Consultation with academics and civil society about the Children's Online Privacy Code; How do children's rights and the APPs intersect?

Reset.Tech Australia
April, 2025

Contents

Introduction

This paper documents notes taken from a workshop with 70 academics and civil society experts held on April 7th 2025 in Sydney. It reflects the discussion and thoughts of the group as much as possible and is presented as a briefing given to the Office of the Australian Privacy Commission, to support their work drafting the Children's Online Privacy Code.

During the workshop, participants worked in small groups to consider and discuss ten of Australia's Privacy Principles (APPs) as outlined in the *Privacy Act 1988* and how they interacted with children's rights in the digital world. These included:

1. APP 1 Open & transparent management of children's personal information
2. APP 2 Anonymity & pseudonymity
3. APP 3 Collection of solicited data (split into two groups, A & B, looking at children and parental consent issues separately)
4. APP 5 Notification of the collection of information
5. APP 6 Use or disclosure of children's personal information
6. APP 7 Direct marketing
7. APP 10 Quality of information
8. APP 11 Security of young people's data
9. APPs 12 & 13 Access to, and correction of, personal information

Participants were asked to consider those Privacy Principles and develop a summary of 'key insights' from each small group discussion to share with the Commission. This report documents these key thoughts, as well as notes from the group discussions and deliberations from participants.

Note, this paper uses both children and young people to refer to those under 18 years old.

This workshop was organised and moderated by Reset.Tech Australia, alongside the Australian Child Rights Taskforce and the Young & Resilient Research Centre. We are hugely grateful for assistance from elevenM for providing expertise input on the day, and AWO. Also, to UNICEF Australia, ChildFund Australia and Youth Law Australia for assistance with moderating and note taking for groups. All errors and omissions reset with Reset.Tech.

With many thanks to the Internet Society Foundation for the support for this event.

APP 1: Open & transparent management of children's personal information

Key insights

- The best interests of the child should be the focus. It's not the child's responsibility to serve the best interest of the platforms
- When it comes to considerations around reasonable steps, it is unreasonable to expect the onus to be placed on young people. It is not reasonable to place responsibility on young people to oversee the complaints process
- Thinking about the complaints element of APP1, while being able to make and receive complaints is important, it is important to recognise that if a company gets complaints then they have failed. To avoid over reliance on requirements for entities to have complaints processes, those entities need to design in child privacy from the start. Where complaints are made, we need straightforward, quick, safe, effective, child-centered mechanisms
- Special protections may be needed to ensure young people from a range of diverse backgrounds can access APP1 protections. These include, for example, young people from CALD communities, young people with disabilities, indigenous young people. Risk assessments should ensure that particular needs of groups vis-a-vis particular services are addressed

Discussion

The discussions around centred around three key prompts:

1. **Do young people have access to clearly expressed and up-to-date privacy online, and can they inquire or make complaints about their privacy to platforms? What might be the barriers or blockages for young people to make inquiries or complaints?**

- Group members asked if the requirements for 'clearly expressed' defined privacy policies included considerations about age-appropriateness and linguistic diversity. For example, 20 page fine print vs half page accessible version for young people

- The different needs of different young people were also discussed:
  - There is a need for recognition that children are not a single cohort, in terms of understanding and capacities. Privacy policies tend to be incomprehensible, they are not designed to be read by users in general, let alone young people, or especially young people who may be experiencing additional vulnerabilities
  - There may be additional barriers to digital inclusion, predicated on class, income, age etc

- Mechanism for complaint handling were also raised:
  - There was a discussion about where complaints go once they have been raised with a platform. These may need to involve to OAIC as well as other digital regulators
  - Most businesses have an automated time consuming complaints system that are hard to navigate and escalate a complaint through. There was discussion around the potential need for a 'privacy specific' ombudsman to circumvent the attrition of

complaints through private companies, noting this is outside the scope of the Code. There was also discussion of the possibility of charging a digital company per complaint to make the systems more efficient, noting that this too would be outside the Code
    - Additionally, children generally don't often know that there is a mechanism. It was unclear to the participants where or when children were meant to learn about these processes, and indeed if this (need to learn) should be their responsibility, rather than the digital providers
    - There was discussion around the length of these processes, and what that means for someone when they are 14-year-old, for example
    - The individualised nature of complaints processes are part of the problem, and the lack of a 'systemic complaint system' places the burden on young people

- Over reliance on complaints mechanisms was seen as a failure in itself:
    - The problem can be improved by taking the onus off young people and focussing instead on the design of system and responsibilities of providers

- Young people need to have faith in the complaints system for it to work, but it is hard to engender trust and confidence in the processes, especially when there is a lack of trust in data processing practices more broadly, and many adults are also confused or uncertain of this too

2. **What would 'good' open and transparent management look like for young people? Are there examples of what works for young people when it comes to communicating with them about their rights? What would reasonable look like? Are there reasonable steps we could expect platforms to take?**

- There was a discussion around different sorts of communication styles that could work for children, including for example Tiktok style video on privacy and rights designed for young people that might be accessible-friendly, or picture books for younger children

- There is a need for transparency to consider the needs of different ages of young people, and other ways to support meaningful understanding of data handling practices

- There was a discussion about co-design for creating trusted pathways for young people to describe and support good and transparent data management practices

- Children may have a fear of losing control, involving them in the process could help engender trust and offer meaningful control

- The discussion explored potential parallel industries that might be worth investigation. Is there, for example, a way to explore how-whether banks meet open & transparent data handling practices to help find a precedent in terms of children's rights and access?

- There is a need to reframe expectations on providers to demonstrate how their privacy processes and understandings are appropriate. For example, providers may need to provide internal training, or map where a child could easily find and access information. It could be a 'reasonable step; to require providers to provide certain proofs of processes around children's data

- There was an awareness that digital companies will likely push back on additional responsibilities, as it works for them when responsibility is placed on children.
    - There was a discussion around the risk of platforms raising the age of use to 18 to use their services so as to avoid meeting responsibilities to younger users, noting that this has not happened in other jurisdictions with 'Children's Codes'. Children have rights to access the digital world
    - Potentially there is the need for an industry body or association to help businesses understand their responsibilities as well as the benefits of the Code

- There is also a role for civil society to play in supporting young people and ensuring the Code adequately protects them, and for improving the understanding of the rights of young people more generally

- The potential role of State and Territory privacy agencies was also discussed. Services likely to be accessed by children should ultimately have responsibility to meet the needs of young people's digital privacy, as described in the Code. There were also questions about whether this could be supported by State or Territory oversight, in state privacy agencies for example? The Code could then be conceived of as nationally consistent *minimum standards*

3. **Are there children and young people who may experience additional risks, or face heightened consequences, where this principle fails to be achieved? What regulatory safeguards, or additional considerations, might be necessary for them?**

- Special protections may be needed to ensure young people from a range of diverse backgrounds can access APP1 protections. They include young people from CALD communities, young people with disabilities, Indigenous young people, neuro-diverse young people, young people in out-of-home-care, experienced domestic or family violence or harm, LGBTIQ+ young people and so on

- Risk assessments, or privacy impact assessments, should ensure that particular needs of groups vis-a-vis particular services are taken into account. These assessments should specify certain risk factors, likely impacts and how they affect different cohorts of children

- There was a discussion about the inevitability of industry 'push back' and the need to set and hold expectations for the 'gold standard' of simple and transparent communications

- Child-friendly documentation and processes a mean greater accessible for everybody!

