alannah & madeline foundation

Privacy Act Review: Report 2022

Response by the Alannah & Madeline Foundation

March 2023

Contents

Executive summary

We welcome the opportunity to respond to the *Privacy Act Review: Report 2022*. This report represents a crucial opportunity to make the Privacy Act and the related regulatory mechanisms fit for purpose in the contemporary era – an era when digital technologies are almost ubiquitous in the lives of Australian families and when individuals' personal information is handled on a vast scale within the digital economy.

As the report observes, the Privacy Act in its current form is almost silent on the topic of children's personal information. This is clearly inadequate for an era when the average Australian child owns more than three screen-based devices,[1] and when 8 out of 10 Australian teens use social media daily.[2] Despite the positives of digital technologies, children's wellbeing and rights have been threatened by the commercial model of many online services, which derive their profits from user engagement and handling of individuals' data.

This report represents an exciting opportunity to change the picture and uphold children's rights online.

Of the report's 116 proposals, we have chosen to respond to the 10 most pertinent to our work: proposals 5.1, 16.1, 16.2, 16.3, 16.4, 16.5, 20.5, 20.6, 20.7 and 30.1. See our Recommendations section.

More broadly, we believe the following approaches should be prioritised when updating the Privacy Act and associated mechanisms.

Firstly, regulation of online services should be led by trusted, expert public regulators, not by industry. These regulators must be adequately resourced to create (for example) a high-quality children's online privacy code in consultation with children and their families, ensure the code is brought to life in industry practice, track its progress, and investigate and address any serious or systemic breaches, including enforcement where necessary. This is no minor task; it must be resourced appropriately. Without a regulator who is truly able and equipped to lead this work, a children's code, however excellent, would soon lose its meaning.

Secondly, to appropriately protect children's personal information, we must place much stronger responsibility on online services to refrain from misusing children's data. We cannot continue to hold children and their parents individually responsible for avoiding harm online, while requiring them to 'consent' to extensive handling of their data as a condition of using online services.

Online services which are likely to be accessed by children should be required to treat the best interests of the child as a primary concern and to refrain from using children's personal information in ways shown to be harmful to children. We want to see a strong threshold of in-built protection for all children under the age of 18 – regardless of whether they (or their parents) have consented to the handling of their data.

A positive way forward would be through the creation of a children's online privacy code, as proposed in the report. This code should be informed by similar mechanisms adopted in the United Kingdom, Ireland, and other overseas jurisdictions. In particular, preliminary learnings are emerging from the United Kingdom about the impacts, strengths and limitations of their Age Appropriate Design Code. These learnings should inform Australia's approach.

More specifically, we support the report's proposals to prohibit trading in children's personal information, and to prohibit direct marketing to a child and targeting to a child unless it is in the child's best interests.

The 'best interests of the child' features prominently as a guiding principle for reform. We support this and would specify that the 'best interests of the child' should be defined clearly in line with the United Nations Convention on the Rights of the Child, including General Comment No.14. It should not be left to industry to define. As the 'best interests of the child' is a complex principle, expert guidance should be developed for industry, informed by experts such as the National Children's Commissioner and UNICEF.

Finally, when changes are made to the regulation of how online services may handle children's personal information, these changes should be evaluated to assess their progress and impacts.

About us

The Foundation was established the year after the Port Arthur tragedy, by Walter Mikac AM in memory of his two young daughters, Alannah and Madeline. Our vision is that all children and young people are safe, inspired and have freedom to flourish.

Over the last 25 years our work has grown and evolved but our purpose remains the same. We have three program streams:

- Safe and Strong: recovering and healing from trauma. Linked to our origin story, we have a specialist trauma recovery and therapy service for children who have experienced significant trauma. This has grown in recent years to include working with early childcare providers, kindergartens, and now primary schools to help them build their trauma informed capability and practices. Most of our work in trauma healing and recovery is Victorian based, with our therapists and consultants working from our client's homes and places of work.

- Safe and Strong: building positive digital citizens. The Foundation works with schools, families and communities nationally to help children build the digital intelligence, skills and competencies they need to stay safe online and to be active, positive digital citizens. With over 10 years' experience working in the cyber bullying and wellbeing space, as technology has become ubiquitous, our work has developed into building digital intelligence, digital ethics and media literacy for all children aged 3-18.

- Safe and Strong: bringing children's rights to life. As a rights-based organisation, this is our policy and advocacy work. Since inception, we have advocated for firearms safety, and we convene the Australian Gun Safety Alliance. In other key policy matters related to our programs, we work closely with the Office of the eSafety Commissioner, the Prime Minister's National Office for Child Safety and other major agencies such as the Australian Federal Police.

In 2018, we partnered with Kate and Tick Everett, after the tragic suicide of their daughter, Dolly. With them we worked to establish Dolly's Dream.

- Safe and Strong: Dolly's Dream, changing the culture of bullying. The purpose is the same, but the programs and services (Parent Hub, telephone help line, school, and community workshops etc.) are specifically designed for remote, rural, and regional families and communities, to meet their unique needs and contexts.

Recommendations

1. **Proposal 5.1 – Foundation response:** We believe Australian Privacy Principles (APP) codes relevant to the handling of children's personal information should not be developed by industry. Rather, they should be developed by an independent, expert, trusted public regulator. A children's online privacy code (or similar) should be informed by meaningful, age-appropriate consultation with children, young people, parents / caregivers, educators and civil society organisations with expertise in child-rights practice. We suggest a consultation period of at least 60 days, not the 40 proposed here.

