment (the General Comment)[11] issued by the United Nations Committee on the Rights of the Child (the UN Committee).

- Existing qualitative and quantitative research with young Australians under 18 undertaken by Reset.Tech Australia in the last 5 years. Where research has connected young people's perspectives or digital experiences with relevance to the Australian Privacy Principles, we have included summaries of findings reinforced by quotes from participating young people as much as possible.

These two commentaries, around children's rights and previous research, do not map perfectly to the APPs. The APPs in practice are interconnected and inextricably linked, as are children's rights and often, children's conversations on the issues. Rather this briefing note attempts to map the rough contours of these bodies within the APP framework.

We are grateful to support from AWO for an initial overview of the APPs.

[10]United Nations General Assembly 1989 *Convention on the Rights of the Child*
https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child
[11]Committee on the Rights of the Child 2021 *General comment No. 25 (2021) on children's rights in relation to the digital environmen*
https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021

APP 1: Open & transparent management of personal information

APP 1 sets out the overarching, rights-driven arrangement between individuals and the organisations collecting, using, and disclosing data on them. APP 1 makes it clear that these organisations are under a series of obligations – cutting across APP 1 to APP 13 – to take both active steps to ensure privacy protection, as well as avoiding downstream consequences like breaches and data errors.

More specifically, APP 1 requires that organisations in scope of the *Privacy Act* ('regulated entities' or simply 'company' for shorthand here) manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

This means that companies are required to take reasonable steps to implement various systems and processes to ensure they can deal with enquiries or complaints from individuals about their data. It also requires companies and services to have a clearly expressed and up-to-date privacy policy available (usually on their website) that includes particular types of information.

This includes how the company manages the personal information it collects, and the information flows associated with it.[12] As of December 2026, the new APPs 1.7-1.9 will require companies to take a further step of disclosing to the public in their privacy policy what, if any, their use of automated decision-making is.

Interacting child rights principles

Transparency is an explicit requirement noted in the *General Comment*, both in terms of policy development and the regulation of the activities of companies, but also in guiding the State as it manages and processes children's data. The UN Committee sets out in the General Comment a number of obligations around transparency, including requiring:

- Legislation and regulation that requires transparency in data protection: "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."[13]
- Ensure businesses are transparent: "require (digital business likely to be accessed by children) to maintain high standards of transparency and accountability and encourage them to take measures to innovate in the best interests of the children.[14]
- Requiring transparency in best interest assessments, where they restrict freedom of expression, or where they use administrative data about children.[15]

Transparency affects the effective implementation of other rights for children. These include:

[12]OAIC nc Chapter 1: APP 1 Open and transparent management of personal information https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information
[13]Paragraph 70, 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
[14]Ibid. Paragraph 39
[15]Ibid. Paragraphs 13, 59, 73

- The right to access information[16]. The digital world provides a unique setting where young people are able to access information. However, many of the business models underpinning much of the digital world involves an implicit trade between access to information and personal data. Without openness and transparency, the nature of this relationship remains obscured and this power asymmetry disadvantages children as they attempt to navigate the modern digital world. This may affect how they access (or do not access) information, and which sources of information they feel safe and confident in accessing.
- The right to education[17]. The global educational environment is increasingly adopting new technologies and softwares (often called 'EdTech'). Many commercial EdTech products have complicated privacy implications, including processing children's data where it is not clear that their privacy policies nor complaint mechanisms are available to children or their guardians, often relying instead on school or education board level 'consent' practices.[18] Young people's ability to engage with, or more specifically their ability to trust, EdTech providers can therefore affect their ability to engage and benefit from the modern tools of pedagogy. This also applies to technology in health care (HealthTech) and children's right to health, including mental health.[19]
- The right to be protected from (commercial) exploitation[20]. The *General Comment* notes that "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. These may result in violations or abuses of children's rights, including through advertising design features that anticipate and guide a child's actions, including 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."
- The asymmetry of power between commercial providers and users leaves young people vulnerable to commercial exploitation from 'surveillance capitalism' models,[21] and online scams. 'Contract' risks are now regarded as one of the '4Cs' of online risks experienced by children.[22]

More broadly, the *General Comment* notes the importance of developing young people's broader understanding about the way the digital world operates — particularly the data fuelled infrastructure that underpins it. The UN Committee describes the role for States in providing for critical digital literacy in education and skills development. It notes that it is "of increasing importance that children gain an understanding of the digital environment, including its infrastructure, business practices, persuasive strategies and the uses of automated processing and personal data and surveillance, and of the possible negative effects of digitalization on societies."[23] In practical terms, this means awareness raising in the formal curriculum; but also the ability to expect (and demand) openness and transparency at the point of service delivery of digital access and engagement in games and social media as well as education services and communication access.

Finally, effective openness and transparency requires due regard to children's evolving capacity, which we will explore in the context of APP5.

---

[16]Articles 13 and 17, United Nations General Assembly 1989 *Convention on the Rights of the Child*
https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child
[17]Ibid. Articles 28 and 29
[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]Article 24, United Nations General Assembly 1989 *Convention on the Rights of the Child*
https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child
[20]Ibid. Article 32
[21]Donnell Holloway 2019 'Surveillance capitalism and children's data: the Internet of toys and things for children' Media International Australia
https://journals.sagepub.com/doi/10.1177/1329878X19828205
[22]OECD 2021 *Children in the digital environment revised typology of risks*
https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/01/children-in-the-digital-environment_9d454872/9b8f222e-en.pdf
[23]Paragraph 105, 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

What Australian young people say about this

"Privacy and transparency are similar, if people are well informed in a concise manner, they can agree or not. It's dangerous not to know."[24]

In July 2021, we ran a poll with 400 16- and 17-year old Australians to ask them about their perceptions about privacy policies and terms of service statements as 'meaningful' consent mechanisms. Key findings suggest that:

- Less than one third of young people feel they understand the terms and conditions on platforms to any degree. Seven percent of young people were confident that they understand all the terms of service, 21% were quite confident that they understand most of it, 41% were a little confident that they understood 'bits' but not most of the terms, and 20% were not confident and felt they did not understand most of the terms of service. (10% were not sure).
- The terms and condition documents themselves on digital platforms struggle to be relevant because young people did not read them. Only 4% of young people reported reading them all the time, 13% said they read them most of the time, 38% read them some of the time and 45% never read them.[25]
- Young people described not reading them because the documents themselves were problematic (see APP 5).
- Beyond the documents, young people described the consent model as problematic. Young people described: feeling forced to click to consent (they've got no choice, so why bother reading the documents 33%); platforms change them so often that it's not worth bothering (15%); platforms don't stick to them, so it's not worth bothering (13%); and they never address what young people are interested in (13%).[26]

The limitations of the consent model were described by a young expert who took part in a policy roundtable in May 2023. They noted that:

- "It's actually very difficult for a young person to just opt out of social media or online sources. For school as well, we use so many digital things, you always have to consent to the cookies. Opting in isn't really a choice anymore."
- "We all kind of depend on it, news, education, communication, or just for socialising with friends. If you're not on social media, you feel quite excluded from other people. Sports teams, clubs, group work – all of these take place online [in messenger groups], mainly through social media, which is easier than getting people's phone numbers."[27]

As one young man we interviewed outlined when we asked him if he trusted that his privacy was protected online, choice and consent did not feel relevant to him because he needed to use this technology anyhow; "'because you rely on it. So it's not even about whether or not you can, you don't really have the choice to trust it or not. You just have to use it because everyone else is on it. It isn't about whether or not you believe in your privacy."[28]

Another young person, who took part in a focus group in 2024 also expressed this dilemma: "by owning a phone you're accepting their terms, but how would you live without a phone and accepting their terms and conditions. It's not too good – it's life and death – what's the choice?"[29]

[24]Unpublished quote from a focus group
[25]We note that young people are not alone here. Research suggests that Australian adults also do not read privacy policies. According to 2023 OAIC research, only 21% of adults read privacy policies before sharing information. See OIAC 2023 *Australian Community Attitudes to Privacy Survey* https://www.oaic.gov.au/__data/assets/pdf_file/0025/74482/OAIC-Australian-Community-Attitudes-to-Privacy-Survey-2023.pdf
[26]Reset.Tech Australia 2021 *Did we really consent to this?* https://au.reset.tech/uploads/l01_resettechaustralia_policymemo_t_c_report_final-july.pdf
[27]Reset.Tech Australia 2023 *Capacity of the consent model* https://au.reset.tech/uploads/The-capacity-of-consent--Policy-Memo.pdf
[28]Reset.Tech Australia 2023 S*ubmission to the Senate Economic Reference Committee's investigation into the Influence of International Digital Platforms: Representing young people's thoughts and opinions* https://au.reset.tech/uploads/YPs-submission.pdf
[29]Unpublished quote from a focus group

