# Response to the Children's Online Privacy Code: Issues Paper

[redacted]

[redacted] *ARC Centre of Excellence for the Digital Child, Deakin University*

## Preamble:

The issues paper details that the Code is specifically meant to ensure privacy protections for *children who engage in a digital world*, and that the code will *apply to online services likely to be accessed by children*.

However, this submission asserts that the code needs to go further, and cover additional services or entities that collect, produce, share or process data *about* children, even prior to children accessing online services themselves.

From the moment they are born, children are *legal subjects* with the right to have others act in their best interest – including protection from the excessive collection and processing of their personal data. These rights are at odds with the current lack of protection for young children's data in online spaces. Children from their earliest life-stages today are becoming *data subjects* whose personal information is shared, collected and processed, without the ability to exercise their agency, and consent or object to these practices.

Parents are often relied upon to make decisions that protect their children's data privacy. However, as will be further outlined below, parents are often unable to provide meaningful consent regarding the sharing of their own and their children's personal data.

Therefore, young children's rights for data protection must be regulated at a higher instance, and the Children's Code provides a unique opportunity to specifically identify and regulate data protection for children from their earliest life stages.

## 1. Scope of services covered by the Code

*1.1 Are there additional APP entities, or a class of entities, that should be covered by the Code? Please provide reasons or evidence to support your view.*

**Yes, any mobile applications whose use collects data about a (developing) child/ren, need to be covered by the Code.**

*Why should these apps be covered by the code?*

**Data surveillance of children begins even before they are born, and mobile applications aimed at parents (to be) play a key role in these processes**.

In the contemporary media environment, children's data is collected from their earliest life-stages and "even before birth", as asserted by Australian Children's Commissioner Anne Hollonds (2021) – echoing arguments made by many high-profile academics researching children and technology (Barassi, 2020; Holloway, 2019; Mascheroni & Siibak, 2021) and by children's rights advocates (Children's Commissioner, 2018; Cannataci, 2021).

Practices such as the sharing of ultrasound images (Leaver, 2015), or the use of pregnancy-tracking apps and other *baby apps* are specific examples brought forward in this context (Hollonds, 2021; Langton, 2024a). These digital practices contribute significantly to the vast

amount of data being routinely collected about children, adding up to around "72 million data points before a child reaches the age of 13" (Donnell, 2019).

The prevalent use of *baby apps* – including fertility-, pregnancy-, and baby-tracking applications – by parents, results in the collection of a wide range of personal data about children. These apps are designed to support parents throughout the transition to parenthood – from family planning over pregnancy to early parenthood. While many of these apps are 'free' to download and use, users commonly 'pay' for the use of these apps with their personal data. This personal data frequently encompasses not only the data of the apps' primary users – commonly parents, or parents-to-be – but also their children. App entities share this data with third parties for monetisation, including consumer profiling (Hamper, 2024; Kemp, 2023). Because this data is not deemed 'health' data, and it is not explicitly recognised as data about children, no special protections apply. The indiscriminate handling of children's data in these contexts increases privacy risks for children, both through data-sharing with third parties, as well as through unnecessarily long data storage periods – increasing the risk of children's data being shared with bad actors in data breaches.

### Wide-spread sense of powerlessness in parents' ability to protect children's data privacy

**The responsibility for the management of children's data collected in these apps must be regulated by a higher instance.**

Baby app users/parents feel that informed, meaningful consent for the sharing of their own and their children's personal data during baby app use is not possible, and there is increasing resignation and acceptance of pervasive data-sharing. Research into users' attitudes towards the datafication of parenthood through baby apps, confirms that the monetisation of personal data through baby apps is becoming increasingly normalised and accepted (Hamper, 2024). This normalisation is promoted by a sense of widely reported *digital resignation* (Draper & Turow, 2019) – when users resign themselves to give up their personal data in exchange for access to a digital service.

Online sources of parenting support – including mobile applications – play a crucial role in the lives of Australian parents in particular, who are often physically separated from sources of familial or professional parenting support (Cann et al., 2021; Langton, 2024b). The increased vulnerability that parents experience during the transition to parenthood and in early parenting (Virani et al., 2019; Langton, 2024a, 2024b), means that parental support needs frequently conflict with their children's right to privacy – complicating parental decision-making regarding the sharing of personal data required to access parenting support through baby apps.

Additionally, the privacy policies of baby apps are often excessively long, vague, and contradictory (Kemp, 2023) – negating users' ability to provide meaningful 'informed consent' (Okoyomon et al., 2019) or opt-out of data-sharing. These factors result in a sense of powerlessness, supporting the perception that "for many [parents] today, it has become impossible to escape this process of datafication, or to protect the privacy of their children" (Barassi, 2020, p. 34).