   It is vital that the regulator is appropriately resourced to lead this work, given the significant and demanding nature of the work and the complex, challenging environment. If the Australian Government envisages a code for children that is comparable to the United Kingdom Age Appropriate Design Code, the public regulator overseeing it must be resourced to a level that would enable them to undertake work equivalent to that led by the United Kingdom's Information Commissioner's Office.

2. **Proposal 16.1 – Foundation response**: We support the proposal to amend the Privacy Act to include a definition of a child as an individual who has not yet reached 18 years of age.

3. **Proposal 16.2 – Foundation response**: We accept that the Privacy Act should codify the principle that valid consent for the handling of personal information must be given with capacity. However, we call for an overall move away from relying on consent models to protect children's data from misuse, and towards a model that provides all children under 18 with a high standard of data protection, through holding industry and government to higher standards of responsibility. (See Proposal 16.5) We also refer to the approach to consent taken in Ireland's Fundamentals for a Child-Oriented Approach to Data Processing, especially the premise that 'Consent doesn't change childhood'.

4. **Proposal 16.3 – Foundation response**: We support the proposal to amend the Privacy Act to require that collection notices and privacy policies are clear and understandable, in particular any information addressed specifically to a child. We would add that published terms should also be honest, accessible to different literacy levels, and developed through meaningful consultation with children themselves. This approach should apply not only to published terms addressed specifically to children, but also to published terms of any online service likely to be used by children.

5. **Proposal 16.4 – Foundation response**: We support the proposal that entities be required to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances. We urge that 'the best interests of the child' be defined in line with the United Nations Convention on the Rights of the Child and its General Comments 14 and 25 – not left to industry to define. As 'the best interests of the child' is a complex concept, we encourage the development of guidance and indicators for policymakers and industry, with appropriate resources set aside to support this. We recommend involving the National Children's Commissioner and UNICEF.*

6. **Proposal 16.5 – Foundation response**: We support the proposal to create a Children's Online Privacy Code. Specifically:

   - The code should apply to online services that are likely to be accessed by children – not just child-specific services.
   - The code should be developed through consultation with children, parents / carers and experts in child rights practice. The United Kingdom's Information Commissioner's Office released a report of their consultations which shaped the Age Appropriate Design Code; this report provides useful learnings, including about the limitations and challenges of such consultations.†
   - The code development process should engage meaningfully with the online safety expertise of the eSafety Commissioner, especially eSafety's work on 'safety by design'.
   - The code development process should be informed by comparable models developed overseas and by common themes identified across them – see reflections by 5Rights Foundation.‡
   - In particular, the code development process should be informed by reflections from the UK's experience of implementing the Age Appropriate Design Code – see our chapter on proposal 16.5.
   - Attached to the code should be mechanisms to track its implementation and address any serious or systemic failures to comply. A certification scheme for digital providers or independent audit process might be explored. This substantial undertaking would require appropriate resourcing.
   - In line with the United Nations Convention on the Rights of the Child, General Comment No.25, the code should make providers of preventative or counselling services to children exempt from

* See for example UNICEF, 'The case for better governance of children's data: a manifesto,' 2021, https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf

† UK Information Commissioner's Office, 'Towards a better digital future: Informing the Age Appropriate Design Code,' 2019 https://ico.org.uk/media/about-the-ico/consultations/2614763/ico-rr-report-0703.pdf

‡ 5Rights Foundation, 'Approaches to children's data protection - a comparative international mapping', 2022, https://5rightsfoundation.com/in-action/approaches-to-childrens-data-protection-a-comparative-international-mapping.html

any requirement to obtain parental consent in order to access such services. Such services should be held to high standards of privacy and child protection.

7. **Proposal 20.5 – Foundation response**: We would support a prohibition of direct marketing to a child unless it is in the child's best interests. We urge that the definition of the 'best interests of the child' be rooted in the United Nations Convention on the Rights of the Child and not left to industry to define. We also note the recommendation of a report commissioned by the Office of the Australian Information Commissioner in 2020: that a children's privacy code should establish a presumption that profiling of children for advertising or other commercial purposes is not fair or reasonable.

8. **Proposal 20.6 – Foundation response**: We would support a prohibition of targeting to a child unless it is in the child's best interests (as above).

9. **Proposal 20.7 – Foundation response:** We would support a prohibition of trading in the personal information of children. We note the recommendation of a report commissioned by the Office of the Australian Information Commissioner in 2020: that children's data must not be disclosed except as necessary to provide the elements of the service in which the child is actively and knowingly engaged, or as required by law or for a defined public interest.

10. **Proposal 30.1 – Foundation response:** We would welcome a review of any amendments to the Privacy Act. Specifically, we call for appropriate resources to be allocated to assess the progress and community impacts of any code developed to address the handling of children's personal information.

Background

This report of the review of the Privacy Act has arrived at an important time, when digital technologies have become almost ubiquitous in the lives of Australian families. We believe legislation and regulation must evolve to better uphold children's rights online, including the handling of their personal information.

Australian children use digital technologies frequently from a young age. In 2021, the average school-aged child owned three personal screen-based devices,[3] while 80% of 16-17 year olds used social media almost every day.[4] While digital technologies can be used positively for learning, social connection and entertainment, the digital world was not designed to uphold children's rights, and many children have had negative experiences online.