This was reinforced by one young person who stated “I don't really think it means much (to click “accept”) since most people don't actually read it or comprehend what they're accepting to. And … I feel like because most people like all their friends and everyone, they've already accepted it. They feel like since it's like safe for them, and everybody's doing it that it's kind of the norm. So most people don't really think twice about it. And they mostly go ‘oh, it's just a notification, I'll just get rid of it’, and continue because they don't want to spend too much time dwelling on it, or thinking too much about what's actually behind it.”[30]

[30]Reset.Tech Australia 2023 *Young people and online privacy* https://au.reset.tech/uploads/For-Print-Final-report.pdf

APP 2: Anonymity and pseudonymity

APP 2 outlines that individuals should have the option of not identifying themselves, or of using a pseudonym, with some limited exceptions. These exceptions relate to issues of practicality, where the company requires the ability to identify the individual (such as to deliver online shopping purchases to a home address).[31] They also include an exception of 'required or authorised by law', which covers situations like opening a bank account or supplying a prepaid phone where legislation requires identification.[32]

This APP does not appear to be well utilised in the digital world, where the collection, use and disclosure of identifiable information, including of children, appears to underpin the business model of most large online platforms and AdTech systems.[33]

Examples provided by the OAIC of measures that could be adopted to facilitate anonymity or pseudonymity include:

- If using online or printed forms, a company could state that any personal identification boxes (such as name and address) are not mandatory fields
- If a company is communicating with an individual, they could inform that at the beginning of the communications that they may interact anonymously or by pseudonym[34]

Interacting child rights principles

From a child rights perspective, anonymity and pseudonymity are an important part of recognising a child's right to their own identity and their freedom of expression. It can also be viewed as a means by which a child can exercise a degree of control over their own personal information and assert their own right to privacy. The *General Comment* states that:

> "Many children use online avatars or pseudonyms that protect their identity, and such practices can be important in protecting children's privacy. States parties should require an approach integrating safety-by-design and privacy-by-design to anonymity, while ensuring that anonymous practices are not routinely used to hide harmful or illegal behaviour, such as cyber-aggression, hate speech or sexual exploitation and abuse."[35]

Anonymity and pseudonymity online can help advance a range of rights. For example:

- Young people who use digital services to seek help around sensitive issues such as sexuality or sexual health may find the perception of anonymity important. For example, the 2021 Australian

[31]OAIC nd *Chapter 2: APP 2 Anonymity and pseudonymity* https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-2-app-2-anonymity-and-pseudonymity, page 7.
[32]Ibid. page 6, 2.17
[33]We note in the context of the new *Online Safety Amendment (Social Media Minimum Age) Act 2024.* The Act provides that designated companies must take reasonable steps to verify a user's age sets minimum requirements. There is an industry narrative that the new minimum age restrictions will 'force' them into breaching APP 2. Respectfully, we reject this argument. There is a vast difference between providing anonymous or pseudonymous user experiences and enforcing a real-name policy. Putting aside that the collection of government IDs would need testing for the purposes of APP 3 and possibly APP 9, companies have a host of methods available to assess users' ages. It would be a cynical and defeatist view to accept the industry argument that the only option available to them is to eliminate any remaining potential for online pseudonymity or anonymity. Furthermore, we struggle to see how the APP 2 exceptions would apply to this use case, noting the Act does not sufficiently 'authorise' companies to effectively breach APP 2, nor is the impracticability argument obvious or uncontested
[34]OAIC nd *Chapter 2: APP 2 Anonymity and pseudonymity*
https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-2-app-2-a nonymity-and-pseudonymity, page 5
[35]Paragraph 77, 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

Survey of Secondary Students and Sexual Health found that after schools, the second most 'turned to' information source students use to young seek out information about sex and sexual health is the internet, with roughly two thirds of students reporting seeking health from the digital world.[36] The ability for online services to be able to identify young people via device IDs, cookies etc, may limit young people's legitimate interest to be anonymous.

- Anonymous and pseudonymous *public* profiles can reportedly help reduce contact risks. For example, the eSafety Commissioner encourages children to use their given name, a nickname or an avatar online instead of full real name online to make it difficult for individual predators to interact with children 'in front of' the screen.[37] While this advice about concrete steps are within the gift of children, parents and teachers, like all attempts to prevent predation that focus on victims behaviours the capacity here is 'downstream'. Platforms have the ultimate power to keep young people anonymous or pseudonymous, and perhaps if platforms implemented APP 2 effectively, this would safeguard children from (commercial) predation behind the screens as well as bad actor predation in front of the screens. This is the capacity of a systemically focussed code.

.

What Australian young people say about this

This APP was not extensively addressed in previous research, but when it came up, young people appeared to understand that anonymity online was not something they currently enjoyed. For example, in a survey around young people's trust in online privacy practices, one young person for example noted that "Although data may be anonymous, it still gives away information about you online that is collected by companies to create an online profile of you."[38]

[36]Jennifer Power, Sylvia Kauer, Christopher Fisher, Roz Bellamy & Adam Bourne 2022 T*he 7th National Survey of Australian Secondary Students and Sexual Health 2021* https://ssashsurvey.org.au/wp-content/uploads/2023/10/2021_SSASH_Report.pdf
[37]Office of the eSafety Commissioner 2025 *Anonymity and identity shielding*
https://www.esafety.gov.au/industry/tech-trends-and-challenges/anonymity
[38]Reset.Tech Australia 2023 S*ubmission to the Senate Economic Reference Committee's investigation into the Influence of International Digital Platforms: Representing young people's thoughts and opinions* https://au.reset.tech/uploads/YPs-submission.pdf

APP 3: Collection of solicited personal information

Collection is where most information flows begin. Setting guardrails on collection means that we can mitigate privacy risks at the source to create a more controlled flow of personal information.

APP 3 outlines when a company can collect personal information. It outlines three core requirements; the collection must be reasonably necessary to its functions and activities, it must be collected lawfully and fairly, and it should be collected directly from the individual. If the information is sensitive information, the company must seek consent.

Importantly, the collection of personal information must be 'reasonably necessary' to the functions or activities of the company. This is an objective test, meaning that a reasonable person who is properly informed would need to agree that the collection is necessary. An example where OAIC deemed collection was *not* reasonably necessary include collecting all of the information on a driver's licence (home address, licence number etc) if the organisation's function only required verifying if someone is over 18.[39] After the reasonably necessary threshold, the company must meet the test of collecting information by lawful and fair means (such as not relying on subterfuge or pressure), and collecting from the individual directly, where possible.

For the collection of sensitive information, the company needs to seek consent, unless an exception applies. Sensitive information includes:

- Racial or ethnic origin
- Political opinions or associations
- Religious or philosophical beliefs
- Trade union membership or associations
- Sexual orientation or practices
- Criminal record
- Health or genetic information, and
- Some aspects of biometric information.[40]

The OAIC outline that consent involves four key elements:

- The individual is adequately informed before giving consent
- The individual gives consent voluntarily
- That consent is current and specific, and
- The individual has the capacity to understand and communicate their consent.[41]

For children, the APP Guidelines states that companies handling children's data must decide if the child has the capacity to consent on a case-by-case basis. Where a child may lack maturity to understand what is being proposed then it may be appropriate for a parent or guardian to consent on their behalf.[42] As a general rule, companies can assume an individual over the age of 15 has capacity,[43] but this is not routinely followed by social media companies. There are certain specific exemptions to this requirement for consent such as where the collection is authorised by law.

