AUSTRALIAN RESEARCH COUNCIL
Centre of Excellence for the Digital Child.

31 March 2023

Privacy Act Review Report
Attorney General's Department, Australian Government
4 National Circuit
Barton ACT 2600

This submission is made by the Australian Research Council (ARC) Centre of Excellence for the Digital Child, prepared by Dr Anna Bunn (Curtin University), Dr Rys Farthing (Deakin University), Professor Tama Leaver (Curtin University), Professor Susan Danby (Queensland University of Technology, Centre Director), Dr Tiffany Apps (University of Wollongong), Dr Karley Beckman (University of Wollongong), Dr Aleesha Rodriguez (Queensland University of Technology), and Professor Michael Dezuanni (Queensland University of Technology).

ABOUT THE ARC CENTRE OF EXCELLENCE FOR THE DIGITAL CHILD

Thank you for the opportunity to provide feedback on the Privacy Act Review Report (the 'Review') (February 2023).[1]

The ARC Centre of Excellence for the Digital Child ('Centre'), funded by the Australian Research Council with AU$34.9M over its seven-year life, is charged with leading national and global research, policy and practice to ensure that all Australian children are healthy, educated and connected in a rapidly expanding digital world. An internationally esteemed team of more than 40 interdisciplinary researchers who have demonstrable expertise, diverse perspectives, and disciplinary expertise address the significant risks and opportunities of digital technologies in everyday lives of families and educators, including screen time, children's digital rights, e-privacy, commercialisation, digital technology innovation, relationships, healthy wellbeing, sociality, education and learning, and digital play. The Centre involves six Australian universities, 13 international universities, and 19 global partners, including Google and the Office of the eSafety Commissioner, and national partners, including Early Childhood Australia, The Smith Family and SciTech. The Centre is particularly well placed to respond to the Review and welcomes the opportunity to do so.[2]

The Centre welcomes the reforms proposed in Review. It is particularly pleasing to see explicit recognition of the need to protect children, alongside acknowledgement of the fact that the digital environment is crucial for children's development and affords them many opportunities, including for connection, play, creativity, education and development. We are pleased that the Review adopts a child-rights focus.

[1] Attorney General's Office, *Privacy Act Review* (Report, 2023) https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report
[2] For more information about the ARC Centre of Excellence for the Digital Child, see https://www.digitalchild.org.au/.

Some specific comments and suggestions in relation to the reforms proposed are set out below.

I. SCOPE AND APPLICATION OF THE PRIVACY ACT

We welcome the recommendations (Proposals 4.1-4.10) that would, among other things, clarify that personal information is an expansive concept which includes technical and inferred information, such as IP addresses and device identifiers relating to a reasonably identifiable individual. Such information is often used to track, profile and then target individuals, including children.[3] However, we have provided further comment, below, on the proposals relating to the regulation of targeting, given that this often involves the collection of information that may not fall within the definition of personal information (even as expanded).

1. Privacy Policies and Collection Notices

We welcome proposals that would require entities to ensure that privacy policies and collection notices are clear and up to date. We particularly welcome proposal 16.3 —amending the *Privacy Act 1988* (Cth) ('Privacy Act') to require that collection notices and privacy policies be clear and understandable, in particular for any information addressed specifically to a child — and to include further guidance in the Children's Online Privacy Code. The Centre is well-placed to assist in future development and testing of child-friendly policies.

We also recommend that consideration is given to including in the Privacy Act a requirement that entities bound by it notify users of their online services as to whether third parties have been given permission to install code (e.g., cookies, pixels or other means) that allows for the automatic collection of information (including but not limited to personal information) about users.

Currently, APP entities are not required to notify individuals about the direct collection of their information *by others*. Although APP entities that collect personal information about an individual are currently required (by APP 5) to take reasonable steps to notify the individual of certain matters, or to ensure the individual is aware of those matters, entities collecting information automatically (such as by cookies, pixels and the like) may escape notification obligations. There are two main reasons for this. First, the information collected may not be considered 'personal information' (as that term is presently defined in the Privacy Act). Second, it may not be considered reasonable to notify the individual of the collection (not least because the collection occurs via a webpage maintained by a third party). An expanded definition of 'personal information' would address the first reason, but not the second. Therefore, placing a requirement on the entity that has given permission for third parties to embed automatic data collection tools into webpages will increase transparency.[4] It is not, of course, intended that these notification requirements replace the need for entities to

---

[3] See, eg, Human Rights Watch, *How Dare They Peep into My Private Life?: Children's Rights Violations by Governments That Endorsed Online Learning During the COVID-19 Pandemic* (2022) https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments; Children and Media Australia, *Summary of Pilot "Apps Can Track" Project 2021-2022* (2022) https://childrenandmedia.org.au/assets/files/news/latest-news/yappcensussummary22fin.pdf.