- Service providers should accept a minimum standard of language use (for example, a reading age of 8) that is age appropriate, but also easier for general understanding

- There needs to be a child friendly version of the code itself

APP 2: Anonymity & pseudonymity for children

Key insights

- Anonymity and pseudonymity are complicated concepts, and need to be made clear to young people. This includes explaining what their rights are, how their data will be used and how anonymity or pseudonymity could impact the use of a platform. These explanations need to be age appropriate to enhance the ability to make meaningful decisions that are mindful of children's evolving capacity.
    - There is a particular need for clarity around public anonymity and anonymity for account creation and management
- Children must be given meaningful choice and have agency around decisions for anonymity and pseudonymity. The role of parents also needs to be considered
- Anonymity and pseudonymity provide benefits for young people, but also present potential drawbacks for services and service providers
- There are risks that requirements for anonymity and pseudonymity will be misused by platforms to:
    - Deny access. There ought to be obligations on platforms to not deny or limit services for children when they are anonymous or pseudonymous
    - Offer a reduced service or 'negative service impact' for children if they choose higher privacy settings in general
    - Collect more information from third parties
- There is a need for impact assessments, be it data privacy impact assessments or child rights impact assessments, around how platforms use children's data in general but these need to consider anonymity and pseudonymity. These need to consider the experiences of vulnerable young people, and ensure that anonymity and pseudonymity are the preferred positions, except where it is in children's best interests to use identifiable data

Discussion

The discussions around centred around three key prompts:

1. **Why, when and how might anonymity or pseudonymity be important to children online? Do young people get to enjoy their right to be anonymous or pseudonymous online, not only with what they post but the data that is collected about them? What rights might this affect?**

- Anonymity is vital to children, it gives them the capacity to explore identities online and to try different ways of seeing and being, safely. This has implications for their other rights both online and offline

- The discussion suggested that general young people do not always enjoy the ability to be anonymous and pseudonymous, but that they should have rights around this, especially to make informed decisions

- Family dynamics and intertwined data needs to be considered:
    - The ability to be anonymous and pseudonymous is complicated for younger children, where parental data and children's data can be intertwined, for example a child could be

pseudonymous on public facing aspects of Roblox, but the underlying data is identifiable and linked to a parent's account
    - Anonymity and pseudonymity might be particularly important for older young people within the family content. Young people may display help seeking behaviours around mental health or sexual health, or be accessing support around sexuality, that they may wish to remain private. Data collection practices could to an extent affect this

- There are potential parallel learnings here from helplines and tiplines, where young people are able to be pseudonymous while support is provided. Again, this raises the question about public facing pseudonymity and 'behind the screen' data collection

- The commercial drive to collect data in general is in conflict with children's right to remain anonymous or pseudonymous:
    - Often identifiable data is only required at the point of translation, but platforms often try to gather identifiable data early on in a user's journey
    - Platforms often incentivise users to create accounts and share personal information, with discounts and deals etc
    - Opt-outs are also problematic for children, as it places the onus on them to take actions

- Research shows that some children are willing to participate in the trade of data for free services. It needs to be made clear to young how their data is being used and in principle, this should not affect their right to remain anonymous and pseudonymous

- Doxxing remains an issue. How do you seek remedy for the right to remain anonymous if you are doxxed? Platforms should have an obligation to remove doxxing materials in general, especially for children

- There may be a few balances or compromises that need to be 'struck' between platform benefit and children's benefit that the Code could address:
    - Some identifiable data collection does help platforms, some helps children while some also harm's children's right to privacy (and other associated rights). For example, where children are logged into services anonymously, platforms do not currently 'turn on' safety features, such as content recommender system filters. In this way being anonymous does not help children. However, platforms could turn on safety and privacy features for anonymous accounts (and some already do). The Code should provide guidance around this
    - Providing children with accounts gives them some control over their ability to access, correct and delete their identifiable data. While this may not matter for truly anonymous data, there are issues in thinking around how pseudonymity may affect data deletion requests in practice (Noting that currently, children do not have the right to request the deletion of even identifiable data)

- The code should help platforms to provide children with both adequate protections and adequate information about data uses

- There was discussion around data brokers in particular, and how anonymity and pseudonymity might affect the trade in children's data. Where data reaches data brokers in identifiable ways, the risks to children are amplified because of unrestricted onward processing

- There are issues in thinking around pseudonymity and the right to delete. How could pseudonymous data be deleted in practice? (Noting that currently, children do not have the right to request the deletion of even identifiable data)

2. **What might good look like for young people? Are there examples of what works for young people when they are able to be anonymous or pseudonymous online? Are there parallel learnings from other industries or areas where anonymity has been improved for young people?**

- There are some examples of good practice online already, such as Reddit where accounts are all handles and users are not encouraged to publicly disclose their identities. However, viewing the user histories of handles can still create issues

- 'Good' included a number of characteristics:
  - Young people having control over their ability to be anonymous and pseudonymous
  - Young people meaningfully understanding the choices available to them and any 'trade offs' they need to make
    - This includes getting the 'timing' right about when to explain anonymity. Helplines and tiplines can provide good practice examples here, where they tell people about anonymity immediately. They tell young people about their privacy policies before connecting them with a counsellor, which creates a 50% drop off but this gives young people time to consider and pull back if they want to
  - Young people 'benefiting' from any initial design decisions (such as opt-ins vs opt-outs etc) and anonymity or pseudonymity by default
    - There was an example discussion about an EdTech app, where the only public information required is a pseudonymous handle and a password. (Noting that depending on the platform and integrations, apps might be pulling identifiable data from child users via SDKs, third parties integrations or cookies and tracking pixels etc)

- There was a discussion about operationalising the Code, and the need for guidance to weigh up different settings and contexts and different platform requirements

- The need for the Code to address children's evolving capacities, rather than chronological age, was discussed. For example, for young children, pseudonymity is helpful to allow them to access health information and websites, while for older young people considerations around the need for and interactions with parental consent need to be considered

- Young people may not understand the difference between anonymity and pseudonymity. Young people want a seamless online experience including the ability to connect with the same friends online. Public facing pseudonymity can offer this, but it is unclear that public facing anonymity can (e.g. playing online each week with 'BlueRabbit27' vs random players each time). Platforms could provide:
  - Guidance to young people around the difference and how to manage this, and
  - Default to the least identifiable information types appropriate at each decision point

- The role of third-party ID tokens could be considered here, to provide the least information necessary at each transaction point possible. However, this raises other privacy concerns that need to be considered

3. **Are there children and young people who may experience additional risks, or face heightened consequences, where this principle fails to be achieved? What regulatory safeguards, or additional considerations, might be necessary for them?**

- Young people in rural areas need particular consideration. Reidentification might be a much easier process in smaller communities/geographies than larger metropolitan areas

- Some young people may face higher risks where this right fails, generally including young people who are more vulnerable in general. These include:
  - Survivors of abuse and violence, including sexual abuse, domestic and famility violence, for whom anonymity might be particularly valued
  - Young parents and young carers, who may seek additional help from online services, may also be particularly vulnerable
  - Young people experiencing mental health issues, who may seek additional services online and for whom anonymity might be particularly valued
  - Young people in out of home care, who may not have access to individual devices and whose help seeking behavior may make anonymity particularly valued
  - Young people with refugee or migrant backgrounds, particularly if they share devices
  - Children and young people with disabilities for whom digital devices and online services may be crucial communication devices

  In considering potential vulnerabilities, there is a need to avoid an overly paternalistic approach, assuming that all cohorts of young people will be additionally vulnerable without reflection about the rationale

- The need for anonymity to be considered as part of a risk assessment process was discussed, whether this is a data protection impact assessment, a best interest assessment or a child rights impact assessment. There is the need for anonymity and pseudonymity to be deployed in children's best interests, and an assessment would be key to this. This includes asking questions such as:
  - Who is the identifiable information for? Is it to benefit other users, the platform or service, or the young user?
  - Who is the information transacting to? Who has access to it, for what purposes and what 'onward sharing' do they do?
  - What are the circumstances where platforms have an obligation to understand identity? Where might this be better for privacy?
  - Will the information be public facing or 'behind the screen'?
  - Where does the risk sit?

  Anonymity is not necessary in every instance, but there was a discussion around whether it was preferable in each instance. Pseudonymity is potentially a more useful default expectation, both in front of the screen and beyond the screen

- Particular types of technology were discussed, including:
  - EdTech platforms. Where there are difficulties with children or parental consent versus school level consent

    - Location tracking services. It's difficult to be anonymous or pseudonymous in these services, but they raise serious issues around offline perpetrators and account access

- The role of parental consent was discussed. There can be a power imbalance between children and adults that needs consideration when relying on consent mechanisms. Meaningful choice is critical here, but often not available. Children need to be able to have sufficient choice, information and the opportunity to exercise their agency to craft their own identities online (and to decide what their online identities are, or to 'select for the durability of identities online'). Anonymity and pseudonymity can be critical in achieving this. Children need agency

- Terms and conditions fatigue is real. Agency and choice cannot be exercised by 'accepting' a privacy policy alone. There needs to be different ways to get this consent from young people. Meta has tried to do this recently with video explanations, but these may still be too overwhelming. More work is needed in this space

- Consideration needs to be given about children's evolving capacities and ongoing consent requirements. Platforms should consider reminders for children, for example asking 'this is how you currently engage, is that still OK with you?'