## Emerging findings from our current study on "Tracking the Trackers" of children's first personal data

Research Fellows from the Digital Child Research Centre (Katrin Langton, Deakin University and Rebecca Ng, University of Wollongong) recently conducted analysis of app code for 38 popular baby apps, including 11 fertility-trackers, 16 pregnancy-trackers, and 11 baby-tracking apps. Static analysis of app code can make visible the data accesses an app requests on a personal device during app installation and use, as well as the tracking signatures for third parties who the app is able to connect to and share data with. Additionally, the privacy policies of three case study apps were reviewed, specifically the fertility- and pregnancy-tracking app *Flo* (Flo Health Inc., 2025), the pregnancy-tracking app *amma: pregnancy tracker* (amma, 2025), and the baby-tracking app *Huckleberry* (Huckleberry Labs, 2025). Apps were chosen for their high level of popularity, and to examine apps that seemed to collect or share particularly large amounts of data. The aim of the study was to explore the infrastructural data-sharing capabilities of baby apps, and how these correlate with how the collection and sharing of users'/children's data are presented in baby apps' privacy policies.

### 1. Ambiguity in baby app's privacy policies may change the ways users and policy-makers think about children's data, downplaying the sensitivity of the data collected, and allowing its embedding into a wide range of data-processing practices, including machine-learning

- The baby-tracking app *Huckleberry* enables parents to digitally track their infants' routines, including feeds, nappy changes, and sleep schedules – with a key feature of the app being the provision of sleep plans and sleep schedule recommendations. A particular concern regarding the data collected, is that it clearly centres around children's health and development – but is not explicitly acknowledged as 'health' or 'sensitive' data. Instead, the policy speaks of 'wellbeing data'. This language categorically "downgrades" the information as less personal or sensitive, and therefore as not requiring particular protection or special consideration to protect the data privacy of the app's primary users and their children.
- Additionally, *Huckleberry* uses AI technology to produce its sleep plans, based on the data provided by users about their children's routines, thereby not just collecting, but also producing 'wellbeing data' through algorithmic processing and predictions. These practices produce data whose ownership is ambiguous, with children's data effectively becoming part of machine-learning and AI models – making data deletion, alteration or retrieval impossible, and raising questions about data ownership. The app's privacy policy therefore effectively requires users to sign ownership of their personal data over to the technology provider:

> "The information that is created when you sign up to use our Products or in fact use our Products; for example, data regarding your child's sleep, information you provide to us in questionnaires or data generated by your use of or progress in the Products (collectively, "Product Data"); is owned by Huckleberry and its licensors. [...] User Content refers to any publicly available content that you submit to us, such as a profile photo or comments in the community. [...] You hereby grant us a worldwide, perpetual, irrevocable, non-exclusive, fully-paid and royalty-free license, with the right to sublicense through multiple levels, to store, reproduce, perform, display, transmit, distribute, create derivative works of, and otherwise use your User Content in connection with providing our Products." (Huckleberry Labs, 2022)

- These observations point to the power of commercial practices in its normative shaping and manipulation of understandings of 'sensitive' data, the ambiguities around the implications of these practices on data ownership and handling, and the increasing difficulty in regulating these practices.

2. Permissions for data access unnecessarily increase over time, and data from apps by the same developer is increasingly consolidated

**Keeping requests for data access through app permissions – especially 'dangerous' invasive permissions – to a minimum, can reduce the likelihood of excessive datafication, and should be a key goal for app developers and policy makers seeking to address privacy concerns for children and their families**.

- There is an overall tendency in baby apps towards what can be described as 'permissions creep' – where the total number of permissions for data access on users' phones increases over time, including for particularly invasive data accesses such as camera and microphone access, or location information. A particularly problematic example in this context is *amma: pregnancy tracker*, which integrates a large number of invasive permissions – including requests to access the device ID, location information and the ability to directly call phone numbers, as well as microphone and camera access. Many of these permissions far exceed the usual data accesses requested for basic app functioning.
  Our work shows that although many baby apps integrate around 30 or more permission requests in their code, their necessity for app functioning and key features is questionable, and the majority of baby apps require only around 20 permissions to support their features.

**Tech providers' reliance on the sale of data provided during baby app use for app monetisation must questioned, to minimise excessive data-sharing and maximise data protections – including effective de-identification and the prevention of re-combination of data that may result in re-identification of users and their children.**

- Apps like *amma: pregnancy tracker* pose a clear risk to users' data privacy, by combining a high number of invasive permissions, with a high number of tracking signatures – including a total of 30 trackers in its code that enable network connections to third parties.
  A key concern is that by establishing network connections for data-sharing during app use, the app's ability to access sensitive user data is extended to third-parties. A combination of a large number of invasive permissions and a high number of tracking signatures is therefore particularly problematic.