Australia's Online Safety Act 2021 represented a major step forward in legislating to address complaints of serious cyber bullying, image-based abuse, illegal content and adult content. It provided for the determination of basic online safety expectations (with online services required to report on their compliance with these) and for the creation of codes by industry leaders to address their handling of issues like illegal and restricted material. Meanwhile, certain egregious online behaviours such as image-based abuse, severe cyber bullying and child sexual exploitation are covered under state and federal criminal codes.

However, if we use the '4Cs classification' of online risks for children – content, contact, conduct and contract[5] – it seems the above laws focus mainly on the most serious concerns regarding content and conduct. Contact and contract risks receive less attention. Nor does Australia have requirements in place, to a level equivalent to the United Kingdom and some other overseas jurisdictions, that digital providers will consider the best interests of the child and refrain from using children's data in ways shown to cause harm to children.

Many digital products and services were designed to maximise user engagement and handling of individuals' data, with platforms collecting vast amounts of information about individuals with broad discretion as to how they use it.[6] Commercial priorities shape digital products and services at a design level.

Digital technologies were not intended to cause harm to children. But they have helped to facilitate it, however inadvertently, by prioritising commercial gain ahead of children's rights. The traditional design of many digital products and services has increased children's risk of negative experiences, including loss of control over personal information; excessive spending; exposure to age-inappropriate material; contact with undesirable individuals; and dysregulated and anti-social uses of technology.[7]

Inappropriate handling of children's personal information by digital platforms could be seen as increasing the risk that children's rights will be violated, especially:

- Article 16 (United Nations Convention on the Rights of the Child): 'No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.'

- Article 34: 'States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse.'

- Article 36: 'States Parties shall protect the child against all other forms of exploitation prejudicial to any aspects of the child's welfare.'

Proposal 5.1

'5.1 Amend the Act to give power to the Information Commissioner to make an APP [Australian Privacy Principles] code[§] where the Attorney-General has directed or approved that a code should be made:

- *where it is in the public interest for a code to be developed, and*
- *where there is unlikely to be an appropriate industry representative to develop the code.*

In developing an APP code, the Information Commissioner would:

- *be required to make the APP Code available for public consultation for at least 40 days, and*
- *be able to consult any person he or she considers appropriate and to consider the matters specified in any relevant guidelines at any stage of the code development process.'*

The report adds *'If implemented, this proposal could be used for the selection of a code developer in the children's privacy context.'* (p.156)

We welcome the proposed change. We believe codes which address the handling of children's personal information should be developed by an independent, expert, trusted public regulator who is accountable to the Australian people and who has a remit to engage the community on this matter.

Under the Privacy Act in its current form, the Information Commissioner is primarily responsible for identifying a code developer and registering codes put forward by that developer. The Information Commissioner is only permitted to create a code if a code developer was requested to do so and did not comply or if the Commissioner decides not to register a code which was developed. A change in favour of greater leadership by a public regulator would be welcome.

Public leadership seems more likely to result in children's rights being upheld, in comparison to industry-led models of self-regulation or co-regulation. Historically, the design of many digital products and services has had the effect of putting children's privacy, safety and wellbeing at risk.[8] Of course, digital platforms did not intend to cause harm to children, and some have taken positive steps for their younger users recently. However, regulatory regimes led by industry seem unlikely to have the confidence of the wider community.

[§] APP (Australian Privacy Principles) codes provide clarity about various issues relating to the handling of individuals' personal information.

We note the analysis of online safety codes in various jurisdictions conducted by Reset Australia and ChildFund Australia, who found that codes drafted and led by regulators and legislators included higher standards of protection for children's rights than codes which were drafted by industry.[9]

Proposal 5.1 also proposes a 40-day public consultation period to inform the development of APP codes. We do not believe a 40-day period is likely to be sufficient to inform the development of a privacy code for children. Many stakeholders – children, young people, parents, caregivers, educators, and civil society organisations – have limited time and resources to engage with formal consultations. If a time period is to be specified, we suggest one of at least 60 days, with appropriate resources allocated to engage children and above-mentioned adults in meaningful, age-appropriate ways.

This points, in turn, to the importance of ensuring public regulators have capacity to meet the demands of their roles. In this instance, regulators must work with large international digital platforms with immense wealth and lobbying power, knowing that regulations introduced in one jurisdiction can influence others – see the influence of the United Kingdom Age Appropriate Design Code on a similar code developed in California. The pressures faced by the regulator are likely to be very significant.

Proposal 16.5 implies that the United Kingdom Age Appropriate Design Code could be a model for an Australian code. We would support that approach, but we note that the United Kingdom's Information Commissioner's Office is better funded than most of its international equivalents, including those in Australia.[10] If our final product is to be comparable to the Age Appropriate Design Code, it will need a comparable level of resourcing.