APP 3A: Collection of solicited data (young people's consent)

Key insights

- Digital platforms and industry have moved far beyond the approach of identifying the purpose of data processing, and then limiting processing to this use. Often, it is not clear how current data practices relate to their original purpose limitations
- The regulatory environment has struggled to keep pace with 'standard' practices, this has created significant issues
- Child rights principles would be a useful foundation for a Code, but the current consent model fails to adequately protect children's rights. The Code would remedy this by shifting the onus from child users — and asking them to consent to unnecessary and unsafe data practices — to platforms
- A code that outlines the obligation on the platforms to use solicited data in reasonable ways, tied to the purposes of collection that young users would reasonably expect, would help advance children's rights. Data should only be used for an identified and specific purpose
- Meaningful consent requires access to transparent and easily understandable information about data and how it is used

Discussion

The discussions around centred around one key set of prompts:

1. **Do young people meaningfully consent to data collection in the current digital environment, especially when it comes to social media, relevant electronic services and designated internet service? What does meaningful consent look like for young people in a world where these services are integrated into digital childhoods?**

- The conditions for informed consent are consistently not reached online:
  - There is significant research that suggests that young people do not feel as if they have any option but to "accept", which raises concerns around meaningful choice
  - Terms and conditions are not accessible, presented in a format for ease of understanding and with clear information as to the content, obligations and consequences
  - Ongoing consent is rarely sought. Once off inferred consent is not appropriate when children use things like chat or forums. Often children and young people change their minds when they get older about what is online of theirs (or of them put up by their parents)

- We note that children and young people are already critical of the mechanisms for obtaining consent. Research consistently reveals that children and young people express the view that they don't want to be 'tricked'. They often have a heightened awareness of being tricked. Different languages are used to express this but the conclusion is the same

- Young people describe often opting in just to use the service; in order to stay connected with their peers and social circles. Privacy notices do not provide clear information and the

assumption is often that it seems like they will collect everything. It may be sometimes useful to provide a clear description of what a provider is not collecting

- Platforms are incentivised to collect, and consistently harvest, more personal data than is reasonably necessary. This may include to target advertising or ostensibly to adjust experience to cater to the person
    - We noted that it usually only requires three pieces of de-identified data to reidentify a person. Easy for even anonymous data to be abused or misused

- The age of consent was also raised as a concern. There are limitations with the current OIAC guidance that states that under 15 years of age, a child cannot meaningfully consent. From a child rights perspective, this is arbitrary and while designed as a protective measure, further undermines the use of a meaningful consent model

- A meaningful consent model is in fact flawed for adults as well. In the context of many services (such as Ed Tech), the consent of a parent on behalf of a child is not meaningful and informed

- It will be important for the Code to unpack the complexity around the interactions of consent by a child and by a parent or carer on their behalf. And the limitations of this as a 'once-off' consent

- We noted that the consultations with children and young people can demonstrate that many are 'digital natives' with a more sophisticated understanding of online environments. But this does not mean that they do not have expectations as to trust and transparency. They do not appreciate being lied to or taken advantage of. They want to know what data is taken and how it is used

- We also noted that young people can be vulnerable, may be more likely to take risks and may lack impulse control to understand and appreciate the risks of doing certain things online. (We also note that many adults are vulnerable and lack impulse control, and that supports for young people will also support adults)

- The Code should find ways to put the onus on the platform / collector of information / potential perpetrator of data misuse. We must shift away from blaming the victim. This includes abandoning the 'meaningful consent model' as it fails to recognise the considerable power imbalances at play

- Transparency is a necessary but not sufficient condition. We support the use of the best interests principle drawn from child rights jurisprudence. The obligation to secure privacy should rest with the collector of data to ensure that they are acting in the best interests of the child

- The introduction of a duty of care that rests with the providers, in the terrain of online safety, is a potential model for the privacy space

- We discussed the need to clarify what is in the best interests of the child. It includes recognition of the right to participation and agency of the child to the fullest extent possible

taking into account development and circumstances. This does include providing a child with opportunities to consent to the fullest extent

- We noted some of the historical criticism of the Convention on the Rights of the Child as paternalistic in its drafting. One correction could be to recognise a child as a citizen. It should be about protecting their rights as citizens. That is, as citizens now and not just as 'citizens in the making'. Current child rights jurisprudence requires the views of children and young people to be considered

- Using child rights principles, children have a right to control the use of their own information and identity. The mechanisms of online consent are problematic. We note that often researchers spend 1.5 hours explaining use of data in seeking informed consent for research purposes. That is almost unthinkable in an industry context

- At the least there must be a meaningful approach to knowing the purpose of collecting and using the personal information and some limits on what can be collected in the first place

- Child rights principles are the founding principles

- We reject the meaningful consent model

- We endorse an examination of whether and when advertising constitutes a purpose that is in the best interests of the child; and that in some circumstances, that will be never

APP 3B: Collection of solicited data (parental consent)

Key insights

- Consent is often flawed in the first instance, both for children and for parental/guardian consent. Alternatives to the consent model are lacking, but we would like to see the development of new models
- Parental consent is not always nor appropriate or safe proxy for children's consent, but has significant consequences for children's lives and ability to access the digital world
- It is difficult to assess when parental consent is appropriate versus children's consent. Age is at best a proxy for the capacity of the child. One potential solution for the Code could be to describe expectations and best practice around parental consent for different age bands
- The role of consent within a school context also needs consideration

Discussion

The discussions around centred around three key prompts:

1. **What is the role of parental consent in the digital world? What circumstances should require parental consent versus young people's consent? What rights could this interact with?**

- There should be greater responsibilities on platforms to minimum data collection in the first instance. This should be prioritised over requirements for 'voluntarinesses' (achieved through 'consent'), or the role of parents or children to consent to excessive data collection. Consideration needs to be given to what we are asking parents or children to consent to

- Consent is often flawed in the first instance:
  - It should be subject to a 'fair and reasonable' qualification for consent. Consent isn't useful without the 'fair and reasonable'
  - Consent fatigue is real, there is a real burden on younger users and their parents to consistently consent
  - Consent is rarely a free choice or seen to be a real choice. The Infrastructural nature of these platforms means that the only way you can access content is through 'consent'. There were questions about if this was consent or coercion
  - Consent processes are a blunt instrument that lack the type of granularity of decision making we hope a Code could support

  Alternatives to the consent model are lacking, but we would like to see new models both in legal protections, but also in practice (for example, could apps take a different approach where consent is declined, rather than 'collapsing in' and denying service)

- Parental consent is not always a safe nor appropriate proxy for child consent. For example, in the context of family violence or out-of-home-care there needs to be the capacity for children to consent or / secure 'guardianship' consent from other adults

- It is difficult to assess when parental consent is appropriate versus children's consent. Age is at best a proxy for the capacity of the child, and there are well documented tensions between human rights capacity, medical capacity and legal age when it comes to consent. An

age-based framing on autonomous data individuals is problematic. One potential solution for the Code could be to describe expectations and best practice around parental consent for different age bands
    - Consideration needs to be given to young people's data collected when they were under 18 via parental consent, and its status once they turn 18. Data consented to by parents or guardians for under 18 year olds should not be processed under the same consent once they turn 18

- The consequences for children where parental consent is sought can be extensive. Many aspects of a child's life depend on the consent of a parent or guardian. Where there are difficulties accessing parental/guardian consent this can diminish the meaning of consent to 'access' to the young child e.g. in the case of after school care, sports clubs. Consent has become synonymous with 'terms and conditions'
    - This is especially true in educational settings. Parental consent is often sought for software or photography purposes, or even school level consent. This can create complications

- The Code should introduce minimum requirements that set the bases for when and where parental /guardian consent is necessary:
    - At a minimum, we would expect parental consent to be sought where sensitive information is being collected or processed
    - Data and information collected under parental consent needs to be time-sensitive. Consent should be renewed, reaffirmed, particularly as children get older
    - The best interests of the child need to be prioritised within the parental consent process

- We discussed the need for a two tier system, where there were lots of extra protections, barriers, cost implications to collecting and using children's informations
    - There was a discussion around the tendency of platforms to make parental consent as limited as possible, and the existence of predatory industries

- There was also a brief discussion around the security of shared data and data sent for onward processing, and requirements to encrypt data 'in transit'

2. **What might good look like for young people? What does a digital world that gets the balance between, or combination of, parental and children's consent look like? How might these processes work?**