[4] It is not perfect given that permission is not always sought or required. See, for example, real-time privacy inspector *Blacklight* by *The Markup* https://themarkup.org/blacklight.

satisfy the fair and reasonable test in relation to their collection, use and disclosure practices. Further consideration should be given as to the form and timing of any such notices.

II. FAIR AND REASONABLE PERSONAL INFORMATION HANDLING

The Proposals (12.1-12.3) for fair and reasonable information handling are welcome and we support the inclusion of a best interests test (12.2f) as a legislated factor that should be taken into account when determining if an entity's information handling practices are fair and reasonable.

A need to take account of the best interests of the child stems from the UN Convention on the Rights of the Child ('UNCRC') and is a key principle in its interpretation.[5] It is also an important guiding principle in 'determining the measures needed to guarantee the realisation of children's rights in relation to the digital environment.'[6] The best interests principle in the UNCRC provides that: 'In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration'.[7] The Committee on the Rights of the Child ('CRC') issued *General Comment No. 14* (2013)[8] on the interpretation of the best interests test in UNCRC. *General Comment No. 14* notes that the use of the word 'shall' in Article 3(1) places a 'strong legal obligation on States' and means that assessing children's interests and ascribing them 'proper weight as a primary consideration in any action undertaken' is not discretionary.[9]

The Review notes that whenever personal information relates to a child, 'an entity would need to consider "whether the collection, use or disclosure of the information is in the best interests of the child"'.[10] However, the wording of the recommendation (Proposal 12.2) states that the legislated factors, including the best interests test, 'may' be taken into account in determining what is fair and reasonable. Although we note that the final wording of any legislative provisions is to be developed through the drafting process, it would be preferable if the recommendation clarified that best interests test *must* be taken into account whenever personal information relating to a child is collected, used or disclosed. This is consistent with the notion, reflected in *General Comment No. 14* (2013), that a child's best interests should not be a discretionary consideration.

In addition, we believe that reference to the child's best interests in the list of legislated factors should be extended to require that the child's best interests should be *a primary consideration* in determining whether an entity's information handling practices are fair and

---

[5] See, for example, Michael Freeman, 'Children's Rights as Human Rights: Reading the UNCRC', *The Palgrave Handbook of Childhood Studies* (2009), 377-393; and UN Convention on the Rights of the Child. (1989) ('UNCRC') https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

[6] UN Committee on the Rights of the Child ('CRC'), *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment* (CRC/C/GC/25), para 8, *https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation*.

[7] UNCRC, art 3(1).

[8] CRC, *General Comment No. 14 (2013) on the Right of the Child to Have His or Her Best Interests Taken as a Primary Consideration* (CRC/C/GC/14) https://www2.ohchr.org/english/bodies/crc/docs/gc/crc_c_gc_14_eng.pdf.

[9] Ibid, para 36.

[10] Attorney General's Office (n 1), 119.

reasonable. Again, this is consistent with *General Comment No. 14* which explains that the requirement to take the child's interests into account as a primary consideration indicates that these interests may not be considered 'on the same level as all other considerations'.[11] This position, the CRC remarks,[12] is 'justified by the special situation of the child: dependency, maturity, legal status and, often, voicelessness …. If the interests of children are not highlighted, they tend to be overlooked.' The need to consider the child's best interests as a primary consideration does not require the child's interests to trump other interests but does mean that considerable weight should be attached to them.