In their manifesto for the better governance of children's data, UNICEF stress the importance of allocating sufficient financial and human resources to ensure that data protection authorities have expertise in children's rights and that children's rights are incorporated into data governance regimes. 'In order to be effective, DPAs (Data Protection Authorities) must have the capacity to litigate, impose fines and other sanctions on lawbreakers, and a mandate to provide remedies to children whose rights have been breached.'[11]

Similarly, the Consumer Policy Research Centre said of digital products and services: 'For legislation to be effective, it needs to be supported by regular surveillance and enforcement by the regulator to educate and shift the market towards a more consumer-centric approach to the digital economy. Australia needs a well-resourced regulator with the capacity and capability to audit and enforce breaches in the complex digital environment.'[12]

Proposal 16.1

'16.1 Define a child as an individual who has not reached 18 years of age.'

The Privacy Act in its current form provides no clear definition of who is a child for the purposes of the Act.

We support the approach proposed of defining a child as a person below the age of 18, in line with the United Nations Convention on the Rights of the Child (Article 1) and the Online Safety Act (2021).

Proposal 16.2

'16.2 Existing OAIC [Office of the Australian Information Commissioner] guidance on children and young people and capacity should continue to be relied upon by APP entities.

'An entity must decide if an individual under the age of 18 has the capacity to consent on a case-by-case basis. If that is not practical, an entity may assume an individual over the age of 15 has capacity, unless there is something to suggest otherwise.

'The Act should codify the principle that valid consent must be given with capacity. Such a provision could state that 'the consent of an individual is only valid if it is reasonable to expect that an individual to whom the APP entity's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.'

'Exceptions should be provided for circumstances where parent or guardian involvement could be harmful to the child or otherwise contrary their interests (including, but not limited to confidential healthcare advice, domestic violence, mental health, drug and alcohol, homelessness or other child support and community services).'

We accept that the Privacy Act should codify the principle that valid consent must be given with capacity. And we see the value of this framing concerning OAIC guidance, exceptions to parental consent, and assuming that individuals over 15 have capacity to consent to their data being handled.

However, we call for a move away from the 'notice and consent' approach to handling children's data, which has proven inadequate for upholding the best interests of the child. Historically, the digital industry has too often required people to agree to their data being used in ways they may not like – or even understand – as a pre-condition for participating in the online world.[13] This approach is especially unacceptable when applied to children. Parental consent raises the bar of protection only slightly, as parents may not understand the conditions of online services and these conditions may remain detrimental to children.[14]

The OAIC provides high-quality guidance. However, public regulators do not necessarily have the resources to ensure their advice is 'relied upon'. The OAIC's guidance on 'Children and young people' gives 15 as the age limit at which an individual may be assumed to have capacity to consent to the handling of their personal information, in situations where a case-by-case assessment of capacity is not practical.[15] However, the current design of many social media and gaming platforms – which permit anyone aged 13 or over to open an account and have their data handled[16] – suggests OAIC guidance is not followed closely by industry.

We would like to see the digital world move towards an approach which treats the best interest of the child as a primary concern, and which does not use children's personal information in ways shown to be harmful to them – and which extends this approach to all children under 18, regardless of whether consent for data handling has been given.

Such an approach seems to be embodied in Proposal 16.5, which we welcome.

We also point to the approach to consent outlined in Ireland's Fundamentals for a Child-Oriented Approach to Data Processing. In particular, they specify 'consent doesn't change childhood' – obtained from children or from the guardians / parents should not be used as a justification to treat children of all ages as if they were adults.[17]

Proposal 16.3

'16.3 Amend the Privacy Act to require that collection notices and privacy policies be clear and understandable, in particular for any information addressed specifically to a child.

'In the context of online services, these requirements should be further specified in a Children's Online Privacy Code, which should provide guidance on the format, timing and readability of collection notices and privacy policies.'

We support this proposal. However, we would add that published terms of online services should not only be clear and understandable, but also honest, accessible to children with different levels of literacy, and developed through meaningful consultation with children themselves.

This approach should be present not only in published terms addressed specifically to children, but in the published terms of any online service likely to be used by children.

We refer to the fourth standard ('Transparency') of the United Kingdom Age Appropriate Design Code for a respected approach, which includes guidance about tailoring information to children of different ages.

Proposal 16.4

'16.4 Require entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances.'

This is a welcome proposal. We urge that the definition of the best interests of the child be rooted in the United Nations Convention on the Rights of the Child and its General Comments 14 and 25, not left to industry to define.

The concept of 'the best interests of the child' aims to ensure the full and effective enjoyment by children of all of their rights, as well as the holistic development of the child. Treating it as 'a primary consideration' means decision-makers recognise the particular vulnerabilities of children and the need to give high priority to children's best interests, not treating them as equivalent to all other concerns.[18]

According to General Comment 14 ('On the right of the child to have his or her best interests taken as a primary consideration'), children have the right to have their best interests assessed and taken into account as a primary consideration in all actions or decisions that concern them, both in the public and private sphere.[19]

According to General Comment 25 ('On children's rights in relation to the digital environment'), 'States parties should ensure that, in all actions regarding the provision, regulation, design, management and use of the digital environment, the best interests of every child is a primary consideration.'[20]

A process to determine the best interests of the child is expected to take the following elements into account (as relevant to the situation): the child's views; the child's identity; preservation of the family environment and maintaining relations; care, protection and safety of the child; situation of vulnerability; the child's right to health; and the child's right to education.

Where different rights, or rights of different individuals, are in tension, they should be weighed against each other and careful effort made to find a balanced solution. 'The best interests of the child' is recognised as a dynamic concept, requiring approaches which are flexible and responsive to context.[21]

Given these complexities, online services may well need expert guidance in this space.[22] We encourage involving the National Children's Commissioner in the creation of such guidance.