- There is a greater need for accountability and transparency from digital platforms and services
    - There were discussions around the need to address the incentive structure that digital platforms and services operate under, to create meaningful accountability — this could be punitive through fines or incentivising good practices
    - With regards to transparency, there were discussions about which process and systems could we ask platforms to report around, when it comes to the efficacy of parental consent processes

- There needs to be ways for parents or guardians, or children, to decline to consent to excessive data processing without being locked out of a service, there has to be the possibility of declining or opting out and still enabling participation

- There were also discussions around the need to place obligations on providers to explain how and why personal information is necessary to the purposes it will be used for. This includes requirements for some sort of 'active reflection' on behalf of platforms, to consider what they are asking for consent for, and to test the adequacy of both the ask itself, and the systems to collect it

- When it comes to ensuring that consent mechanisms for parents are meaningfully understood, the need for comprehension testing was discussed. This includes understanding comprehension levels among different target demographics

- There are a range of actors involved in parental consent processes. For example, schools require families to sign up to apps, and parents are often consenting within a social environment. Regulators need to look at the relationship between the school and the family, rather than simply the platform and the parent. There are other parties shaping how this consent is applied

- The Code will be enacted within a range of social contexts such as sports clubs, youth groups, schools etc, so the Code needs to design it with this in mind . There is a relational aspect of privacy, and it is contextual in nature

- There were discussions about health and wellbeing data gathered under parental consent, and the exemptions. This needs to be considered explicitly in the Code

3. **Are there children and young people who may experience additional risks, or face heightened consequences, where we fail to get the balance between/combination of parental consent and children's consent right? What regulatory safeguards, or additional considerations, might be necessary for them?**

- Some children and young people are 'experiencing vulnerability' rather than 'being vulnerable', so that we don't penalise and deficit certain people through additional safeguards

- The Code should prevent platforms collecting additional information to identify 'vulnerable people'

- The onus needs to be on the services provider to take extra efforts to clearly discern when collecting data is appropriate

- When it comes to vulnerability based on age, the benchmark of 15 years has never been tested; we're stuck between the prescriptions of legal regimes and the definition of a child as 18-year-olds being. The Code could help provide guidance around this, for example, addressing;
    - How to balance children's views and the need for children's consent *vis a vis* parents.
    - The best interests of children and how to prioritise these
    - Potential proactive approaches to consent through tiered ages

- There may be different sets of accountabilities and controls between under 18 and over 18 year olds.

APP 5: Notification of the collection of information

Key insights

- The formats of notifications need to change. Online education design techniques need to be deployed, such as the use of images, graphics and videos rather than just words. Where “dark patterns” are currently deployed, they need to be replaced with “fair patterns” that nudge young people towards meaningful comprehension
- Meaningful and clear information needs to be provided to children about the nature of data collections and use, as well as potential consequences of data collection
- The timing of notifications also needs to be more ‘proactive’. There is a need for notice to be continuous rather than a one off, rather than bundled in with signing up
- The length and burden of notification also needs to be addressed. There is a need to balance the wants of users to access services and platforms quickly, and also to be informed about the data consequences of doing so. Currently, notice of collection of information is seamlessly presented to children and there may need to be some friction so young people are more effectively engaging with notices
- There are contextual issues around notification; children are not a homogenous group and will have different abilities to understand notice and different supports around them (see APP1). Parents, caregivers and teachers will also have different abilities to understand notices.
- The goal must be to protect children’s rights, and the ability of ‘notice’ alone to achieve this is limited.

Discussion

The discussions around centred around three key prompts:

1. **Are young people made sufficiently aware of who, why and where their data is processed? Are current online privacy notices working? Do young people access them to be sufficiently informed as APP 5 imagines?**

- There was a general consensus that children are currently not made sufficiently aware of data practices through the currency notice regime. Children were not alone in this regard; notices aren’t done well generally, and the consequences are particularly acute for young people
  - Research into adults comprehension suggests that less than 12% of adults are reading notices, so notices become part of a process which you just tick to access them
  - Young people do not have a greater sense of ‘control’ over data than adults

- There were also questions about the ‘value’ or meaningfulness of notices in general, given that consent is rarely a free choice. Users often need to accept any notice that is given to them, because declining restricts service and locks people out of online communities

- Notices are difficult to read and comprehend
  - Frequent changes to privacy policies complicates things further
  - Disclosures can be excessively general (for example statements around ‘we disclose to third parties’ does not always make clear who the third parties are)

    - Cookies banners and policies might not even be seen by children
    - The use of terms and conditions can be overly complex

- Notification and consent are not the same, but often where parental consent is sought, children do not even see the notice. A parent may just consent to the terms and conditions and these are not always distinguished
    - There are also questions about when and how parental consent is sought instead of children's consent (see APP 3B)

- The role of notices within school also needs to be considered. Edtech companies often seek school level consent, and design their notices accordingly. It is unclear what children know about how their data is being collected and used in these products

- In general, digital business models do not incentivise meaningful notice. There are limited expectations and no incentives for data processors to offer meaningful notifications (or limit data collection). Those who want to extract information have a significant bias in terms of determining what they can do or what harm can occur, and platforms have a 'goal' to increase profit rather than focus on data protections. There is a power imbalance between the digital service and the end-user. This creates additional burdens on regulators to increase standards as well as update expectations around what is done with data

- Children often experience notices in specific ways:
    - Many do not read privacy notices, often feel coerced in providing data, and just click yes or they won't have access
    - Sata collection feels normalised and like an inevitable part of their online lives
    - Young people sometimes do not care about data collection, their awareness and care factor is low unless the potential consequences are spelled out for them
    - Young people may have short term needs in relation to getting access to data and may not see the long-term consequences of the data
    - 'Privacy' as a concept has different meanings for different children, especially a relational aspect. While this is beyond the scope of the Code it is important to note that for children, the concept of privacy is also about whether parents or teachers can see what they are doing. Privacy from parents and teachers is important in terms of balancing emerging agency and evolving capacities

- Poor notices can create additional risks of harm. They can convey to children that there is an effective or 'fancy' privacy protecting policy in place, but this is not always the case. There is a danger here from creating a false sense of security through a complicated notification regimes

- More effective notices would focus on:
    - Succinctly highlighting what personal information platforms are collecting and how platforms are going to use data, rather than showing long privacy and policy information
    - Highlighting where information is going, potentially through case studies

2. **What might good look like for young people? Are there examples of what works for young people when it comes to communicating policies or complex processes that we can reflect**

on? Are there parallel learnings from other industries or areas where 'business' policy communications has been improved for young people?

- 'Good' looks like:
  - Changing the focus of existing notices from 'getting someone onto a site in the least amount of time' to as much time as it takes to provide meaningful notice (as the APP requires)
  - Changing the true north and privacy notices to change the objective of understanding. This involves changing objectives for user group and the platform
  - Changing the framing from compliance from looking at 'the ability of a user to see and quickly leave a notification' to the ability for a young user to 'see and understand the privacy policy'. This should incentivise the end of sneaky policies
  - Making notification a little bit more 'active'. Currently notifications are very passive and are not being read
  - Notices that provide clarity around not only what data is being collected and how it is being used and shared, but also what the impact or potential consequences of this could be. A good notice is contextual and talks about the information in the context of what is happening.
  - Notice is a range and may be children and parents as relevant

- A rights-based lens may be useful in helping think through how the form, content and timing of notices could work in children's best interests

- The form or presentation of notices matters:
  - What works in digital environments is dark patterns or more interactive or visual nudging techniques, these could be deployed but to increase comprehension. Such as "fair patterns". We could use these sorts of visual tools and techniques to get people to move beyond just clicking yes to accepting data collection requests. Discussion noted that the EU's *Digital Markets Act* and *Digital Services Act* prohibits the use of dark patterns in consent pathways, creating more genuine options around choice in accessing a platform
  - There is a tricky interaction between the purpose of APP 5 – to give notice – and the purpose of nudging and changing behaviour. But this could be considered harnessing the essence of APP5 — a requirement to give sufficient and effective notice — towards children's best interests
  - Short visual summaries are possible, and platforms already do this. For example, Spotify wrapped is a strong infographic, and could provide a model for a visual lead notification

- The timings and timeframes of notices also matter:
  - Ongoing notice requirements could be helpful
  - At the moment, notice and consent is designed to be as frictionless as possible. There is an unhelpful motivational alignment between young users wanting to get to sites as quickly as possible, and platforms wanting to through the notice process as quickly as possible. There is a question about the need to add friction to make the notification engaging, meaningful and understood for children
  - Signposting a time frame for notification (such as this policy takes 7 minutes to read) and comparing this to the time spent on a platform (such as the average users uses this website or platform for 4 minutes, or 4 hours a day) could also be useful