Exemption to the requirement to collect information directly with consent exists for situations where

[39]OAIC nd *Chapter 3: APP 3 Collection of solicited personal information* https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information
[40]OAIC nd *What is personal information?* https://www.oaic.gov.au/privacy/your-privacy-rights/your-personal-information/what-is-personal-information
[41]OAIC nd *Chapter 3: APP 3 Collection of solicited personal information* https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information
[42]OAIC nd *Children and young people* https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/children-and-young-people
[43]Ibid.

companies are required to collect information by law or if it is unreasonable or impracticable to do so.[44] This latter exception is either too widely interpreted — despite OAIC guidance clarifying that being time-consuming, costly or simply inconvenient are not adequate reasons — or APP 3 is widely ignored.[45] Children's data is routinely gathered by third parties without consent, including and especially from online services, such as third party trackers in EdTech products,[46] mobile phone apps[47] or data collected about children by data brokers.[48] Analysis suggests that APP 3 should in principle prevent the prolific flow of data to data brokers across Australia, but an industry culture of poor compliance has prevented this.[49]

Interacting child rights principles

Controls around the collection of solicited information are part of the digital story of recognising children's agency, the right to their own identity and to exercise some control over the use by others of their own personal information. "Privacy is vital to children's agency",[50] and in the schema of the APPs, APP3 is perhaps the most agentic.

The added protections around sensitive information have the capacity to protect children from discrimination with regards to characteristics associated with the sensitive information. The UN Committee notes that "the right to non-discrimination requires that States parties ensure that all children have equal and effective access to the digital environment in ways that are meaningful for them", and that discrimination can arise from exclusion to the digital world, online hate speech *and* the inappropriate processing of data about special characteristics. "Forms of discrimination can arise when automated processes that result in information filtering, profiling or decision-making are based on biased, partial or unfairly obtained data concerning a child."[51]

APP3 also notes the need for meaningful consent when it comes to collecting, using or disclosing sensitive information. However, from a child rights framework, consent to processing any personal information is central to the realisation of young people's privacy and agency.

The UN Committee notes that consent must be meaningful;

> "Where consent is sought to process a child's data, States parties should ensure that consent is informed and freely given by the child or, depending on the child's age and evolving capacity, by the parent or caregiver, and obtained prior to processing data. Where a child's own consent is considered insufficient and parental consent is required to process a child's personal data, States parties should require that organizations processing such data verify that consent is informed, meaningful and given by the child's parent or caregiver."[52]

APP3 addresses the unnecessary collection of data. From a rights perspective, the over-collection of data represents a real risk for young people. The UN Committee notes that, in general, unsolicited surveillance

[44]Specifically, APP 3.5 and 3.6
[45]OAIC nd *Chapter 3: APP 3 Collection of solicited personal information* https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information
[46]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
[47]Children & Media Australia 2022 *Apps can track* https://childrenandmedia.org.au/app-reviews/apps-can-trap-tracking
[48]Reset.Tech Australia 2023 *Australians for sale* https://au.reset.tech/news/coming-soon-australians-for-sale-report/
[49]Katherine Kemp 2022 *'Australia's Forgotten Privacy Principle: Why Common 'Enrichment' of Customer Data for Profiling and Targeting is Unlawful*' https://ssrn.com/abstract=4224653
[50]Paragraph 67, 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
[51]Ibid. Paragraph 9 & 10
[52]Paragraph 71, 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

is a risk to children's privacy:

> "Any digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy and should not be conducted routinely, indiscriminately or without the child's knowledge or, in the case of very young children, that of their parent or caregiver; nor should it take place without the right to object to such surveillance, in commercial settings and educational and care settings, and consideration should always be given to the least privacy-intrusive means available to fulfil the desired purpose."[53]

What Australian young people say about this

The importance of meaningful consent to data collection was consistently described as central to young people's ideas about good data protection practices.

- In a survey of 500 young 16 & 17 year olds in 2023, the idea of having more control over your data was listed as the third most important aspect of improving trust in the data environment online.[54]
- We (again) surveyed 400 young people aged 16 &17, and found that consent was the first and second most important principle, with 85% of young people noting that they didn't want their data used for a purpose they had not consented for, and 83% of people outlining they wanted better rules to restrict data sharing without consent. We asked an open questions about what else young people would like done to protect their data, and 1 in 8 comments was around consent; "Just to be more private and have my full consent before sharing something with others", "Maybe please don't use my personal data without my permission", "Definitely more clarity and ask of permission to access and use personal data.[55]
- In anticipation of the *Enhancing Online Privacy Bill 2020*, we workshopped a number of ideas with young people and consent was consistently described as important. When presented with the idea that a (then) potential Code should include a rule that children's data should require consent to collect, young people in grade 6 rated that idea as 9-9.5/10, and young people in grade 8 rated in 9-10/10 (the highest scoring suggestion). They wanted this rule in place "to give us more privacy online. So that we have control over what they can see over what we do and search for", and described it as important as a mechanism for safety; "making sure that nobody knows too much about you" and "making sure you're safe." This was especially important since they did not feel that they generally understood exactly what was happening with their data, "terms and conditions are not easy to access." They were also aware that a lot was at stake; "to access social media you have to sacrifice some pretty big stuff." Other suggestions in turn made by these young people themselves expanded on the idea of consent, ranging from ""No tracking or collecting data without getting permissions", "Websites should not be able to look at or share your personal photos unless you have given permission" and "Permission to access information doesn't last forever - ask each time it is needed."
- A community college class noted that their first substantive 'right' they wanted in a Code was consent, after noting that it should protect every one up until the age of 18. "Young people should have more choice around data collection; Data should only be gathered with consent; We should have 'the right to choose' about data collection; Young people should be able to choose what data they collect"

However, consent alone was not always described as enough, and in many discussions with young people, it became clear that 'consent did not change childhood'. That is, young people did not feel that it was fair for consent to be used as a way to justify predatory data practices. For example, one group of

[53]Ibid. Paragraph 75
[54]Reset.Tech Australia 2023 *Young people and online privacy* https://au.reset.tech/uploads/For-Print-Final-report.pdf
[55]Reset.Tech Australia 2021 *Response to the draft Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021, reflecting the views of children and young people* https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/consultation/view_respondent?_b_index=60&uuId=1044012677

young people who were preparing a list of 'asks' to share with the Office of the Information Commissioner developed an ask that "Companies should not be able to ask young people to consent to use their data in really bad ways, some things are off limits, young people shouldn't be asked to think about the full extent of risks."[56]

In a more nuanced way, a group of young people involved in a longer project came to the same conclusion. Here, however, consent *did not* emerge as one of the group's key 'asks' to share with decision makers but for the same reason. This group did not want the responsibility of data protection to be handed to young people with blunt 'accept' or 'reject' options. We workshopped an initial list of ideas for core 'asks' about privacy and ideas like "Do collect data only where they have clearly asked for it", "Do - unbundle consent" and "Do-Only be collected and used only when young people have clearly been asked" appeared.[57] However, these did not make it into their final list of policy asks. Instead, this group decided that consent was not enough (see APP 1), and they wanted broader protections placed around their data

> "We believe that children and young people's data should only be collected and processed in ways that are in their best interests."[58]

With regards to parental consent, in 2025 we polled 1,624 young people aged 13-17 years old. We asked them what age they felt online platforms should seek parental consent to process data and found that young people wanted parental consent for:

- 12-years-old or under 38%
- 16-years-old or under 39%
- 18-years-old-or-under 19%
- Never 2%[59]

[56]Unpublished quote from a focus group
[57]Unpublished focus group notes
[58]Reset.Tech Australia 2023 *Submission to the Senate Economic Reference Committee's investigation into the Influence of International Digital Platforms: Representing young people's thoughts and opinions* https://au.reset.tech/uploads/YPs-submission.pdf
[59]Reset.Tech Australia 2025 *Results from a survey with young people about the Children's Online Privacy Code* forthcoming

APP 4: Dealing with unsolicited personal information

APP 4 outlines how APP regulated entities must deal with unsolicited personal information. APP 4 captures use cases where an organisation (generally a government agency), has not taken action to seek out that information.[60] The effect of APP 4 is organisations need to treat this information with the same protection as if they had gone out and collected it.

APP 4 covers situations like misdirected mail, correspondence to members of parliament from community members, and petitions with names and addresses.[61] For children, APP 4 may be triggered in situations like:

- A school asks students to write a message in a thank you card to a departing staff member and some include photos of themselves and their friends, or
- A child returns a basic consent form to their soccer teacher for a competition trip and attaches a letter from their GP giving details of an unrelated medical condition, or
- A company, intending to purchase a dataset on the purchasing habits of adult males over 40, receives a dataset including children's survey responses.