**The consolidation of data from baby apps, specifically the aggregation and combination of user data over time, must be considered in terms of the risks to users' and children's data privacy.**

- The development of hybrid apps combining functionalities of different baby app categories (*Flo* for instance can switch between a fertility-tracking and a pregnancy-tracking mode) and the development of baby app 'ecosystems' – are a common trend. This trend means that data about reproduction and children's development over time is less likely to be collected via distinct apps with separate data flows; instead, more data is collected through the same app, or complementary apps from the same provider, over time. Hybrid apps such as *Flo*, or its competitor *Clue*, which over different 'modes' of

app use for fertility and pregnancy-tracking (Flo Health Inc., 2025; Toler, 2021), and the development of app ecologies such as the *Glow* range – offering a fertility-, pregnancy-, and baby-tracker by the same developer (Glow Inc., 2025) – promote not only the increasingly extensive datafication of this life-stage, but also the aggregation and combination of all data collected throughout this period.

3. Baby-tracking applications now commonly integrate AI-capabilities into their functionalities

**Considering the rapid rise of AI and the increasing integration of AI 'solutions' and predictions into everyday decision-making, it is crucial to consider who is served through access to vast amounts of data on children's bodies and family routines.**

- Aside from the total number of tracking signatures, the distribution and frequency of particular trackers across the sample provides insights into the data-sharing ecologies of baby apps. Our research shows a very clear skew towards Google and Facebook as the entities that get to benefit most from baby apps' data sharing, exposing significant concentration of control over data access and processing, and the commercial gains from these practices. Notably, the parent companies behind Google and Facebook – Alphabet and Meta – are both developing their own AI systems.

### Risks to children's data privacy and rights

**These practices may breach children's rights to non-discrimination in ways that are difficult to anticipate and cannot be undone.**

At a minimum, data entered into baby apps identifies to advertisers/commercial actors that a child exists, but often these apps promote the recording of children's personal information - including gender, age, (estimated) date of birth, location, behavioural and health information. This data can easily be shared and aggregated well beyond the contexts in which it was originally provided (Kemp, 2023). Once baby app users' and their children's data traces are passed on to third parties, the data is outside of the parents'/app user's control, and cannot be retrieved, viewed, corrected or deleted.

This data-sharing may have serious and permanent implications for children, if data is consolidated into online profiles, constructing a consumer identity and influencing children's self-understanding and online participation well before they ever generate digital traces themselves. It may also have serious implications regarding identity theft and fraud. The United Kingdom's financial institution Barclays has estimated that data from "sharenting" practices – including any information shared about children's names, birthdates and home address, and other family details deduced data traces that are collated over time, will account for two-thirds of identity fraud facing young people (Children's Commissioner, 2018). These data traces can include ultrasound images, or personal data collected and stored through baby apps. Data analysis for online profiling and prediction of young people's behaviours, routines and abilities, based on their available data traces, is also likely to become more prevalent, through increasing integration of AI technologies and sophisticated machine-learning.

**Children's data privacy must be future-proofed, against the negative implications that may result from the AI-driven processing of their personal data.**

Aside from explicitly identifying, personal information, many of the data traces produced during baby app use pertain to everyday family routines and are seemingly mundane. Yet, as long as

there are enough of them, algorithmic analysis and specifically AI capabilities are employed to produce commercial value through predictions and evaluations of this data. These assessments are often highly simplified and reductive, despite narratives of 'data-driven insights' that lean into long-standing power dynamics associated with scientific authority (Moretti & Maturo, 2018) and data as trustworthy (Beer, 2019). The kind of 'transparency' assumed to be provided in privacy policies, does not provide sufficient basis for meaningful consent (Ananny & Crawford, 2018; Okoyomon et al., 2019) – making the use of children's data in the training of AI tools and other automated systems even more concerning.

Including baby apps' data and commercial entities in the entities regulated through the children's code would not only significantly contribute to future-proofing children's data privacy, but also the data privacy of all users of baby apps, including the bodies of (pregnant) women, who are particularly vulnerable and disproportionately datafied (Cahn & Manis, 2022; Kemp, 2023).

**The entities who stand to gain commercially from the sharing of users' and children's personal data, need to take responsibility for users' and children's data privacy. Children's rights as *legal subjects*, must outweigh their commercial value as *data subjects*.**

*Recommendations for risk mitigation*

- App providers need to ensure any subsequent data processing does not interfere with children's right to privacy as children's best interest must outweigh the business interests of the commercial entities behind baby apps (United Nations, 2021, para. 68-69).
- App providers must take responsibility for the way that children's data may be processed by third-parties, particularly if it may be passed on to further data-processors and data-brokers, including marketing and advertising networks (United Nations, para. 40 & 42).
- Fines or other remedies for misuses of children's personal data need to apply, to encourage compliance