    - Parents and children are time poor, so excessive notifications should be discouraged. Consider what is meaningful information for young people, and include only this in notifications
    - Ongoing notifications might also be important. Intermittent notification might improve trust or satisfaction with data collection in general. If platforms show you about what data they have about young people, and how it is being used as they use a service, this may increase understanding

- The content and language of notifications also matter:
    - There is a need for translation into child-friendly information. Currently notifications are very legal and not very clear nor accessible for most people. For young people to understand, the legal language needs to be revised

- Children's evolving capacity might also create changing preferences for notices, for example:
    - What is appropriate to ages of 11 to 13 can vary dramatically, things change and they may want to change the way they share
    - The concept of permanency and the concept of time will be different to teenagers, so notifications around data retention may need additional clarity
    - The idea of a 'quick escape button' was discussed, or the idea that good notification include the ability to 'escape' and remove the data if they change their mind

- Dynamic presentations about data use might be useful tools to make notices 'real'. For example, web browser could more clearly show where data is going so young people can see what is being tracked everything

- Guidance that could be useful in a Code includes:
    - Provide further clarification around requirements for notices by age band, or at least primary and secondary age young people
    - Outlining proactive expectations and obligations on platforms to do cognitive testing of their notices, including reviews of language, timing, cadence and the 'meaningfulness' of content. Others noted that cognitive testing was 'murky waters' for a whole host of reasons
    - Provide clarity around the scope of collection of information and describing requirements for ongoing notification where necessary
    - Require platforms to demonstrate the steps they have taken to increase the ease at which users can understand data and to improve their mechanisms of notifications. Ideally, this would be coupled with clearly articulated obligations for platforms to address risks identified in their notification systems (and other risks as well)

- There was discussion around if platforms have the capacity to know and evaluate what is working for children, and implement improvements in notices for children. Online learning design may show what children know, and integrative learning is possible, but there is currently no incentive for platforms to adopt this voluntarily

3. **Are there children and young people who may experience additional risks, or face heightened consequences, where this principle fails to be achieved? What regulatory safeguards, or additional considerations, might be necessary for them?**

- From a rights perspective, children are too often represented and treated as a homogenous group. There is a need for systems to adapt and respond to different demographics needs and cohorts of children. Notices cannot always be blanket statements so need to be wary they have different needs. Different notification methods may be needed to increase privacy (and safety) for different young people

- Different young people might have different needs from notices:
    - Young people who may have experienced online trauma may engage with privacy in a different way
    - Young people who have had experiences with the youth justice system or out of home care may have different perceptions about the risks described in notices
    - Age, developmental differences and neurodiversity may also affect the way young people cognise notifications
    - Young people from whom English is a second language may also find current notification scheme daunting
    - First Nations students may also face issues with literacy of language and need different modes in which information is presented. In addition, there is a complicated history for Aboriginal and Torres Strait Islanders when it comes to the collection and use of their data. Government data collection is often not trusted, and there is a mistrust in data handling practices in general

- The use of technology at school also creates an additional layer of complexity for many young people. Not all schools will equally share the notification with young people, and there are potential inequalities across school processes that map onto existing inequalities. Trust is an issue

APP 6: Use or disclosure of children's personal information

Key insights

- The fiduciary principle of do no harm needs to be the first principle in governing the use and disclosure of children's information. This could be understood as a way of interpreting requirements
- Like all APPs, APP 6 is interconnected, and the use and disclosure of children's data is closely connected to:
  - The collection of solicited data under APP3. Improvements in data collection practices would also help to reduce risks in data use and disclosure practices
  - Notification requirements under APP5. Simpler, cleaner and more streamlined notice would reduce reliance on exemptions under APP 6.
- The Code could allow for authorisation for the use of data for academic or public interest research purposes
- Overall, the code needs to be rights based and prioritise children's best interests, rather than the rights of for profit companies

Discussion

The discussions around centred around three key prompts:

1. **Thinking about how young people use and experience the digital world, what are the risks that 'onward' use or disclosure of their data might pose? Do you think data use is sufficiently limited to its original purpose? What about the 'advertising exemption'? What rights are impacted here?**

   - Before we think about how children's data can (or cannot) be used or disclosed, we need to think about:
     - Data minimisation in the first instance (APP 3). This is the most effective harm reduction principle
     - Notification. There must be an obligation on platforms to explain why they are collecting certain information. The Code should include requirements for notifications to be prepared in 'closed ways', such as 'we will only use data for XYZ'. This forces platforms to be very specific about what they're doing

   - When it comes to requirements for fair and reasonable use of children's data:
     - Reasonable expectations will differ from a children's perspective to a legal perspective
     - They will also differ between children and adults. Just because an adult's reasonable expectation is that their data will be used for XYZ does not mean children have this expectation. It is reasonable to expect that children would not expect their data to be used in certain ways as they have not experienced life or digital life long enough to know that data is used (including for secondary purposes). However, cynicism may bleed into children too
     - Other activities for which data is used (secondary purposes) needs to be proportionate and specific

        - An example was provided of universities using information collected to organise an open day for high school students, with a secondary purpose to send them information via email. In this instance, there is a direct related use of that data
    - On secondary use on onward processing:
        - If the secondary use has no benefit to children, there should be a presumption against the use built into the code
        - Secondary uses should not include training for AI models for example. Privacy policies around the world are being rewritten to include AI uses, but this is not necessarily reasonable for children
    - There were questions around the use of the material benefit test to understand fair and reasonable use. This may be too lenient, and too easy for industry to meet without meaningfully realising children's right to privacy
    - There was discussion around potentially exclusionary approaches to defining reasonable use. For example, for clarity the code could draw a clear line that says "personal information cannot be used for commercial benefit XYZ alone". The discussion noted that it will be difficult to prohibit certain uses, likely with pushback from industry around this, but the principle has the capacity to bring clarity

- Different use cases were discussed, including;
    - Geolocation data. There is a need to clarify the difference between sensitive and not sensitive information. Geolocation data can become sensitive for children quickly, and there is a need for guidance around reasonable uses of this
    - Mental health services online. Many say they use data collected for research purposes, but there is a need to be clear about what this means (e.g. commercial business research or public interest research). Usually, this is research to market their product better to other young people

- Date use can raise issues of economic exploitation. For example:
    - Through the business model of platforms. Children have become a 'product' of information capitalism, and some platforms' 'jump onto' vulnerable people. There was discussion around the harms of shaping children as economic subjects in general
    - The use of children's data for advertising (see also APP 7). Advertising, and the influence of advertisers was extensively discussed. There was discussion around if advertising in general is fundamentally harmful to children, or just advertising for harmful products. Restrictions in advertising for harmful products have different data and privacy implications than restrictions on advertising, or targeted advertising, *per se*. There was an additional issue that the targeted nature of advertising also might cause harm for vulnerable children in itself, such queer young people receiving clearly 'queer targeted' ads may out them to their family. A broadcast advertising model could be more appropriate, that is advertising that doesn't use personal information, rather is generalised advertising towards children. Industry may not like it but they usually make enough money to work around it
    - There were questions about whether children ever meaningfully consent to be marketed to. The discussion noted that children, including younger children, experience targeted advertising even when parents have not received notification or consented. Despite this, this practice happens 'in the open' and most targeted ads are clear that they are targeted. However, limiting direct marketing could mean parents have to pay for service (noting that this has not been the experience in other jurisdictions that have limited advertising the children on online platforms)

- Children often don't know about their rights until they are harmed. Code has to be realistic and find some way of supporting young people to transition into adulthood

2. **What might good look like for young people? What would a digital world that did not onward use, or share or disclose their data look like? Are there examples in the digital world where you see this happen?**

- A good Code would include:
  - A clear list of "things" that set out the expectations of the industry. The Code needs to provide shape to what we want from them
  - Proactive obligations on industry. This would include submissions to the OAIC to describe use and disclosure of children's data, and showing regulators how they use it, test it and improve it
  - The principle of transparency, and a duty to disclose if you use data and how
  - Requirements for public transparency too, to allow civil society and academics to see the data and see what industry is doing. That is, a requirement to make improvements and make them in public. The private sector may say that they don't want to disclose this information as it takes away their commercial advantage, but this has not been the situation internationally
  - Exemptions where necessary, and clarity around the use of children's data in academic and public interest use. This includes understanding the nature of the proposed research, who the researchers might be, who funds the research and if there are any conflicts of interest
  - Clarity for industry around the fiduciary responsibility and children's best interests. The Code needs to make clear that industry should be expected to do no harm