APP 4 puts companies on notice to handle all information they receive – whether they sought it out or not – with equivalent levels of responsibility and protection. If they could have validly collected the information under APP 3, standard information handling procedure per APPs 5-13 apply. If they could not have validly collected it, APP 4 sets out they must (generally) destroy or de-identify it.

Interacting child rights principles

The concept of unsolicited data is relatively unique, and not a frequently used formulation outside of privacy and public sector data handling. A rights respecting approach for handling unsolicited information would suggest that there remains an onus on handlers to address the risk of harm, respect and support a child's agency and take steps to preserve or return sovereignty over personal data to children (and their caregivers).

The *General Comment* notes that all data collected about children — presumably regardless of whether it was solicited or not — needs to be processed in ways that respect privacy and data protection rules. It states "Children's personal data should be accessible only to the authorities, organizations and individuals designated under the law to process them in compliance with such due process guarantees as regular audits and accountability measures. Children's data gathered for defined purposes, in any setting, including digitized criminal records, should be protected and exclusive to those purposes and should not be retained unlawfully or unnecessarily or used for other purposes."[62]

Secondly, when it comes to data that is unnecessarily collected or retained — which suggests the inclusion of unsolicited data — the *General Comment* notes that this data needs to come under the 'control' of children and parents.

[60]Parliament of Australia 2012 *Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, page 45, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4813
[61]OAIC nd *Chapter 4: APP 4 Dealing with unsolicited personal information*
https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-4-app-4-dealing-with-unsolicited-personal-information
[62]Paragraph 73, 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

> "States parties should ensure that children and their parents or caregivers can easily access stored data, rectify data that are inaccurate or outdated and delete data unlawfully or unnecessarily stored by public authorities, private individuals or other bodies, subject to reasonable and lawful limitations."[63]

Unsolicited data ought to be handled with at least the same care and standards as solicited data.

What Australian young people say about this

Our previous research with young people has not explored differentiations between unsolicited and solicited information.

[63]Paragraph 72, 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

APP 5: Notification of the collection of personal information

APP 5 outlines 'when and in what circumstances an APP entity that collects personal information must tell an individual about certain matters'. Practically speaking, APP 5 governs the process and content of materials like collection notices. APP 5 provides that regulated entities need to be *timely* about how they notify (ideally, before or at the time of information collection), and notify *clearly* and comprehensively. In basic terms, APP 5 is a 'no surprises' policy, to ensure people understand when and how regulated entities are collecting information about them.

Relevantly for children, APP 5.1(b) places obligations on regulated entities to ensure the individual is aware of various matters around the information collection. These 'matters' are set out in APP 5.2, and extend from the *fact of* collection, the *purposes of* and likely *disclosures* (onwards information sharing) flowing from that collection, to the rights the individual has available to them under the other APPs, like the rights to access, correction, and complaint. APP 5.1(b) and 5.2 clearly indicate the notification procedure can't be just a tick-box exercise, to meet a threshold of a child's awareness, a company will need to ensure collection notices are in accessible language and expressly *put to* the child (i.e., not buried in fine print and back-links on web pages).

Note APP 5 does intersect with APP 1, in that both APPs relate to transparency measures and documents. In general, APP 1 is about overarching privacy policies, whereas APP 5 narrows down to time-sensitive materials tied to the collection phase.

Interacting child right's principles

The *General Comment* acknowledges the importance of suitable notification schemes for children. It places explicit obligations on State parties to "require all businesses (that are likely to be accessed by children to) require the provision of age-appropriate explanations to children, or to parents and caregivers for very young children, of their terms of service."[64]

Providing adequate notification to children and young people in transparency and understandable ways requires due regard for their evolving capacity. Children's capacity will vary, but respecting their capacity and emerging agencies is central to ensuring effective transparency. *General Comment* 25 notes that:

> "States parties should respect the evolving capacities of the child as an enabling principle that addresses the process of their gradual acquisition of competencies, understanding and agency. That process has particular significance in the digital environment, where children can engage more independently from supervision by parents and caregivers. The risks and opportunities associated with children's engagement in the digital environment change depending on their age and stage of development. They should be guided by those considerations whenever they are designing measures to protect children in, or facilitate their access to, that environment. The design of age-appropriate measures should be informed by the best and most up-to-date research available, from a range of disciplines.
>
> States parties should take into account the changing position of children and their agency in the

[64]Paragraph 39, 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

modern world, children's competence and understanding, which develop unevenly across areas of skill and activity, and the diverse nature of the risks involved. Those considerations must be balanced with the importance of exercising their rights in supported environments and the range of individual experiences and circumstances. States parties should ensure that digital service providers offer services that are appropriate for children's evolving capacities."[65]

What Australian young people say about this

In a focus group with young people aged 13-16 held in 2024, we asked young people to imagine their 'digital utopia' and what happened with their data in it. Many of their visions included more clear and accessible notifications. For example, suggestions include:

- "In my utopia, there would be terms and conditions with all the details, but also a simplified version, so I know what I am accepting. A simple version if I don't have the time. If we can haggle our positions, maybe have a 'choose' at least 3 things it can access… you can choose 2 of 3."
- "Plain language version of terms and conditions for customers, that refer to full terms and conditions."[66]

In July 2021, we ran a poll with 400 16- and 17-year olds addressing privacy and their perceptions about privacy notice. Young people described how they rarely read privacy policies partly because the documents themselves were problematic. They were described as:

- Too long (76%)
- Too numerous, with too many terms and condition documents (58%)
- Presented in ways that are difficult to read (46%)
- Using complex and difficult language (38%) and
- Too hard to find (7%).[67]

This poll was run alongside research exploring the use of dark patterns in the sign on processes of Australia's most popular apps, which found that alongside confusing policies and terms of services, digital products deploy design features and choices that actively encourage Australian children to share unnecessary information.[68] The exploitative nature of terms of service was not lost on young people. As one young person said in a focus group "sometimes it just feels like it's impossible to make an informed choice. Who has the time to read all the small print? It can kind of feel a bit predatory."[69]

We asked similar questions in 2025 of young people in a poll of 1,624 young people aged 13-17 years old. We asked about requirements they would like to see in a Code to help them better understand what information was collected about you, and found that:

- 63% wanted terms of service in simple, easy-to-understand language
- 62% wanted to make it easy for users to access and manage their privacy settings
- 54% wanted regular updates users on any changes to their data collection practices in an easy-to-understand format (simple language/short)
- 46% wanted shorter terms of service.[70]

In accessible terms of service hamper young people's ability to understand what they are consenting to. As one young person simply put it: "Well I don't read the terms and conditions because they are too long

[65]Paragraph 19 & 20, 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
[66]Unpublished quote from a focus group with young people 2024
[67]Reset.Tech Australia 2021 *Did we really consent to this?* https://au.reset.tech/uploads/l01_resettechaustralia_policymemo_t_c_report_final-july.pdf
[68]Ibid.
[69]Unpublished quote from a focus group
[70]Reset.Tech Australia 2025 *Results from a survey with young people about the Children's Online Privacy Code* forthcoming

so I don't know what they are doing with my info."[71] This was best summarised by young people when authoring a submission; "privacy policies are confusing and complex, and tricks are often used to sneak our data."[72] They especially find the name "cookie" to be sneaky. One young person we spoke to described how, right up until the focus group they were participating in, they always clicked yes on cookies, because they thought they were a good thing "who doesn't want a cookie?"[73] They went on to describe how. "cookies" should be called "data grabbers."[74]

Despite young people's general malaise around the concept of consenting via accepting a flawed collection notice, there was still a broad appetite among all the young people we spoke to around ensuring that privacy policies and collection notices were comprehensible. "There should be plain wording… of the company and the website… explaining what they can do with our data. A few plain words in normal language and we might be able to see what we agreed to."[75]

Collection notices and privacy policies were still important documents for the young people we spoke to and they wanted to be able to understand them and inform themselves. They believed that informed knowledge about data processing allowed them to develop their own personalised privacy risk mitigation strategies. As one young person put it, "at the very least we need to know the risks" so they can start to think about "what are the ways to lessen the risk."[76]

They also talked about adequate notification as a way of allowing them to exercise better choice as a consumer:

> "I think that you know, increased transparency does lead to greater accountability because you know, a company can go out and take your information because like, you don't know that they're doing it, but if it's like transparent, you know, they can't really go out and say like, I'm taking your information now like, because like people would never allow that. So I think no, with transparency comes greater trust, but I also agree that you know, when people wouldn't know what the company might be doing with your information like, they don't want that anymore. Like they don't want, they don't want to use your app and they know it, or they don't want to interact with it."[77]