We also refer to UNICEF's manifesto for the better governance of children's data, which posits that basic requirements in relation to children's best interests should include the following.

- Governments and companies should ascertain the impact on children of their data collection, processing and storage practices.
- Best interests need to have greater strength and validity than any other established legal basis for data processing activities.
- Children's data should not be processed in ways that are shown to be detrimental to them.
- In all products and services used by children it is important to: limit biometrics collection; prevent the economic exploitation of children's vulnerability for marketing purposes; and to restrict profiling that could lead to behaviour modulation or discrimination.
- Data should not be used to power algorithms that interfere with children's rights to autonomy and self-determination.[23]

Proposal 16.5

'16.5 Introduce a Children's Online Privacy Code that applies to online services that are "likely to be accessed by children". To the extent possible, the scope of an Australian children's online privacy code could align with the scope of the United Kingdom Age Appropriate Design Code, including its exemptions for certain entities including preventative or counselling services.

'The code developer should be required to consult broadly with children, parents, child development experts, child-welfare advocates and industry in developing the Code. The eSafety Commissioner should also be consulted.

'The substantive requirements of the Code could address how the best interests of child users should be supported in the design of an online service, including:

- *whether, in the context of online services that are likely to be accessed by children, specific requirements are needed for assessing capacity*
- *whether certain collections, uses and disclosures of children's personal information should be limited*
- *which default privacy settings should be in place for children that use online services*
- *whether entities should be required to 'establish age with a level of certainty that is appropriate to the risks' or apply the standards in the Children's Code to all users instead*
- *how privacy information (including collection notices and privacy policies) and tools that enable children to exercise privacy rights (including erasure requests) should be designed to improve accessibility for children, and*
- *if parental controls are provided, how to balance the protection of the child with a child's right to autonomy and privacy from their parents in certain circumstances.'*

We would welcome the development of a code to address the handling of children's personal information by online services. This would be an important step forward in ensuring that children can enjoy the benefits of the digital world while their rights are upheld.

Progress has been observed since the introduction of the United Kingdom Age Appropriate Design Code in 2020. Since then, several online services have taken positive steps such as blocking targeted and personalised ads for children; setting children's accounts to private by default; blocking adults from direct messaging children; turning notifications off at bedtime; improving parental supervision tools; introducing prompts encouraging children to take a break from scrolling; and turning off autoplay on video sites.[24]

In line with Proposal 16.5, such a code should encompass all online services likely to be accessed by children. Many children use online services not aimed specifically at them, sometimes contrary to terms of service. For example, a 2020 survey of a nationally representative sample of 1,034 children aged 9-12 in the United States found that in the previous year two-thirds of the children had used YouTube, almost one-third had played Fortnite, almost 3 in 10 had used TikTok, and more than 1 in 6 had used Instagram and/or Snapchat.[25]

We would also stress – and this seems to align with Proposal 16.5 – that a children's code should not reduce children's access to high-quality, age-appropriate support services like online counselling. We refer to the United Nations Convention on the Rights of the Child, General Comment No.25, which states that providers of preventive or counselling services to children in the digital environment should be exempt from any requirement for a child to obtain parental consent in order to access such services – and also that such services should be held to high standards of privacy and child protection.[26]

Proposal 16.5 makes the welcome statement that a code developer should be required to consult broadly with children, parents and a range of experts. We agree, and, as an example, point to the consultations that informed the United Kingdom Age Appropriate Design Code. Those consultations used a mixed methods approach, with a combination of qualitative and quantitative work, to hear from hundreds of children and adults in different locations via focus groups, interviews and surveys. The findings proved highly beneficial,

while also identifying risks and limitations in consulting with children, from which an Australian code developer could learn.[27]

Of course, research into children's experiences online has already been conducted for the eSafety Commissioner. In light of this and other work by eSafety – eg. the Safety by Design project and the negotiation of industry codes under the Online Safety Act – we worry the wording of Proposal 16.5 that eSafety should be 'consulted' is too perfunctory. eSafety's expertise in online safety should is vital here.

Proposal 16.5 lists a number of topics to be addressed by the proposed code. We agree that a code should cover those topics. We also point to an analysis by the not-for-profit charity 5Rights Foundation, which advocates for the rights of children in the digital world. 5Rights analysed respected legislative and policy initiatives about children's data protection from different jurisdictions and identified their common principles:

- Children are defined as anyone under the age of 18.
- The best interests of the child should be the primary consideration whenever children's data is handled.
- Children's data should not be used in ways shown to be detrimental to children's wellbeing.
- Data protection impact assessments are required and should particularly assess risks to children that arise from the handling of their data.
- Privacy / safety settings should be set to 'high' by default for products and services used by children, unless there is a compelling reason to do otherwise guided by the best interests of the child.
- Age assurance mechanisms should function to help protect children's rights and should be proportionate to the nature and risk of the data processing activities.
- Communication with children should be clear, concise, accurate and accessible.
- Parental controls should supplement safety-by-design, not replace it, and children should be told how and when parental controls are being used.[28]

Proposal 16.5 suggests an Australian code could align in scope as much as possible with the scope of the United Kingdom Age Appropriate Design Code. We believe the United Nations Age Appropriate Design Code is a strong model, but we trust a code developer would also engage with models in other jurisdictions. Ireland's Fundamentals for a Child Oriented Approach to Data Processing, in particular, is highly regarded.