- Around the Code
  - Fundamental problem as there is an absence of a fiduciary duty to do no harm on industry. However, this is not built into the *Privacy Act* so may sit outside the Code
  - The Act is principles based, which allows interpretation and gives the Privacy Commissioner some capacity to develop a child-centred approach to guidance in the Code
  - The Code needs to prioritise children's best interests and children's rights. The best interests of children needs to be/is always pluralised, it is best interests and a collective model rather than individualised
  - Beyond the Code, there may be the need for a right of action in courts. This would help create a body of case law and a detailed articulation of what the responsibility of industry is
  - There is a need to better implement current privacy laws
  - The Commissioner needs to be able to review and enforce existing law and this new Code and this requires better resourcing

3. **Are there children and young people who may experience additional risks, or face heightened consequences, where this principle fails to be achieved? What regulatory safeguards, or additional considerations, might be necessary for them?**

- The ‘baseline’ consideration of children and young people for whom these Codes are created needs to reflect a wide diversity of children from varying backgrounds, in order to better support and secure their privacy
- Young people experience different vulnerabilities:
    - At different ages
    - With different experiences like disability, trauma, out-of-home-care etc
    - Context, for example socio-economic backgrounds

APP 7: Direct marketing to children

Key insights

- The Code needs to be co-designed with young people. 'Good' could look like young people playing a formative and active role in the design and management of their data (and consent processes where needed), with respect to marketing
- Behavioural data collection must be limited and managed, without removing young people's agency in terms of giving marketing consent in specific circumstances
- Young people who proactively offer identity markers could experience additional risks. Clearer, 'active' opt-ins and greater transparency should be required from companies who wish to directly market to young people

Discussion

The discussions around centred around three key prompts:

1. **Should young people receive direct marketing that is targeted to them based on the use of their data? What rights does this affect? Thinking about the specific exemptions in APP 7, do young people currently have the ability to adequately consent to data use for direct marketing, or the right to opt-out?**

    - There was a wide chorus of 'Nos' when the current capacity for advertisers to directly market to children was, and the exemptions that may allow them to do so

    - However, there was a counter discussion around the possibility that some young people may appreciate targeted ads, but in general research does not agree. There are layers in this conversation, for example, is it better for children to get targeted ads than untargeted ads, what is better? From a commercial purpose, consumer purposes or from a child right's approach?

    - There was a discussion about the role of age in affecting the perceptions of acceptability of direct marketing, and if differentiations are needed by age.
        - A 16-year-old can make a choice in response to marketing that may be very different from a younger child, but could be just as 'informed' as an adult
        - Recognising rights and supposed 'autonomy' for older children when it comes to consenting to privacy-invasive practices is an 'ethically murky practice' regardless
        - If we are pushing for code that recognises young persons right to exercise agency, their various capacities and consent, what are the benefits? The Code is an opportunity to drive up standards that protect the privacy of children
        - The code should protect children, regardless of their relations with adults

    - There are differences between targeted advertising (behavioural advertising) and consensual direct marketing. There was a discussion about different levels or expectations for these different types of advertising. If I have a commercial relationship with a brand I expect to be advertised to that might fall under direct marketing, but if I don't know why or how I am being advertised to, even if it is by that same brand, that is different, and children should be protected (and adults too)

- There was also a discussion about direct marketing and targeted advertising aimed at achieving a 'public benefit-good' or as PSAs (public service announcements) such as health or civil society ads:
    - A social enterprise example was discussed. Where ads are beneficial to children (such as bushfire awareness ads) a blanket ban on marketing might prevent children accessing them
    - There is a balance to be considered. How many 'public benefit ads' are run to children, vs harmful ads, vs ads that operate only for commercial purposes to trade with children? The iniquities and ubiquity of passive consumption of commercial (or worse) advertising for young people was discussed, despite limited examples of advertising to the contrary
    - Could we create exemptions for 'public benefit' ads targeting children, using best interests principles, or would this create an exclusion regime that would be exploited
    - But this exemption also raised questions about 'what happens to the data', and how would the data be collected just for these purposes. While some companies may be benevolent in their marketing and data collection practices underpinning this, others are not
    - Safeguards and exemptions are often duplicitously manipulated by companies, such as social media companies

- There was a discussion around the 'missing gap' around being able to distinguish between target marketing and direct marketing (as the Privacy Review Report proposals would have addressed):
    - The elements of bracketing out 'targeted advertising' would have been helpful in this context, and will still be helpful if they are passed later
    - We need to make sure that the Code is nuanced enough to provide guidance around direct marketing and targeted advertising differently. We don't want children to lose out on the ability to consent to receive helpful direct marketing, but we do not want them exploited by targeted advertising practices

- If the Code gets the processes for children right, this could also benefit adults who often experience the same privacy harms from the direct marketing / targeted advertising nexus. A step up in standards for children can improve the situation for adults

- Beyond the scope of the Code, there was also a discussion about protections for children and adults, specifically if we should outlaw targeted marketing to *everyone*? Or should a deliberate consent process without exemptions be more appropriate?

2. **What might good look like for young people? What would a digital world that did not use young people's data to deliver direct marketing look like? What does a good 'opt-out' look like? Are there examples in the digital world where you see this happen?**

    - There has been a fundamental shift in the nature of advertising that is worth considering. A Code based on 80s models of individualisation will not be helpful.
        - These models are no longer relevant, especially considering levels of addiction and volume of advertising that have become prevalent in the digital world

    - Algorithms are pushing the number of data points collected to facilitate advertising exponentially. This increases the power and potential privacy dangers to young people. This is no longer a debate about if advertising is good or bad for young people, or the content of advertising. This is a debate about how this model of advertising implicitly harms young people's privacy

- There were discussions around the possibility of design features for more control:
    - Such as as switch-off or toggle for (age appropriate) targeted marketing, however this is only appropriate if consent *is a justificatio*n to send targeted marketing to children (see discussions above)
    - The role of co-design, and enforcing active opt-ins and expiring opt-ins. For example, platforms may design their user-journey so that new opt-in are required after a period of time

- The difficulties of a consent model to allow targeted advertising were discussed:
    - Informed consent and recognising a young person's agency is important, and we do not want to patronise children *but* there is an uninvited risk of harms to privacy (and all the associated rights that connect to this). The discussion about the content of public service announcements (PSA) emerged again, and the idea of creating exemptions for the delivery of PSA style advertising but not through the mechanisms of data heavy targeted advertising emerged. Does the difference in the content that might be delivered to children justify an exemption around data processing in the Code?
    - Regardless, children's data should not be captured and used without specific consent in any instance. The potential for harm is far greater than the potential benefits
    - It's not a level playing field, and in this context, consent might not be the appropriate mechanism. Corporate interests *create* the platforms, *collect and sell* data - the Code need to provide guardrails to counter this imbalance, rather than relying on children's consent alone
    - We also need to learn from young people's existing lived experiences and current inconsistencies (ideally, to create consistencies). For example, young people often 'opt out' and still get marketed to, or 'unsubscribe' but still get advertised to. It's unclear if consent currently works, and if it should be 'baked into' the Code

- The role of targeted advertising that draws on the 'surveillance capitalism' model was discussed. This is the route through which most personal data collection is monetisation in the online context. Any moves that curb targeted advertising reduces the incentives to collect children's data, and could be the most effective method to create a culture of data minimisation. If you reduce the value of data collection, you (largely) circumvent the problem

- The potential impacts on industry were discussed:
    - Genuine ad creatives could reinvigorate the quality of advertising in the absence of 'lazy' profiled advertising, currently based *only* on data point profiling etc. This could actually be beneficial to the creativity of the advertising sector!
    - There was a general discussion that given the size and scale of the advertising industry and the fact that their own Advertising Codes to children are tightly defined, they will be fine. The scale of the changes created by any protections offered in Code will be minimal

- There is a value in transparency and embedding this within the Code:
    - The Commissioner may want to use the Code as an opportunity to outline what good transparency from platforms looks like
    - Advertising transparency models are additionally required to make companies share information that they use for targeting