[71]Reset.Tech Australia 2013 *Submission to the Senate Economic Reference Committee's investigation into the Influence of International Digital Platforms: Representing young people's thoughts and opinions* https://au.reset.tech/uploads/YPs-submission.pdf
[72]Ibid.
[73]Unpublished focus group notes
[74]Reset.Tech Australia 2023 *Submission to the Senate Economic Reference Committee's investigation into the Influence of International Digital Platforms: Representing young people's thoughts and opinions* https://au.reset.tech/uploads/YPs-submission.pdf
[75]Reset.Tech Australia 2023 *Young people and online privacy* https://au.reset.tech/uploads/For-Print-Final-report.pdf
[76]Ibid.
[77]Unpublished interview transcript

APP 6: Use or disclosure of personal information

APP 6 is one of the 'chunkiest' APPs. It governs how companies can 'use' and 'disclose' personal information. After collection, use and disclosure are the fundamental phases of information flows. Both activities involve handling information in all of the foreseeable post-collection ways. The difference between use and disclosure is ultimately about control: when information leaves the effective control of one entity and enters the domain of another, we would consider that transfer a 'disclosure'.

The starting point is a use or disclosure is permitted under the APPs when it keeps a consistent chain back to the original collection purpose. That means, if a company collected a child's personal information for the purpose of administering a program, it can only use and share it with third parties for that same purpose.

Companies may use and disclose a person's information for a secondary purpose, subject to a set of conditions. These include:[78]

- The person consented to that use or disclosure, or
- The person would reasonably expect that use or disclosure, and
    - The secondary purpose is related to the primary purpose, or
    - If the information meets the 'sensitive information' threshold, the secondary purpose is **directly** related to the primary purpose.

This is a really important principle when it comes to protecting children's personal information. If a child provides their personal information such as name, DOB, emergency contact etc online in order to register for a summer school for example, that organisation cannot then disclose that information to a third party to undertake a study on children nor can the summer school itself start to use that data for other random reasons such as predicting learning outcomes. Predictably, APP 6 is one of the most regularly breached (and enforced) of the APPs.Breaches of APP 6 often run in tandem with other information handling issues, such as APP 8, 10, or 11.

Interacting child rights principles

The *General Comment* notes that children's data ought to be processed only by those with legal authority to process it, and that states have an obligation to ensure this:

> "Children's personal data should be accessible only to the authorities, organizations and individuals designated under the law to process them in compliance with such due process guarantees as regular audits and accountability measures."[79]

It is explicit that onward processing of children's data is potentially violative, and should only be permissible where explicit consent is given:

> "Children's data gathered for defined purposes, in any setting, … should be protected and exclusive to those purposes and should not be retained unlawfully or unnecessarily or used for other purposes. Where information is provided in one setting and could legitimately benefit the child through its use in another setting, for example, in the context of schooling and tertiary education, the use of such data should be transparent, accountable and subject to the consent of the child,

[78]APP 6 covers a range of other restricted exceptions around authorisations through law or court orders, enforcement activities, and specific 'permitted general situations' and 'permitted health situations'.
[79]Paragraph 73, 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

parent or caregiver, as appropriate."[80]

We should remind ourselves that in a digital world, these are profound issues that impact a child's experience of their right to identity and autonomy and agency and shape the way that they see the world around them.

What Australian young people say about this

Young people had a lot to say about APP6 in our previous research, and we have divided this into commentary around; the over-collection of data; the over-sharing of data, and; a general lack of trust in the way their data is used and disclosed.

1. Over-collection of data (Collecting excessive data for the original purpose)

When it comes to the over-collection of data, young people also expressed strong desires to curb this. In a youth-authored submission to a Senate Inquiry around digital platforms, for example, young people noted their concerns about the 'enrichment' of their data, and potential misuse of largely unsolicited data profiles about them:

> "We are concerned that too much data is too often collected about children and young people, and that it is stored for too long, and shared with too many people. We think better protections are needed to prevent massive databases being created about young people.
>
> We also believe that children and young people should also have more control and say in how data is collected and used, where it is in their best interests and not too much has been collected. We are concerned that we are often not clearly asked or consulted, especially when it comes to the way data is used in advertising or profiling."[81]

2. Over-sharing of personal data (Unexpect disclosures)

Young people's expectation that privacy frameworks would protect them from onward sharing and use of data for non-legitimate purposes was depressingly low. As one young person we interviewed as part of a 2023 research project noted:

> "We can't expect the government to, you know, make (digital products and services) default to "no, you can't share my data." . . . Because like that wouldn't get passed, like no matter what. Because it's just like, it's really unrealistic for them to be able to do that and then make profit at the same time."[82]

Or another young woman put it:

> "We have so many privacy concerns now, and it's kind of like, what has the government done to, like, implement systems to like, make sure that our, like, concerns are kind of alleviated? So it's like, will they do that in the future? Or will they, you know, kind of just turn a blind eye to like the third parties that they give, that our information is like sold to. I think that."[83]

There was a level of normalisation around the idea of excessive sharing speaks more to a failure of privacy protections for these young people, than a failure of desires for privacy. When we asked young

[80]Paragraph 73, 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
[81]Reset.Tech Australia 2023 *Submission to the Senate Economic Reference Committee's investigation into the Influence of International Digital Platforms: Representing young people's thoughts and opinions* https://au.reset.tech/uploads/YPs-submission.pdf
[82]Rys Farthing, Katja Koren Ošljak, Teki Akuetteh, Kadian Camacho, Genevieve Smith-Nunes & Jun Zhao 2024 'Online Privacy, Young People, and Datafication: Different Perceptions About Online Privacy Across Antigua & Barbuda, Australia, Ghana, and Slovenia' *Social Media + Society*, *10*(4). https://doi.org/10.1177/20563051241298042
[83]Unpublished interview transcript

people about the possibility of a better, more privacy realising digital environment they expressed a strong desire, “that would be awesome, to go online and know my privacy will be mine."[84]

In fact, young people spoke at length about the extent to which they tried to protect their own privacy, but felt let down by those who have ultimate power over their data. “I check my privacy settings every few months. (But companies have) ways to get around it and send suggested posts and ads anyhow. It’s annoying”, and that placing the burden on users to keep themselves private was unfair, “people shouldn’t have to consider buying a VPN if they are scared of people tracking them."

As one young person clearly put it, “sometimes there are choices you can make to protect your privacy – but it often feels like even if you take all these steps it doesn’t really help. All of these websites can get data about you even if you're making conscious decisions to try not to”[85] or another “you have to work really hard to be protected online. If there was more effort put into protecting people at this age, it would be really good.”[86] The Code could be an effective way to rise to this challenge.

3. General lack of trust in data use and disclosure

Time and time again in our discussions with young people, they have described their privacy online as some sort of trade off when it came to ‘offering it up’ to access the digital world, but having it used for other (largely commercial) purposes.

> “Basically a trade off. And the whole world is full of different perspectives and views, just like the internet. So if we have a look at the two, it’s big. Your privacy for something else, or that fun for just a few, like a little bit of information. But I think what makes most people willing to share that information is they think, “Oh, who would be interested in me, like, I’m just one drop out of the ocean. You know, there’s millions of other people who do the same thing.”[87]

They talked about wanting fair use of their data, that was governed by their autonomy (consent and control) and transparency (understanding and clarity). In a youth-authored submission to a Senate Inquiry around digital platforms, young people talked about wanting a re-balance about who was considered in control of their data:

> “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. We believe that children and young people’s data should only be collected and processed in ways that are in their best interests. This means that where profiling, behavioural advertising or other uses are not clearly in young people’s best interests, it should not be allowed.”[88]

This was reiterated by a focus group of young people held in 2024, when participants asked “Ads include my personal information, where is this data going? What are advertisers doing with it? Our phone is our property, we should be able to stay private, it should belong to us, not taken by some dodgy terms and conditions.”[89]

Ideas around limiting the disclosure of personal information appeared popular with young people. In one poll of 500 16 & 17 year olds in 2022, 61% of young people said they would trust digital platforms more if they “only used my information in ways that I had signed up for, and not for other purposes whenever they want.” A number of responses to an open question about what they’d like from platforms to increase trust