Moreover, we trust that an Australian code developer would learn from the preliminary lessons emerging since the United Kingdom Age Appropriate Design Code was introduced in 2020. From a rapid scope of reflections available publicly, we submit that the United Kingdom's experience suggests a meaningful children's code needs the following elements in place:

- Sufficient resourcing for an independent supervisory authority (in the United Kingdom, the Information Commissioner's Office) to monitor industry's conformance with the code and address any violations. For example, the Information Commissioner's Office has examined how dozens of online services are conforming and has conducted several audits and ongoing investigations.[29]

- A clear legislative context. The United Kingdom Age Appropriate Design Code is rooted in the Data Protection Act 2018, the General Data Protection Regulations, and the Privacy and Electronic Communications Regulations 2003.[30]

- A clear basis in the United Nations Convention on the Rights of the Child, including alignment with the Convention's definition of the 'best interests of the child'.[31]

- Detailed explanations, guidance and examples provided for each standard in the code.[32]

- Detailed scoping undertaken ahead of time. For example, the Information Commissioner's Office released estimated costings for compliance and what this would add up to per affected child.[33]

- A 'regulatory sandbox' where companies can test products with regulators' support in a confidential environment.[34]

- Further stakeholder consultation and a policy position on the sensitive topic of age assurance, with a focus on upholding children's rights and leveraging 'privacy by design'.[35]

- Constructive relationships with civil society experts. 5Rights Foundation has provided detailed feedback to the Information Commissioner's Office about strengths and systemic breaches in the implementation of the United Kingdom Age Appropriate Design Code.[36]

- Clear exceptions to the principle of data minimisation if an online service demonstrates a compelling reason to do otherwise in the best interests of the child – eg. sharing data for safeguarding purposes to prevent sexual exploitation and abuse online and to prevent/detect crimes against children like online grooming.[37]

Unfortunately, the United Kingdom's experience has also shown that conformance with the code has been uneven. Various online services continue to show problems, including age-inappropriate recommender systems; 'dark patterns' and 'nudge' techniques; adult-only services being accessed by children; failures by platforms to enforce their own community standards; low default privacy settings; age-inappropriate financial messaging (e.g. in-game purchases); excessive data sharing with third parties; published terms that are confusing to children; and advertising on app stores that misrepresents the safe age of use for an app or game.[38]

These ongoing concerns show the importance of investing in monitoring and compliance mechanisms. Mechanisms might potentially include a voluntary certification scheme for digital providers (see the United Kingdom's certification scheme under the United Kingdom's General Data Protection Regulation)[39] or an independent audit process incorporated into the code.

Proposals 20.5, 20.6 and 20.7

'20.5 Prohibit direct marketing to a child unless the personal information used for the direct marketing was collected directly from the child and the direct marketing is in the child's best interests.'

'20.6 Prohibit targeting to a child, with an exception for targeting that is in the child's best interests.'

'20.7 Prohibit trading in the personal information of children.'

We support these proposals. Again, we trust the definition of the 'best interests of the child' will be rooted in the United Nations Convention on the Rights of the Child.

We are led by General Comment No.25 of the Convention, which observes 'States parties should make the best interests of the child a primary consideration when regulating advertising and marketing addressed to and accessible to children.' (para 41).

General Comment No.25 specifies the need to prohibit profiling or targeting of children for commercial purposes on the basis of a digital record of their actual or inferred characteristics (para 42), and the need to regulate targeted or age-inappropriate advertising and marketing to prevent children's exposure to promotion of unhealthy products, in line with regulations in the offline world (para 97).[40]

Also valuable are the recommendations made by Assoc. Prof. Normann Witzleb and Prof. Moira Paterson (Faculty of Law, Monash University) in a report commissioned by the Office of the Information Commissioner: that a children's privacy code should establish a presumption that profiling of children for advertising or other commercial purposes is not fair or reasonable; and that children's data must not be disclosed except as necessary to provide the elements of the service in which the child is actively and knowingly engaged, or as required by law or for a defined public interest.[41]

Proposal 30.1

'30.1 Conduct a statutory review of any amendments to the Act which implement the proposals in this Report within three years of the date of commencement of those amendments.'

We would welcome a review. Specifically, we call for appropriate resources to be allocated to assess the progress and impacts of any children's online privacy code.

We would hope that any such evaluation would address the impacts of a code on the community, especially children, through consideration of issues such as:

- the evolving context of children's lives online
- changes made to digital products and services since the introduction of the code
- any areas of non-compliance
- any areas of concern not covered by the code
- any influence of the code on overseas jurisdictions.

We are given to understand that initial evaluation processes have been conducted in relation to the United Kingdom Age Appropriate Design Code, although findings do not seem to have been published yet.

Evaluations should include meaningful, age-appropriate engagement with children, young people, parents/carers, educators and civil society.