3. **Are there children and young people who may experience additional risks, or face heightened consequences, where this principle fails to be achieved? What regulatory safeguards, or additional considerations, might be necessary for them?**

    - There are a range of young people who might experience particular risks from use of their personal data for direct marketing or targeted advertising purposes, including:
        - Children from different demographics, where data about their background would constitute sensitive personal information, such as indigenous young people, young people from culturally and linguistically different backgrounds, young people affected by disability, young people who identify as LBGTIQ+. The collection and use of data that contains these 'markers', for advertising purposes, creates additional risks
        - Children with particular health issues, such as those affected by mental health issues and body image issues etc, where data about their health may constitute sensitive data

    - For young people experiencing certain vulnerabilities, the content of the advertising that is deliberately targeted to them could be problematic. That is, the use of the data itself to enable the targeting mechanisms can create further risks. Patterns of self reinforcement can accelerate through profiling and targeted marketing. For example, 'skinny' ads can be targeted to young people with body issue concerns precisely because they engage with this content

APP 10: Quality of children's personal information

Key insights

- When companies hold incorrect information on children, it can lead to bad decisions and harmful outcomes, impacting on their safety, wellbeing, and access to opportunities. The risks of incorrect information is particularly relevant in a children's context, where lots is changing about their circumstances on a year-to-year basis
    - There needs to be special considerations for children at risk of heightened consequences (for example, children in out-of-home-care, those experiencing domestic or family violence, homeless, on income support, or experiencing mental health issues etc). For these young people, their details change frequently and the need for a fixed address for example can hinder delivery of services
- Inaccurate inferred or 'profiled data' can also have really negative outcomes for children. Where platforms create profiles and make decisions based on these, children should be able to see and edit and correct their profiles. (Limitations around the use of profiled data may also be necessary, see APP6 & 7)
- Health information and financial information is particularly important from an accuracy perspective. These datasets need to be in scope of the Code
- Platforms need to provide easy-to-access, frequent-prompted user update mechanisms for children and parents/carers (where appropriate) to review and update their information. All companies should have processes in place to audit and review their information holdings.
- Safeguards for vulnerable children could include: risk assessments, more control over data access and sharing, and 'online suitcase' data services
- 'Up-to-date' and 'accurate' data are key needs for the advancement of children's rights. This needs to mean that platforms should destroy old data that is no longer relevant

Discussion

The discussions around centred around three key prompts:

1. **What might the risks be for young people where this principle is not realised, and incorrect, out of date or incomplete information is used? What rights could this affect? Are there types of data that should require additional protections?**

    - As a starting point, digital platforms have long held that they do not collect personal information on their users, relying on the 'aggregation' argument. As a result, this keeps them out of scope of APP 10. But the profile data ('this is who we think you are') may as well be personal information, as the platform uses it to make assumptions about users. There is an obvious 'between two chairs' problem here where users cannot view or access information (see APP 12) digital platforms hold on them because the platforms deny its existence or re-shape its characterisation

- If incorrect or simply out-of-date information earlier in a teen's life is in ready circulation, this may affect their employment prospects later in life, even their social and emotional wellbeing

- There are risks from adults sharing information about their own children. Could be as simple as photos shared by their parents that may impact them in future.
    - Scope of Code is 'services likely to be accessed by children'. But what about services used by parents, where they share their children's information? For example, Facebook, Medicare

- Obligations for quality information tie in to requirements for data minimisation and retention. You can meet data minimisation requirements while also ensuring accuracy – judicious approaches to data retention ultimately are good for accuracy. There will likely be some arguments around the obligation for 'completeness', important that this is not used to justify over-collection and data hoarding

- Health-related services have a particular need for up-to-date, good quality information. These include support apps, various acute services – thinking as well about particular needs of gender-diverse young people who may be misgendered if inaccurate information is held on them

- With regards to content recommended systems:
    - Some uses of out-of-date data can also harm children. Children may be retraumatised if apps re-target them with content when they are in recovery for example. But there are broader questions around children's best interests and targeting in general, beyond 'out of date' profiling data
    - Research tells us that young people appreciate moments of friction in their digital flows, as it reminds them what they are engaging with, and the limits of digital tech

2. **What might good look like for young people? What could the systems or practices be that keep young people's data up to date?**

- A rights-based approach enables us to weigh up the benefits of data collection and use versus the potential harms in a way that considers their best interests, and affords them a duty of care. A holistic approach is needed, rather than relying on single principles. Rights based approaches become complicated where they stray into paternalism, and children have to co-design what their best interests are

- Improving data quality for children requires consideration around:
    - The cadence of communication mechanism: Platforms will need to have regular points of communication with users to check if their information is up to date and correct. Children will need to be asked much more frequently because of the dynamic nature of their lives. Children need to be able to take charge of their information and its accuracy. This will need to be a different sort of approach based on the young person's age
    - Transparency around what data is held about children. Children should be given transparent access to their profiling info, so there is control about what assumptions have been made. This control should be given as children grow and change. But

handing responsibility over to businesses to make the decision of what is reasonable is part of the problem

- There is a need for clarity about definitions of personal information. It is difficult to imagine what quality standards can improve about information holdings without a clear picture on whether user profiling data for example is in scope of personal information definitions

- Beyond the scope of APP 10: There was also discussion about:
    - The validity of sensitive data collection for very young children (for example, those under 6 years old). In 'real life' scenarios, sensitive data about them is needed all the time (around allergies, disability etc). Discussions about online services and platforms collecting their data, and if these should be prohibited were held
    - The monetisation of younger children's personal data. Young children are going online and using platforms and making purchases, and this exposes them to data surveillance. This was described as another part of the problem, and an exploitation of people's lives

3. **Are there children and young people who may experience additional risks, or face heightened consequences, where this principle fails to be achieved? What regulatory safeguards, or additional considerations, might be necessary for them?**

- There are a range of young people who might experience particular risks from low quality data, including:
    - Children in out-of-home-care or those who don't have a significant adult who gives consistent guardianship, for whom much data exists and has the ability to determine significant decisions about their lives
    - Young people in the youth justice system, for whom much data exists and has the ability to determine significant decisions about their lives
    - Vulnerabilities are exacerbated by other systems of 'care' for whom data is equally important
    - Those experiencing or at risk of domestic or family violence, where information held about a child is out-of-date, particularly where it relates to abusive parents and their ability to consent
    - Homeless young people as well, who frequently change details and have unstable online access. Models from homelessness and youth-centric policy of 'online suitcases' for young people's information
    - For First Nations youth, if their indigenous status is not correct, it can lead to cultural erasure risks or cultural identity issues. Just as there needs to be strict parameters on the collection and use of sensitive information such as indigenous status information, there also need to be strict requirements for it to be accurate when it is used

- Age itself might also create particular vulnerabilities. Consideration needs to be given to the ages where it is appropriate for children to log in and correct data themselves. (And alongside age, other indicators of capacity). It may be developmentally appropriate for some ages to do so, and at other ages they may need support and clear processes to enable this. Consideration also needs to be given to the role of parents for when children aren't old enough to run these processes themselves

- There were also concerns that requirements for up-to-date, ‘complete’ data could be misused to create an expectation that platforms need more personal data in order to meet that threshold. There needs to be an interpretation in relation to the specific purposes in which the information is being collected

- Beyond the scope of APP10, there was also a discussion about different types of data. Specifically school information and photos, and sexting

APP 11: Security of children's personal information

Key insights

- Data minimisation and effective deletion are the best type of 'security'. Prohibitions on collecting and storing children's data in the first place, which exist in other jurisdictions, may provide the best form of security available
- Consideration needs to be given to the security measures platforms need, including enforceable guidelines and prescriptions for the purposes of reasonable steps within the Code
- Third-party access risks are particularly significant in a children's data context. Many companies have 'back door' security vulnerabilities, and the risks are exacerbated by poor auditing measures on security, as well as excessive pools of held information
- Children's information should have strict and automatic rules around deletion and destruction (for example, mandated expiry dates) given its sensitive nature
    - Beyond the scope of APP 11, there is a lively debate about ensuring young adults have a 'fresh start', and the potential of deleting children's public information when they turn 18 to extinguish the risks of historic and extensive digital data trails on their childhood

Discussion

The discussions around centred around three key prompts:

1. **What are the risks for young people when this principle is violated? What rights might this affect? Are there particular sorts of data that should warrant additional protections?**