III. CHILDREN

1. Child's capacity to consent (Proposal 16.2)

The need to respect a child's evolving capacities is central to achieving the appropriate balance between protection from harm within the digital environment and participation within it. The concept, introduced through the UNCRC (Article 5), requires us to recognise that children 'progressively acquire knowledge, competencies and understanding, including acquiring understanding about their rights and about how they can best be realised'.[13] As the CRC has recognised, this process of progressive acquisition of knowledge, competencies and understanding has 'particular significance in the digital environment, where children can engage more independently from supervision by parents and caregivers'.[14] Crucial to the concept of evolving capacities is a recognition that each child is different, and it is impossible to specify a fixed age at which children are considered competent to make autonomous-decisions.[15]

We therefore very much welcome Proposal 16.2 which recommends that existing OAIC guidance[16] on capacity of children and young people continue to apply. That guidance recognises that capacity should be assessed on an individual basis where possible but that certain presumptions can apply where this is not possible. One of those presumptions is that 'an individual **aged 15 or over** has capacity to consent' [emphasis added]. This means that anyone aged 15 or over is presumed to have capacity and anyone under 15 is presumed not to.

However, we note that Proposal 16.2 suggests that an entity that is not able to individually assess the capacity of a child or young person to provide consent may presume that a 'individual **over the age of 15** has capacity, unless there is something to suggest otherwise' [emphasis added]. This would mean that anyone aged 16 or over would be presumed to have capacity and those under 16 presumed not to.[17]

---

[11] CRC, *General Comment No. 14* (n 8), para 37.
[12] Ibid, para 37.
[13] CRC, *General Comment No. 7 (2005)*, *Implementing Child Rights in Early Childhood*, (CRC/C/GC/7/Rev.1), para. 17.
https://www2.ohchr.org/english/bodies/crc/docs/AdvanceVersions/GeneralComment7Rev1.pdf
[14] CRC, *General Comment No. 25 (2021)* (n 6) para 19.
[15] CRC, *General Comment No. 12 (2009) The Right of the Child to be Heard* (CRC/C/GC/12) https://www2.ohchr.org/english/bodies/crc/docs/advanceversions/crc-c-gc-12.pdf.
[16] Office of the Australian Information Commissioner. *Children and Young People* https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/children-and-young-people
[17] Note, confusion may have arisen from the fact that although the APP Guidelines state '15 or over' the APP's webpage on *Children and Young People*

In our opinion it is appropriate to allow for a presumption of capacity to consent on the part of young people aged 15 and above (rather than 16 and above, as per Proposal 16.2). This is consistent with the OAIC's current guidelines which steer a 'middle ground between individualised assessment and practicability'.[18]

2. Children's Privacy Code (Proposal 16.5)

We strongly support the introduction of the Children's Privacy Code, something that the Centre advocated for in its submissions to the Online Privacy Bill Exposure Draft.[19] A code that applies to online services likely to be accessed by children is appropriate given the risks posed by online services, regardless of sector or size.

A Children's Privacy Code modelled on the UK's *Age-Appropriate Design Code*,[20] and informed by similar Codes in Ireland (the *Fundamentals of Child-Oriented Approach to Data Processing*)[21] and California's *Age-Appropriate Design Code*[22] will ensure a precautionary approach to the collection and use of a child's data and will promote the best interests of child users.

a. *Consultation with Children*

A requirement to consult with children, among other stakeholders, is important and consistent with UNCRC Article 12, which affords to children capable of forming their own views, the right to express them freely in matters concerning them, and for those views to be given due weight in accordance with the age and maturity of the child. Meaningful involvement in the reform process requires more than just giving children a chance to have their say. Children must be facilitated to express their views and these views must be listened to and acted upon, as appropriate.[23]

The Centre is well-placed to facilitate and support consultation processes with children, and to ensure that children are given the tools to understand and talk about their rights, including their rights to privacy, participation and protection.

(https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines) uses the term 'over 15'.

[18] Normann Witzleb & Moira Paterson, *Privacy Risks and Harms for Children and Other Vulnerable Groups in the Online Environment* (18 December 2020), Research Paper commissioned by the Office of the Australian Information Commissioner (OAIC), 83.

[19] See response to Online Privacy Bill Draft by the ARC Centre of Excellence for the Digital Child https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/consultation/view_respondent?uuId=748212539.

[20] UK Information Commissioner's Office, *Introduction to the Age Appropriate Design Dode* (2020) https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/.

[21] Data Protection Commission (Ireland), *The Fundamentals for a Child-Oriented Approach to Data Processing* (2021) https://www.dataprotection.ie/en/dpc-guidance/fundamentals-child-oriented-approach-data-processing

[22] State of California. *Age-Appropriate Design Code* (2022) https://leginfo.legislature.ca.gov/faces/billPdf.xhtml?bill_id=202120220AB2273&version=20210AB227393CHP.