We would welcome the opportunity to discuss any of these matters further. Please contact:

Sarah Davies AM, CEO
sarah.davies@amf.org.au

Ariana Kurzeme, Director, Policy & Prevention
ariana.kurzeme@amf.org.au

Dr Jessie Mitchell, Manager, Advocacy
jessie.mitchell@amf.org.au

[1] A. Graham and P. Sahlberg, 'Growing Up Digital Australia: Phase 2 technical report,' Gonski Institute for Education, UNSW, Sydney, 2021, https://www.gie.unsw.edu.au/growing-digital-australia-phase-2-results
[2] P. Rioseco and S. Vassallo, 'Adolescents online (Growing Up in Australia Snapshot Series – Issue 5)', Melbourne, Australian Institute of Family Studies, 2021, https://growingupinaustralia.gov.au/research-findings/snapshots/adolescents-online
[3] Graham and Sahlberg, 'Growing Up Digital Australia: Phase 2 technical report'
[4] Rioseco and Vassallo, 'Adolescents online (Growing Up in Australia Snapshot Series – Issue 5)'
[5] S. Livingstone and M. Stoilova, M, 'The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics), Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online Research and Evidence, 2021, https://doi.org/10.21241/ssoar.71817
[6] Australian Competition and Consumer Commission (ACCC), 'Digital Platforms Inquiry: final report', June 2019, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf
[7] Examples of these concerns are outlined in documents including: 5Rights Foundation, 'Risky By Design', https://www.riskyby.design/ ; Tiffani Apps, Karley Beckman, Sarah K. Howard, 'Edtech is treating students like products. Here's how we can protect children's digital rights,' *The Conversation*, 10 June 2022, https://theconversation.com/edtech-is-treating-students-like-products-heres-how-we-can-protect-childrens-digital-rights-184312 ; ACCC, 'Digital Platforms Inquiry: final report'; Consumer Policy Research Centre, 'Duped by design: Manipulative online design: Dark patterns in Australia,' 2022, https://cprc.org.au/dupedbydesign/ ; Consumer Policy Research Centre, 'Submission to the ACCC on the Digital Platform Services Inquiry on updating consumer law for digital platform services – Discussion Paper,' 13 April 2022, https://cprc.org.au/wp-content/uploads/2022/04/CPRC-Submission-ACCC-Digital-Platforms-Inquiry-Discussion-Paper-Digital-Platform-Services-April-2022-1.pdf ; Agatha Court, Bill Browne, 'Devil in the detail: privacy and some popular digital platforms,' Australia Institute, Centre for Responsible Technology, 2020; eSafety, 'Recommender systems and algorithms: position statement,' 2022, https://www.esafety.gov.au/industry/tech-trends-and-challenges ; Essential Research (prepared for the Australia Institute), 'The Essential Report: Data Attitudes,' 2019, https://australiainstitute.org.au/wp-content/uploads/2020/12/Essential-Report-tech.pdf; Alison Hung, 'Keeping consumers in the dark: addressing "nagging" concerns and injury,' *Columbia Law Review*, vol.121, issue 8, Dec 2021; Eric Osika, 'The negative effects of new screens on the cognitive functions of young children require new recommendations,' *Italian Journal of Pediatrics*, vol.47, 2021; Jenny Radesky, MD; Alexis Hiniker, PhD; Caroline McLaren, BS; Eliz Akgun, BA; Alexandria Schaller, BA; Heidi M. Weeks, PhD; Scott Campbell, PhD; Ashley N. Gearhardt, PhD, 'Prevalence and Characteristics of Manipulative Design in Mobile Applications Used by Children,' *JAMA Network Open*, 5(6), 2022
[8] 5Rights Foundation, 'Disrupted Childhood: The cost of persuasive design,' June 2018 https://5rightsfoundation.com/uploads/5rights-disrupted-childhood-digital-version.pdf; 5Rights Foundation, 'Pathways: How digital design puts children at risk,' July 2021, https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf
[9] Dr Rys Farthing, Reset Australia & ChildFund Australia, 'How outdated approaches to regulation harm children and young people and why Australia urgently needs to pivot', Dec 2022, https://au.reset.tech/uploads/report_-co-regulation-fails-young-people-final-151222.pdf
[10] Centre of Excellence for the Digital Child, 'New partnership tackles children's privacy and digital rights,' 7 July 2022, https://www.digitalchild.org.au/news/new-partnership-tackles-childrens-privacy-and-digital-rights/
[11] UNICEF, 'The case for better governance of children's data: a manifesto,' 2021, https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf
[12] Consumer Policy Research Centre, 'Duped by design: Manipulative online design'
[13] See for example ACCC, 'Digital Platforms Inquiry: final report'; Consumer Policy Research Centre, 'Submission to the ACCC on the Digital Platform Services Inquiry'
[14] Lisa Archbold, Moira Paterson, Normann Witzleb, 'Adtech and children's rights,' *University of New South Wales Law Journal*, September 2021
[15] Office of the Australian Information Commissioner (OAIC), 'Children and young people,' https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/children-and-young-people
[16] eSafety, 'The eSafety Guide,' https://www.esafety.gov.au/key-issues/esafety-guide