    - There are significant risks that emerge from poor data security practices, including:
        - Data breaches and data 'leakages':
            - Vulnerabilities to malicious attacks by bad actors and hacking
            - Thinking specifically to the EdTech sector, and the masses of data those companies collect and the risks of significant data leakage. Particular vulnerabilities with third-party plug-ins, companies are generally unaware of how these are exploited by third-parties, giving rise to pretty serious APP 11 breaches
            - Other risks from third-party access can include SSOs, thinking about how requirements or regulations can create security risks by requiring SSOs to be used
        - Unauthorised access from abusive family members in a family violence situation can lead to serious harm, just like how family courts have to be extremely diligent about assessing FDV risks and information access, so do platforms

    - The consequences of this can be extensive:
        - More and more intimate forms of personal/sensitive information via image, video, voice-recording and the heightened risks of these being misused – considering how criminals, scammers, impersonation artists accessing this sort of data and using in scams
        - Data holdings containing sensitive information on young people which can make malicious use more damaging

- Beyond the scope of APP 11, the group also discussed:
    - Deidentification of data in general, and in research (Small sample sizes for research can mean easily identifiable data sets, and a lot of apps deidentify but connect in certain ways to enable reidentification)
    - Deliberate design and disaggregation of businesses (e.g. Disney) that links online gaming to gambling or wearable devices on an infant and implications for health insurance in future

2. **What would a 'reasonable step' be in this space? And beyond this, what might good look like for young people? What redress mechanisms or remedies should be available to them where this principle is violated?**

    - The implementation of stronger security measures by platforms:
        - Obligations for multi-factor authentication to tighten security and access to datasets, ensuring no unauthorised access in the first instance. Ringfencing datasets to expressly exclude certain users as well
        - Companies need higher security standards when they are handling children's personal information, as the risks are more acute

    - Third party access restrictions and onward data flows:
        - There are particular issues with managing third-party risks, supply chain issues in data sets and across integrated companies, security measures are a good way to ensure there is some sensible mitigations incorporated into processes that have been set up to encourage maximal aggregation
        - Commercial collection, trading, pooling, and disclosure of children's data creates serious security risks. It is likely commercial practices (provided the data is identifiable) will have serious APP 11 issues when it comes to children's data

    - Improved data retention and deletion practices:
        - Deletion and destruction requirements are vitally important, also considering issues around de-identification and re-identification
        - Need children to be able to exercise a right to delete their information - onus here is on the provider to make it really easy for the individual to do this. But this still presupposes the ability of the young person to do this, and their awareness of what information is collected and held on them

    - Improved data minimisation practices:
        - Prohibitions on collecting and storing children's data in the first place exist in other jurisdictions and should be looked at

    - Improved communication with young people:
        - Young people need to know what information has been collected on them for companies to be accountable to them under this APP, there should be transparency requirements (see APP 1) where organisations need to provide information to young people about the data collected on them and implications for holding/deleting it

    - Improved 'privacy by design':
        - For under 18s everything should be the highest privacy settings by default, that should also include really strict expectations for deletion and destruction for APP 11. Consider

in other jurisdictions where children's data cannot transfer across borders, strict storage rules

3. **Are there children and young people who may experience additional risks, or face heightened consequences, where this principle fails to be achieved? What regulatory safeguards, or additional considerations, might be necessary for them?**

- Children who are the most vulnerable offline are the most online, and more personal information will be circulating about them in general. For example;
    - Those in out-of-home or state care and those whose family have gone through the family law system
    - Children in the child protection system are at far higher risk of rights based violations, including child sexual abuse

  We often assume parents are protecting their children — especially around consent — but this is not always the case

- To meet the needs of these cohorts, all of the rules we're putting in place in the Code need to opt for the highest protection. The focus should be on what have we learned from how the most vulnerable children are impacted and we apply this protection for all

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

Key insights

- Access is dependent on awareness on what existing personal information is held. In reality in most circumstances there is no awareness and subsequently there is no access.The issue of access needs to be addressed as early as possible; ideally firstly at the point of initial collection and should be an ongoing process. Attention should then be given to making the process of providing access and seeking correction as efficient as possible
- Platforms need to have well-running systems and processes to make responding to requests more efficient and increasing knowledge and access of users. These must include clarity about timeframes and the periods in which information is retained and used
- Platforms need to have consistent and comprehensive data export processes, so children can easily access and download copies of their own data

Discussion

The discussions around centred around three key prompts:

1. **Can young people currently request data access and corrections with ease? What are the barriers? Why might this be important? What rights does it affect? Are there some sorts of data that should be more 'accessible' and 'correctable' than others?**

    - The group agreed that there is a lack of awareness of an ability to request data access, which creates a significant barrier for children in accessing their data. Most young people will not know what data is held, nor that they can request access to it
    - While general awareness of the right to request access to data might be low, it was not unheard of among young people. Some researchers present in this working group knew young people who were aware they could access their data, and on some apps request deletion. For these young people, their key concern was the speed at which these requests were actioned
    - To address this:
        - Ideally there should be multiple, clear touch points for children so they know what data is being collected about them and are constantly reminded of what the use and disclosure of this might be. This is also important as children progress and move through different capabilities and different priorities.
        - More clarity about the right to access and correct. Platforms need to try to make their processes more child friendly. Platforms need to be particularly mindful of fatigue users (of all ages) feel attempting to access their data

2. **What might good look like for young people? What would good processes that let them request access or correction to data look like? Are there examples from other fields we can reflect on? What could encourage data requests or corrections? What might discourage them?**

- This is a poorly known data right, and awareness raising is needed. More often, children are not aware of what data has been collected, is being used or is circulating about them. The entry step to better access to data, and the ability to correct data, is that children and young people (or their guardians) need to be aware of the existence of their information, and the mechanisms to access it

- A lack of awareness is not the same as a lack of interest:
  - Research was discussed that suggested that 79% of respondents said they would like to know what data is held about them, this is an issue about making access in an age appropriate matter
  - The group discussed google profiles as a 'type' of data about young people that they often felt irritated about when it was inaccurate. When young people look at their google profile, and it is inaccurate a lot of the time young people get frustrated. There is some agency over the algorithm the curate to make it personal (e.g. you can go incognito to avoid skewing algorithm), but this is not a systemic fix

- This is a question of agency and ownership. Access and correction enables some 'ownership' over their data

- The process of how children could access and correct data also matters:
  - Timelines matter, access and the data should be immediately available as much as possible
  - The simplicity of any process also matters, access to information needs to be meaningfully understandable. It needs to be able to be comprehensible (for example, described in clear language) and must be intelligible for children

- Access requests should not be predicated on the child proving a particular understanding or awareness of their information (some information access systems can take this more aggressive approach with applicants). As a child, you should not bear the onus to prove that you understand it, you should just be able to get access and your understanding is matched by the available explanation and presentation

- Larger platforms need to be held to higher standards in terms of ease and access. We considered some particular circumstances where children or young people might want to access their social media data for example. Some noted that young people leaving Twitter when it became X, wanted their archive and they wanted it in a format that they could access it and navigate it

3. **Are there children and young people who may experience additional risks, or face heightened consequences, where this principle fails to be achieved? What regulatory safeguards, or additional considerations, might be necessary for them?**

- Younger young children may be at a particular disadvantage when it comes to accessing or correcting data. The group explored the question of whether there should be an incentive to make data meaningfully available for younger children in particular (particularly those under 15). This age group, while widely recognised as having less agency and capacity than their older peers (for the purposes of entering agreements and transacting) still need to be included in access and correction measures

- Tangled data is an issue, where children are ‘co-using’ accounts with others, or they are joined with their parents. There need to be processes in place where children can pull their own data out for the purposes of access and correction

- Children of ‘influencer parents’, or children who have their childhoods broadcasted online by parents who are active on social media, may have particular concerns around their information. Some considerations included:
    - When and how they can access their own data, whether they had a role in the process (e.g. content publication) or not
    - The right to have information deleted, when you did not post it
    - Legislations coming in from a child influencer from a labour lens but then there is the representation of harm
    - Who consented to the use of that data, and whether it was the parent who was consenting on behalf of the child

- A range of technical solutions were described as options to create a good ‘data access’ process:
    - There could also be ‘quick release buttons’ to download data. Platforms could advertise these as a feature to give themselves a marketing edge around trust and privacy
    - Pop ups or chat bots could be an alternative
    - Beyond APP 12 & 13 technical solutions could also be used to remind young people that data collection is happening. Like the Cookies notifications, with clear accept or reject buttons, to help raise awareness about data processing in general