[23] CRC, *General Comment No. 12 (2009)* (n 15); Laura Lundy, 'Voice 'is Not Enough: Conceptualising Article 12 of the United Nations Convention on the Rights of the Child' (2007) 33(6) *British Educational Research Journal*, 927-942.

b. *Inclusion of Specific Rights*

As the code will apply to a wider range of entities than do the APPs, it should also provide users with all of the rights set out in the APPs including, but not limited to, the right to object to information processing, and the right to erasure.

We commend the introduction of a right of erasure (Proposal 18.3) enabling individuals to have specific information erased on their request. As currently outlined, this is a general right for all individuals. For those under the age of 18, the right of erasure has particular value as it can enable young people having a childhood the traces of which are not available online forever if this is contrary to their wishes.[24] We would recommend that **a specific right of erasure for children's data and data about children** be established specifically within the proposed *Children's Privacy Code* (Proposal 16.5) to the effect that data erasure should be actioned when data (whether generated, captured or inferred) pertains to a child and erasure of the data has been requested by the data subject (even if no longer a child) or by a parent or caregiver, without further explanation being required. Similarly, this right should align with Proposal 18.2 and provide that an APP entity must disclose what, if any, data they hold about a child if requested.

Thus, a specific right of erasure for children's data, and data generated while someone was a child, would ensure, effectively, that in terms of digital traces and footprints children's right to privacy is respected.

c. *Drafting of the Code*

We support the intention that this Code should be drafted by the Office of the Australian Information Commissioner, rather than being a co-regulatory Code. This is in keeping with Proposal 5.1. Difficulties in finding an appropriate code developer to represent all services that children are likely to access, and the problematic experience with developing the Online Safety Codes,[25] suggest that a regulator-drafted Code would be in children's and the public's best interests. We also note that consultation with young people themselves suggests that they would prefer a regulator or legislator drafted Privacy Code, with polling suggesting that only 14% teenagers trusted social media companies to 'write the rules' around their privacy.[26]

3. Regulation of Targeting

We would recommend that the Privacy Act is clarified to stipulate that targeted advertising for commercial purposes is not in children's best interests, thus preventing it even where data is collected directly from children (Proposal 20.6). We appreciate that some targeted advertising may be in children's best interests, such as identifying those in need of mental

---

[24] See Tama Leaver, 'Balancing Privacy: Sharenting, Intimate Surveillance and the Right to Be Forgotten' in Lelia Green et al (eds), *The Routledge Companion to Children and Digital Media.* (2021, Routledge) 234–244 <https://doi.org/10.4324/9781351004107-22>.

[25] See, eg, Australian Child Rights Taskforce, *Letter to the eSafety Commissioner re Online Safety Codes* (2022) <https://childrightstaskforce.org.au/wp-content/uploads/2023/01/Online-Safety-Codes_-ACRT-letter-to-eSafety.pdf>.

[26] Rys Farthing, Reset Australia, *How Outdated Approaches to Regulation Harm Young People* (2022) https://au.reset.tech/uploads/report_-co-regulation-fails-young-people-final-151222.pdf.

health support and providing information about available services, but we remain concerned that advertisers may distort the definition of 'best interests' to include brand awareness or commercial choice.

Likewise, we note that Proposals 20.5, 20.6 and 20.7 combined may not have the effect of protecting children from the exploitative *data harvesting* underpinning the delivery of targeted ads. Much of the commercial data harvested about children is done by large, vertically integrated companies, often through placing tracking cookies, pixels or SDKs—such as Facebook Pixel or Google AdMob—into other digital products and services. Where tracking cookies, pixels or SDKs are used, large vertically integrated companies collect data directly about children, even if children are ostensibly using a third party digital product or service. Due to the vast troves of data that these large, vertically integrated companies collect, they have no need to trade this proprietary data so may avoid being curtailed by the proposal to prohibit trading children's information (Proposal 20.7). Likewise, they may simply be able to turn off their ad delivery systems and replace them with contextual ad delivery systems, as many platforms are now doing to meet EU requirements. This would avoid curtailment by Proposals to prohibit *targeting* a child (Proposal 20.6), and the prohibition on direct marketing to a child *unless the data was directly collected* from that child (Proposal 20.5)[27].