[84]Reset.Tech Australia 2023 *Young people and online privacy* https://au.reset.tech/uploads/For-Print-Final-report.pdf
[85]Unpublished quote from a focus group
[86]Reset.Tech Australia 2023 *Young people and online privacy* https://au.reset.tech/uploads/For-Print-Final-report.pdf
[87]Reset.Tech Australia 2023 *Young people and online privacy* https://au.reset.tech/uploads/For-Print-Final-report.pdf
[88]Reset.Tech Australia 2023 *Submission to the Senate Economic Reference Committee’s investigation into the Influence of International Digital Platforms: Representing young people’s thoughts and opinions* https://au.reset.tech/uploads/YPs-submission.pdf
[89]Unpublished quote from a focus group with young people 2024

pointed to a desire to limit data flows "Them not selling my info", "Not selling my data to third parties, not subscribing me to emails and letting me control what data they collect and having full transparency."[90]

In general, the young people we spoke with were supportive of the idea of greater protections about the way their data was collected, used and disclosed. As one young man simply put it: "(I want) more regulation from government to prevent data being shared and sold."[91]

[90]Reset.Tech Australia 2023 *Young people and online privacy* https://au.reset.tech/uploads/For-Print-Final-report.pdf
[91]Reset.Tech Australia 2021 *Response to the draft Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021, reflecting the views of children and young people* https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/consultation/view_respondent?_b_index=60&uuId=1044012677

APP 7: Direct marketing

APP 7 sets the parameters for 'direct marketing' under the *Privacy Act*. Direct marketing refers to the use or disclosure of personal information to communicate directly with an individual to promote goods and services. This would include displaying an ad on social media that an individual is logged into using personal information collected by cookies or other SDK trackers.[92]

The general rule is the use of personal information for direct marketing is prohibited, unless it is permitted by way of exception.

One exception arises if:

- The company collected the information directly from the person, and
- The person would reasonably expect the direct marketing, and
- The company provides a 'simple' way for the person to 'easily' opt-out of direct marketing approaches, and
- The person has not already opted-out.

Another exception covers situations of third-party data collection and direct marketing, with the same expectations as above for the company to provide simple and easy opt-out mechanisms. The exception also requires companies to seek consent from the person, unless it is 'impracticable' to do so.

Aggressive third-party data collectors and marketers routinely rely upon the 'impracticable' limb. Evidently, the construction of this APP comes from a time before marketing practices took on the complex, rapid, and technologically sophisticated ways that have made digital marketing and online services so notoriously intrusive.

Where a child logs on to their social media account and is displayed ads on the basis of their age, gender, religion, race etc that was collected by a third-party organisation without consent, this is unlawful because it involves sensitive information used for direct marketing without consent.

Interacting child right's principles

Consideration of the special protections afforded to children and what is in their best interests justifies a higher bar on what is acceptable in the use of the personal information of a child for commercial or marketing purposes. The *General Comment* stipulates that children's best interests need to be:

> "a primary consideration when regulating advertising and marketing addressed to and accessible to children. Sponsorship, product placement and all other forms of commercially driven content should be clearly distinguished from all other content and should not perpetuate gender or racial stereotypes."[93]

The content of advertising can impact a child's right to be free from discrimination. There is also a risk of harm from advertising for services or materials that are unsafe or unhealthy for children.

The *General Comment* also examines the impact of advertising practices — which will sit outside the

[92]OAIC nd *Chapter 7: APP 7 Direct marketing* https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-7-app-7-direct-marketing
[93]Paragraph 41, 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

immediate scope of the Children's Online Privacy Code — to call for stronger protections around the use of children's data to drive behavioural or targeted advertising. It notes that:

> "States parties should prohibit by law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling. Practices that rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products, applications and services should also be prohibited from engagement directly or indirectly with children."[94]

What Australian young people say about this

Across 2022 and 2023, Reset.Tech Australia held repeated workshops with a group of 12 young people where they described a nuanced and ambivalent understanding about the way their data is used to deliver them advertising. In essence, they experienced targeted advertising as violation of privacy:

- "I just feel as if they are storing my data for ulterior reasons, primarily ads"
- "I understand where some young people's frustrations may lie, because I guess when you do see an ad that it's targeted to you, kind of like consciously realise that our data is being taken. Where usually when you're using social media, you don't actually realise it. But it kind of is, kind of strange. It's kind of like scary almost to do that. Like your phone is listening to you or the internet is like listening to you. So it can be like frustrating in that sense"
- "Not just (big) advertisers, but any companies. Even not for profits will get up in your face sometimes. It's unnecessary. Advertising can be really in your face. It's not looking after young people. It's not the best thing for young people"
- "It's pretty bad that people can just pay and have stuff shown to minors. I understand some stuff, like councils (and ads for public interest stuff). But overall, it's hard to pick and choose, for companies. So you shouldn't be able to."[95]

In a youth-authored submission to a Senate Inquiry around digital platforms, young people outlined the principle they believe should underpin targeted advertising. They started out their list of asks by stating "Fundamentally, young people do not want their data used to sell them things, especially without their consent", and went on to state that:

> "For advertising and profiling, young people's data should:
> - Only be used in ways that are in their best interests (and not to target them with risky ads or because they're vulnerable);
> - Only be collected and used carefully and where needed (rather than collecting loads of data so they can really personalise ads, based on your live location for example), and;
> - Young people should have more control over the way it is used for advertising and profiling (rather than this being hidden in the terms of service with a 'click to accept', or having data sold and shared that we don't know about or haven't clearly agreed to).
> - Young people should be able to simply and easily request that any data collected and profiled about them for advertising should be deleted (rather than it being held forever without any control).
>
> Specifically, this means that we think that advertising should not be turned on by default for young people. Young people should be able to opt-in and choose to have advertising overall, and also be able to choose if they want their data used to personalise these ads or not. These options and what they mean need to be clearly and honestly explained and meaningful choices provided. Where young

[94]Paragraph 42, 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
[95]Reset.Tech Australia 2023 *Young people and online privacy* https://au.reset.tech/uploads/For-Print-Final-report.pdf

> people opt-in, data collection to personalise advertising needs to be done carefully and with not too much data. If young people do 'opt-in', they need to be able to change their mind and request that the data be deleted. We support a ban on behavioural advertising, but we are aware it might be unpopular or difficult to implement."[96]

It is telling that the young authors of this submission felt that it was unpopular or difficult for young people not to be subject to direct marketing using their data. It was almost as if there was a chilling effect around what could be imaginable or expressed as desirable. In their submission, the opening gambit (as described in APP 4 above) was "fundamentally, young people do not want their data used to sell them things", but they end their submission by moderating this statement by calling for advertising to "not be turned on by default for young people.[97] However, in the discussions around developing this submission, participants described that this was not because they felt young people wanted or needed a choice about receiving advertisements, but because, in their words, they wanted to be "realistic" in their discussions with policymakers. We unpacked this desire to be realistic with the group, as it came up multiple times. Young people expressed genuine concerns that what they really wanted might not be "too much" to ask for. There appeared to be a belief that young people needed to be sources of profit for technology companies to access the digital world. Notes and transcripts from the discussions included multiple comments like "but they won't do that, so don't add it (to the list)," "but that won't make them a profit," "if they don't profit, they won't do it."

[96]Reset.Tech Australia 2023 *Submission to the Senate Economic Reference Committee's investigation into the Influence of International Digital Platforms: Representing young people's thoughts and opinions* https://au.reset.tech/uploads/YPs-submission.pdf
[97]Ibid.

APP 8: Cross-border disclosure of personal information

APP 8 relates to when personal information moves across Australia's borders. It sets out the steps a company must take to protect personal information. APP 8 invokes the 'reasonable steps' standard to put companies on notice prior to the information leaving Australia, to adequately mitigate the risks of an overseas recipient breaching the APPs. The purpose of APP 8 is not to *prevent* overseas disclosures, but to ensure the APPs continue to protect Australians, even when their information goes offshore.

APP 8 often comes up when companies engage overseas-based contractors to perform services on their behalf, such as a Sydney-based consumer products shop relying on back-office functions in Manila. Reasonable steps for the purpose of APP 8 usually include negotiating enforceable data sharing provisions in their relevant contracts.