[17] Data Protection Commission, Ireland, 'Fundamentals for a Child-Oriented Approach to Data Processing,' 2021, https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf
[18] United Nations Convention on the Rights of the Child, 'General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration,' 2013 https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=5&DocTypeID=11
[19] United Nations Convention on the Rights of the Child, 'General comment No. 14'
[20] United Nations Convention on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment,' 2021, https://www.ohchr.org/en/treaty-bodies/crc/general-comments
[21] United Nations Convention on the Rights of the Child, 'General comment No. 14'
[22] Dr Jonathan Collinson, Jen Persson, 'What Does The 'Best Interests of the Child' Mean for Protecting Children's Digital Rights? A narrative literature review in the context of the ICO's Age Appropriate Design Code,' *Communications Law*, 27(3), 2022 https://eprints.whiterose.ac.uk/194985/3/Communications%20Law%20-%20BIC%20in%20digital%20rights%20-%20Revisions%2028-2-22.pdf
[23] UNICEF, 'The case for better governance of children's data: a manifesto'
[24] 5Rights Foundation, '5Rights has reflected on the 1 year anniversary of the introduction of the Age Appropriate Design Code,' 2022, https://5rightsfoundation.com/in-action/5rights-celebrates-the-first-anniversary-of-the-age-appropriate-design-code.html; 5Rights Foundation, 'Approaches to children's data protection - a comparative international mapping,' October 2022, https://5rightsfoundation.com/Approaches-to-Childrens-Data-Protection---.pdf; UK Information Commissioner, '"Children are better protected online in 2022 than they were in 2021" - ICO marks anniversary of Children's code', 2022, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/children-are-better-protected-online-in-2022-than-they-were-in-2021/
[25] Justin W. Patchin, 'Tween Social Media and Gaming in 2020,' 14 October 2020, https://cyberbullying.org/tween-social-media-and-gaming-2020
[26] United Nations Convention on the Rights of the Child, 'General comment No. 25'
[27] ICO, 'Towards a better digital future : Informing the Age Appropriate Design Code,' 2019, https://ico.org.uk/media/about-the-ico/consultations/2614763/ico-rr-report-0703.pdf
[28] 5Rights Foundation, 'Approaches to children's data protection - a comparative international mapping'
[29] ICO, 'Letter to 5Rights Foundation in response to the charity's research into systemic breaches of the Age Appropriate Design Code (Children's code),' 17 Nov 2021, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/11/letter-to-5rights-foundation/ ; Future of Privacy Forum, 'Policy Brief: Comparing the UK and California Age Appropriate Design Codes,' Dec 2022, https://fpf.org/wp-content/uploads/2022/11/FPF-Comparative-Analysis-of-CA-UK-Codes-of-Conduct-R3.pdf; Martyn Landi, 'Children 'safer online now than a year ago because of safety code', Press Association, London 1 Sep 2022
[30] Centre of Excellence for the Digital Child, 'New partnership tackles children's privacy and digital rights'; Information Commissioner's Office, 'Age Appropriate Design Code: Impact Assessment,' 3/7/2020 https://ico.org.uk/media/about-the-ico/documents/2617988/aadc-impact-assessment-v1_3.pdf
[31] Centre of Excellence for the Digital Child, 'New partnership tackles children's privacy and digital rights'; Future of Privacy Forum, 'Policy Brief: Comparing the UK and California Age Appropriate Design Codes'
[32] Future of Privacy Forum, 'Policy Brief: Comparing the UK and California Age Appropriate Design Codes'
[33] 5Rights Foundation, 'Baroness Beeban Kidron, Chair, 5Rights, response to the ICO's opinion on Age Assurance for the Children's Code,' Oct 2022, https://5rightsfoundation.com/in-action/baroness-beeban-kidron-chair-5rights-response-to-the-icos-opinion-on-age-assurance-for-the-childrens-code.html ; Information Commissioner's Office, 'Age Appropriate Design Code: Impact Assessment'
[34] Centre of Excellence for the Digital Child, 'New partnership tackles children's privacy and digital rights'
[35] ICO, 'Letter to 5Rights Foundation in response to the charity's research into systemic breaches of the Age-Appropriate Design Code (Children's code),' 17 Nov 2021, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/11/letter-to-5rights-foundation/; Future of Privacy Forum, 'Policy Brief: Comparing the UK and California Age Appropriate Design Codes'
[36] 5Rights Foundation, '5Rights has reflected on the 1 year anniversary of the introduction of the Age Appropriate Design Code'
[37] Future of Privacy Forum, 'Policy Brief: Comparing the UK and California Age Appropriate Design Codes'

[38] 5Rights Foundation, 'Letter to the ICO: Breaches of the Age Appropriate Design Code,' Oct 2022, https://5rightsfoundation.com/in-action/letter-to-the-ico-breaches-of-the-age-appropriate-design-code.html; UK Information Commissioner, '"Children are better protected online in 2022 than they were in 2021" - ICO marks anniversary of Children's code'; Virginia N. L. Franqueira, Jessica A. Annor, Ozgur Kafali, 'Age Appropriate Design: Assessment of TikTok, Twitch, and YouTube Kids', *Psychology*, Aug 2022, https://www.researchgate.net/publication/362489352_Age_Appropriate_Design_Assessment_of_TikTok_Twitch_and_YouTube_Kids

[39] Information Commissioner's Office, 'Certification,' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/certification/

[40] United Nations Convention on the Rights of the Child, 'General comment No. 25'

[41] Assoc. Prof. Normann Witzleb and Prof. Moira Paterson, Faculty of Law, Monash University, 'Privacy risks and harms for children and other vulnerable groups in the online environment,' Research paper commissioned by the Office of the Australian Information Commissioner, 2020, https://www.oaic.gov.au/__data/assets/pdf_file/0012/11136/Report-Privacy-risks-and-harms-for-children-and-other-vulnerable-groups-online.pdf