While the proposal to prohibit targeting a child may therefore stop the delivery of targeted advertising to children—which corresponds with children's best interests—it will not stop the massive data harvesting that occurs every time children use one of these large platforms or any other digital product or service with a cookie, pixel or SDK embedded in it. That is, these proposals will not require vertically integrated platforms to redesign their products or processes, so children's data will inevitably be caught in the data 'dragnet.'

Even if it is not used to serve targeted advertising, this widespread data collection poses unique risks to children and young people. This includes risks arising from data security failures (such as breaches and hacking); errors on the side of data processors (such as inadvertent use or failures to policy within companies); and the ongoing risk of commercial use by large platforms. For example, data collected by tracking children's online activity may not be used to serve them targeted ads, but it may be used to train AI or enhance extended-use algorithms. A stronger approach would be to include an additional proposal to prohibit the collection of data normally associated with direct marketing to children, such as cookies, pixels and SDKs (which would require a change in product) or to require these to be deleted as soon as they are collected (which would require a change in process). At the very least, the collection of this information should be subject to the fair and reasonable test even to the extent that it does not fall within the proposed expanded definition of personal information.

IV. PARENT AND FAMILY DATA

We note that the child specific privacy protections in Proposal 16 and prohibitions in Proposals 20.5, 20.6 and 20.7 do not consider the connection between children's data, parent data and family data. When considering children as data subjects it is critical to

[27] Indeed, if either clause 20.5 or 20.6 falters, it might have the perverse effect of strengthening the market dominance of large, vertically integrated platforms as providing the only ad delivery systems for children in Australia.

understand the processes of datafication (including harvesting, profiling and tracking of children) as non-linear, plural and connected to parents and family data.[28] This unfolds through business models, algorithmic design and shared practices. There is evidence that commercial data harvested about children is done through a parent proxy.[29] This occurs as digital products designed for children, including educational technologies that children are required to access across home and school, prohibit the creation of children's profiles or accounts in place of parent or family accounts. The child then accesses the digital product or service via the parent or family account and 'parent' data is collected despite the child being the likely data subject.[30]

We note that the prohibitions in Proposals 20.5, 20.6 and 20.7 may not protect children from exploitative data harvesting and trading in the circumstance where a digital children's product and/or service uses the collection of parent data through cookies, pixels and SDKs as a proxy for children's data. We therefore recommend that the Review specifically recognises that parent/family data is often used as a proxy for children's data. The non-exhaustive examples of 'personal information' to be provided in the Act (pursuant to Proposal 4.2) should include collection of 'parent/family data where that relates to or can be related to an identified child, or a child who is reasonably identifiable.' As noted earlier (under Regulation of Targeting), a stronger approach would be to prohibit the collection of data normally associated with direct marketing to children. This should include parent/family data that is used as a proxy for children's data. We recommend that Proposal 20.7 is amended to 'Prohibit trading in children's personal information *or information relating to children*.'

We emphasise the need for Proposal 16.3 to address the overlap between parent and children's data. Specifically, in instances where the collection of 'parent' or 'family' data is permitted, we recommend that collection notices and privacy policies should provide clear and understandable articulation of the nature of children's data (if any) that is captured through the collection of parent data. We also recommend that this type of data collection be articulated in the design of a *Children's Online Code* (Proposal 16.5).

—

Thank you for the opportunity to provide submissions to the Review. We look forward to further engagement with you on these proposals and we stand ready to answer any questions you may have in relation to these submissions.

---

[28] Veronica Barassi, 'The Child as Datafied Citizen: Critical Questions on Data Justice in Family Life' in Giovanna Mascheroni et al (eds), *Digital Parenting: The Challenges for Families in the Digital Age* (2018, NORDICOM) 169-177.

[29] See, eg, Tiffani Apps, Karley Beckman, & Sarah K. Howard, 'Valuable data? Using Walkthrough Methods to Understand the Impact of Digital Reading Platforms in Australian Primary Schools' (2022) *Learning, Media and Technology*, 1–16.

[30] *Epic*, *StudyLadder,* and *Spriggy* are a few examples of applications (designed specifically for children's use) that require parents to create children accounts; and then collect 'parent data' which by design implicates children's data.