For children's data in particular, it is important to note that each jurisdiction will have different frameworks and protections for personal information which can make it difficult to ensure consistent safeguards for children's personal information. We note that the 2024 privacy reforms introduced a clarifying amendment to APP 8 around 'substantially similar frameworks', to reduce burden for regulated entities.[98]

Interacting child rights principles

In general, child rights principles are internationally developed and responsibility for their implementation rests significantly on national governments. In this context, it is unique that APP 8 contemplates that APP obligations should extend across national borders. This logic means when children's best interests enter the APPs via the Code, the protection of children's best interests will also flow across borders. The *General Comment* is explicit when it comes to outlining that protections for children's rights in the digital environment, including and especially privacy, requires Australia to co-operate internationally:

> "The cross-border and transnational nature of the digital environment necessitates strong international and regional cooperation, to ensure that all stakeholders, including States, businesses and other actors, effectively respect, protect and fulfil children's rights in relation to the digital environment. It is therefore vital that States parties cooperate bilaterally and multilaterally with national and international non-governmental organizations, United Nations agencies, businesses and organizations specialized in child protection and human rights in relation to the digital environment."[99]

It also stipulates that State parties should contribute to the international and regional development of standards, regulations and protections across national borders that enable the realization of children's rights in the digital environment,[100] which would presumably include privacy codes and standards. Specifically however, the *General Comment* outlines that where international businesses operate in the digital world, States have an obligation to ensure children's rights are realised by these transnational businesses, including in their extraterritorial practices. This would include ensuring that their data handling practices were rights respecting, even where data was processed internationally:

> "Children may face particular difficulties in obtaining remedy when their rights have been abused in

[98]Parliament of Australia 2024 *Privacy and Other Legislation Amendment Bill 2024, Explanatory Memorandum,* https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r7249 page 44
[99]Paragraph 123, 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
[100]Ibid. Paragraph 124

> the digital environment by business enterprises, in particular in the context of their global operations. States parties should consider measures to respect, protect and fulfil children's rights in the context of businesses' extraterritorial activities and operations, provided that there is a reasonable link between the State and the conduct concerned. They should ensure that businesses provide effective complaint mechanisms; such mechanisms should not, however, prevent children from gaining access to State-based remedies. They should also ensure that agencies with oversight powers relevant to children's rights, such as those relating to health and safety, data protection and consumer rights, education and advertising and marketing, investigate complaints and provide adequate remedies for violations or abuses of children's rights in the digital environment."[101]

It is interesting to note that this also requires government agencies — such as the OAIC— be able investigate and provide remedy for children from violations that originate in international platforms.

What Australian young people say about this

This APP was not extensively addressed in previous research, however during a focus group with young people held in 2024, one young person noted that offshore processing raised questions for them about autonomy and control over their data:

> "I have concerns about after the data is collected, is there any way we can take back control or have any say about how that data is used? There was that debate about banning TIkTok, because they are based in foreign countries and they are collecting large amounts of data, but there is no way to take back control about how that data is used, stored or misappropriated once it is stored in an offshore farm."[102]

[101]Paragraph 48, 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
[102]Unpublished quote from a focus group

APP 9: Adoption, use or disclosure of government related identifiers

APP 9 regulates when and how regulated entities can use government related identifiers. The general rule is they cannot, unless an exception applies. The exceptions include situations like necessary identity verification, law and compliance issues, enforcement needs, and exceptional situations (generally emergencies).

In simpler terms, APP 9 aims to prevent the misuse of personal identifiers issued by governments (such as Medicare numbers, centrelink reference numbers, passport numbers, driver licence numbers) and other sensitive information that could be used for identity theft or other malicious purposes. The purpose of APP 9 is to restrict government identifiers from entering into routine private sector circulation and becoming universal identifiers.

Additionally, the drafting intent behind APP 9 included preventing data-matching by organisations from universal or near-universal identifiers.[103] Notably and worryingly, in the decade following the enactment of APP 9, companies in the data matching business have innovated numerous ways to identify people across data sets and build sophisticated, aggregated profiles, with or without universal identifiers.

Interacting child rights principles

The implementation of child rights principles rests significantly on national governments. As an exemplar of good practice, it is to be expected that the use of the personal information of a child by a government agency will be respected and protected. The *General Comment* notes that any onward processing — which would include using administrative data collected for one purpose such as Medicare numbers to access health care — for other purposes needs to be dictated by children's best interests:

> "Children's personal data should be accessible only to the authorities, organizations and individuals designated under the law to process them in compliance with such due process guarantees as regular audits and accountability measures. Children's data gathered for defined purposes, in any setting, including digitized criminal records, should be protected and exclusive to those purposes and should not be retained unlawfully or unnecessarily or used for other purposes. Where information is provided in one setting and could legitimately benefit the child through its use in another setting, for example, in the context of schooling and tertiary education, the use of such data should be transparent, accountable and subject to the consent of the child, parent or caregiver, as appropriate."[104]

What Australian young people say about this

Our previous research with young people has not delved into young people's perspectives about adoption, use or disclosure of government identifiers.

[103]Parliament of Australia 2012 *Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012,* https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4813 page 84
[104]Paragraph 73, 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

APP 10: Quality of personal information

APP 10 is about ensuring regulated entities apply certain quality assurance requirements to the personal information they collect, use, and disclose. APP 10 states that a regulated entity must take such steps (if any) as are reasonable in the circumstances to ensure:

- that the personal information that the entity **collects** is accurate, up-to-date and complete; and
- that the personal information that the entity **uses** or **discloses** is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

As with the other APPs, the more sensitive the information, the higher the expectations on the regulated entities to mitigate the privacy risks, via a standard of 'reasonable steps'.[105] It is likely children's personal information will hit either the 'sensitive information' threshold, or a threshold with equivalent risk mitigation obligations. Reasonable steps in an APP 10 context include:

- Regular procedures and systems to review and 'flag' poor quality or inaccurate personal information – at the collection stage, this can look like adding settings to online forms to ensure emails are verified and names are spell-checked,
- Prompting individuals to review and update their information,
- Ensuring third-parties handling the information follow similar quality assurance processes and checks.

Interacting child right's principles

The *General Comment* makes provision for children and caregivers to correct incorrect information[106] (see discussion in APP 12 & 13), which implies a general expectation of accuracy.

What Australian young people say about this

Our previous research with young people has not delved into young people's perspectives about data quality, however it did frequently address children's ability to access, delete or correct data that was held about them. The need to correct data potentially speaks to issues around data inaccuracy. Issues of access and correction are further discussed in APP 12 & 13.

[105]OAIC nd *Chapter 10: APP 10 Quality of personal information* https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-10-app-10-quality-of-personal-information
[106]Paragraph 73, 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

APP 11: Security of personal information

APP 11 covers security risks including misuse, interference, loss, unauthorised access, unauthorised disclosure, and modification. APP 11 provides that regulated entities must take steps to protect personal information from these outcomes. APP 11 makes regular appearances in privacy breaches and OAIC determinations, and breaches of APP 11 often run hand-in-hand with breaches of APP 6. Additionally, a notifiable data breach for the purposes of the Privacy Act will often concurrently be a result of an APP 11 breach.

As with the other APPs, companies must meet a 'reasonable steps' test for their APP 11 security obligations. The 2024 amendments to the *Privacy Act* clarified the breadth of expectations on APP regulated entities. The new APP 11.3 sets out that reasonable steps include organisational as well as technical measures, meaning that companies must pair their technical efforts (MFA, encryption, strong passwords) with non-technical measures like staff training and awareness, risk assessments, and various standard operating procedures.

In addition, APP 11 introduces a 'data hygiene' or 'data minimisation' style principle in APP 11.2 to obligate regulated entities to destroy or de-identify information they no longer need or have reason to hold. We would expect this APP is routinely breached by companies in Australia, given well-known practices of 'data hoarding' or simply unnecessarily prolonged data retention.

The 'reasonable test' in this principle is useful as it ties back to the circumstances. Children's personal information can generally be accepted to require greater protection and therefore further security measures and safeguards in place.

Interacting child rights principles

Cyberattacks are defined as a type of online violence that can affect children,[107] and children's right to be protected from violence extends into the digital world. The *General Comment* makes clear the expectation that "States parties should protect children from cyber aggression and threats, censorship, data breaches and digital surveillance."[108]

There is a clear expectation that a range of legislative and administrative measures will be deployed to protect children's data from cyberattacks and information warfare, including but not limited to "regular review(s), updating and enforcement of robust legislative, regulatory and institutional frameworks' to protect children from risks in the digital world."[109]

On the complicated issue of encryption, the *General Comment* notes that the value of encryption as a tool to ensure children's cybersecurity requires consideration of the potential issues that this raises when it comes to scanning the digital environment for materials that violate children's rights to protection from harm (notable, child sexual abuse and exploitation material):

> "(State parties should) regularly review privacy and data protection legislation and ensure that procedures and practices prevent deliberate infringements or accidental breaches of children's privacy. Where encryption is considered an appropriate means, States parties should consider

[107]See for example, its inclusion in Paragraph 82, 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
[108]Paragraph 60, 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
[109]Ibid. Paragraph 82

> appropriate measures enabling the detection and reporting of child sexual exploitation and abuse or child sexual abuse material. Such measures must be strictly limited according to the principles of legality, necessity and proportionality."[110]

This issue has been more widely addressed by UNICEF[111] and CRIN,[112] both arguing that encryption is an important part of realising children's right to privacy, and needs adequate consideration in discussions around protecting children online.

Children's rights are also an important consideration where security has failed and hacks, data leaks or other breaches of privacy occur. As with all violations of privacy, the *General Comment* makes clear that children have a right to remedy and redress. It outlines that when State agencies are investigating digital crimes against children online — which would presumably include hacking and cyberthreats— "the investigation of such crimes (needs to) provide remedy and support for children who are victims."[113] Current notifications and remedies around hacking, leaks and breaches may be inadequate in general,[114] but children deserve extra consideration when discussing any improvements in remedy and redress.

What Australian young people say about this

Data security is important to young people. In a 2022 survey of 400 16 & 17 year olds, we asked an open question to allow young people to share their thoughts about what they wanted to improve their data security. A large cluster of responses pointed to the importance of data security for these young people, with for example suggestions to improve privacy through "Two factor security", "a VPN", "Make sure no one hacks" or more broadly "The assurance by the platform to keep my data safe."[115]

Young people also wanted more accountability from companies when breaches occurred. During an interview with two young women in 2021, they stated that "Apps should be accountable for data breaches and leaked information." They noted that security and privacy went hand in hand. They talked about individual security solutions like "we should have passwords to our accounts and apps to keep them secure." They also wanted to know more about their security, saying "security information should be made accessible to users."[116]

Incidentally, breaches were a particular concern for young people when it came to geolocation data (and also when it came to data sharing and data sale). As one young person outlined during a discussion about geolocation data, my "main worry is data breaches, we don't know who can get this data."[117]

[110]Paragraph 70, 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
[111]See Danial Kardefelt-Winther, Emma Day, Gabrielle Berman, Sabine Witting, and Anjan Bose 2020 *Encryption, Privacy and Children's Right to Protection from Harm. Innocenti Working Paper* https://www.unicef.org/innocenti/reports/encryption-privacy-and-childrens-right-protection-harm
[112]CRIN 2023 *A children's rights approach to encryption* https://home.crin.org/readlistenwatch/stories/privacy-and-protection
[113]Paragraph 25, 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
[114]See for example, the fall out from the Optus data breach. SBS News 2022 *Tanya Plibersek blasts Optus over 'extraordinary' lack of communication since data breach* https://www.sbs.com.au/news/article/tanya-plibersek-blasts-optus-over-extraordinary-lack-of-communication-since-data-breach/0xktxt7c1
[115]Reset.Tech Australia 2023 *Young people and online privacy* https://au.reset.tech/uploads/For-Print-Final-report.pdf
[116]Reset.Tech Australia 2021 *Response to the draft Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021, reflecting the views of children and young people* https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/consultation/view_respondent?_b_index=60&uuId=1044012677
[117]Unpublished quote from a focus group

APP 12 & APP 13: Access to and correction of personal information

Read together, APP 12 and APP 13 provide individuals with the right to access and correct their own personal information. These are critical, and generally underused principles in Australia. For clarity, they operate separately to the better-known information rights under the *Freedom of Information Act 1982*.

APP 12 requires an entity to give a person access to their information on request. APP 13 requires an entity to address requests for correction. APP 13 also interacts with APP 10, in that it sets out the obligations for regulated entities to take reasonable steps to correct personal information that is incorrect, outdated, irrelevant, or misleading.

When a similar right to APP 12 was introduced under the GDPR in the EU and UK, it came with a rising tide of public awareness about information rights, matched by an uptake of people seeking to realise their access rights. The relevant requests are known as DSARs (data subject access requests) and are regularly used by individuals across the UK and Europe to get a clearer picture about how their personal information is being processed by companies and other providers.

Interacting child right's principles

The ability to 'control' your own data is an integral part of recognising children's autonomy, and this includes the ability to see what data is collected about you and to — at the very least — have a say about the accuracy or quality of it. The importance of children's right to access and correct their data is laid out in Paragraph 72 of the *General Comment* states that national governments:

> "should ensure that children and their parents or caregivers can easily access stored data, rectify data that are inaccurate or outdated and delete data unlawfully or unnecessarily stored by public authorities, private individuals or other bodies, subject to reasonable and lawful limitations. They should further ensure the right of children to withdraw their consent and object to personal data processing where the data controller does not demonstrate legitimate, overriding grounds for the processing. They should also provide information to children, parents and caregivers on such matters, in child-friendly language and accessible formats."[118]

We note that this guidance extends beyond the right to access and correct and highlights the ability to request deletion of data that is unlawfully and unnecessarily stored, and to withdraw consent for ongoing processing of data.

What Australian young people say about this

Young people frequently and repeatedly suggested they would like more control over what happens to their data after it is collected. This connects to both the need to access information and the right correct information.

[118]Paragraph 72, 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

A poll of 400 16 & 17 year olds in 2021 asked young people what rules they would like to see in place to improve their privacy. Seventy-nine percent of respondents said they would like to 'be able to access and know what data is held about them through easy mechanisms'. This also appeared as a frequent suggestion in an open question in this same poll, for example, one young person noting they would like "to have the ability to review and delete data collected."[119]

Likewise, a similar poll of 500 16 & 17 year olds in 2021 asked young people about concepts of trust online. When we asked young people what would improve their trust in digital platforms, 62% of young people stated that trust would improve if platforms offered them more control over their data.[120]

In 2025 we polled 1,624 young people aged 13-17 years old. We asked them about which requirements they would like to see in a Code to help them access and correct their data.

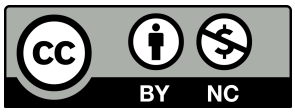
- 63% said platforms should give me the option to view how they have profiled me, show me what data it is based on and give me the option to change it
- 55% said platforms should provide a clear section under settings to view and correct my data
- 50% said platforms should let me view a history of changes made to my data
- 48% said platform should give me the option to download my data in a readable format
- 2% said none of these.[121]

Beyond this, the desire to request the right to *delete* data was a longstanding request from young people we researched with. In a youth-authored submission to a Senate Inquiry around digital platforms, for example, young people noted their their desire for the ability to request data be deleted:

> "Lastly, as a principle, we believe that children and young people should have the right to delete their data. We would like to see clear and simple ways developed that young people can ask for their data to be deleted, including for advertising and profiling if it is collected."[122]

This was repeated in a workshop held in 2024, where young people spoke about wanting to have control over their data. They said "it's important to be able to access proper data that was given permission and being able to revoke different information" and noted that "The thing about data deletion is that even if it is possible they tend to make it VERY difficult to do." Given this, the group developed an idea they wanted to put forward to decision-makers. They wanted a "one stop shop, run by the Government" to oversee requests for data control and deletion. They felt that without this, companies that held their data would not give due consideration to their requests.[123]

.



[119]Reset.Tech Australia 2023 *Submission to the Senate Economic Reference Committee's investigation into the Influence of International Digital Platforms: Representing young people's thoughts and opinions* https://au.reset.tech/uploads/YPs-submission.pdf
[120]Reset.Tech Australia 2023 *Young people and online privacy* https://au.reset.tech/uploads/For-Print-Final-report.pdf
[121]Reset.Tech Australia 2025 *Results from a survey with young people about the Children's Online Privacy Code* forthcoming
[122]Reset.Tech Australia 2023 *Submission to the Senate Economic Reference Committee's investigation into the Influence of International Digital Platforms: Representing young people's thoughts and opinions* https://au.reset.tech/uploads/YPs-submission.pdf
[123]Unpublished quote from a focus group