**There is 'offline' precedence for instances of excessive and problematic data-sharing, including the in-person collection of mothers' and newborns personal information through commercial actors.**

One example is the maternal 'goody bag' provider Bounty, which shared personal information about new mothers and their babies, which they directly collected from new parents at the hospital bed while distributing 'baby essentials' such as nappies and samples of creams. This data was subsequently shared with third parties for advertising and marketing purposes. Bounty was fined £400,000 for 'misuse of private citizen data', which included "highly sensitive information [such as] the birth date, gender and addresses of infants, as well as names, addresses, pregnancy status and other details about new and soon-to-be parents" (Murgia, 2019, para. 2). Data collection from baby apps is not dissimilar, in how they collect data directly from new parents who are experiencing increased vulnerability and reliance on support that makes opting out of these services difficult, only to share this information for commercial gain.

## Issues summary:

- User data from baby apps frequently encompasses children's data

- Users cannot meaningfully consent to the collection of this data on their children's behalf, since purposes of data collection and future uses of data cannot be accurately detailed and anticipated by app entities or app users, leaving children's data unprotected
- Data is often retained for unnecessarily long periods (Kemp, 2023, p. 26), exposing users and their children to risk of potential data breaches
- Data can be shared with third parties, including data-brokers who may circulate this data well beyond the contexts in which it was provided, and for which users provided their consent
- Data may be combined with other data traces, which could enable data-brokers to identify children specifically and accumulate data profiles about them, that can shape children's online experiences (access to information, media content, opportunities for online participation), their self-understanding and identities
- Especially concerning in the age of AI

*1.3 Is there criteria that should be used to determine whether a particular APP entity, or class of entities, is appropriately included or excluded from the scope of the Code?*

**Any entity that collects, shares, or processes children's data (meaning data *by* as well as *about* children), needs to be included**.

Children's data is frequently used as a stand-in for children themselves and emerges well before children ever actively engage in the digital world, through the data traces shared and collected *about* them. Hence, if the aim of the code is about protecting not only flesh-and-blood children, but children as *data subjects* it needs to specifically define *what* (and *when*) data being generated during online engagements, constitutes children's data.

If it is not possible to specifically say whether an entity does collect data about children, but children's data *may be* collected during app use, all data produced in the context of app use should be considered sensitive, or a kind of 'family data', to which additional protections should apply (e.g. shorter retention periods, strict limitations on data-sharing and processing).

## References


amma (PERIOD TRACKER & PREGNANCY AND BABY CALENDAR). (2025). Pregnancy Tracker: Amma [App Store]. *Google Play*. https://play.google.com/store/apps/details?id=ru.mobiledimension.kbr&hl=en_AU&pli=1

Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society*, *20*(3), 973–989. https://doi.org/10.1177/1461444816676645

Barassi, V. (2020). *Child Data Citizen: How Tech Campanies Are Profiling Us from Before Birth*. The MIT Press.

Beer, D. (2019). *The data gaze: Capitalism, power and perception*. SAGE Publications Ltd.

Cahn, A. F., & Manis, E. (2022). *Pregnancy Panopticon: Abortion Surveillance After Roe* (pp. 1–16). Surveillance Technology Oversight Project. https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/6297d83433c19479f037ab8c/1654118453441/2022.6.1_STOP+Report_Pregnancy+Panopticon.pdf

Cann, W., Matthews, J., Petrovic, Z., Wade, C., Almendingen, A., & McDonald, M. (2021). *Parenting today in Victoria: Parent's information seeking*. Parenting Research Centre.

https://www.parentingrc.org.au/wp-content/uploads/2024/10/ResearchBrief_ParentsInformationSeeking86.pdf
Cannataci, J. A. (2021). *Artificial intelligence and privacy, and children's privacy*. United Nations General Assembly. https://docs.un.org/en/A/HRC/46/37
Children's Commissioner. (2018). *Who knows what about me?* https://assets.childrenscommissioner.gov.uk/wpuploads/2018/11/cco-who-knows-what-about-me.pdf
Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society*, *21*(8), 1824–1839. https://doi.org/10.1177/1461444819833331
Elvery, S., & Tan, T. (2025, February 27). You read the terms and conditions, right? *ABC News*. https://www.abc.net.au/news/2025-02-27/classroom-apps-technology-kids-data-terms-conditions/104966952
Flo Health Inc. (2025). *We're Flo, the world's #1 women's health app*. Flo. https://flo.health/
Glow Inc. (2025). *Glow: The Most Comprehensive Women's Health Apps*. Glow. https://glowing.com/?srsltid=AfmBOoqnzqkoN0K2ZUMBOd5VE6tOs6-jpyMoqDduo9LVjPmIXzCUsQhV
Hamper, J. (2024). 'Babies are a massive money spinner': Data, reproductive labour and the commodification of pre-motherhood in fertility and pregnancy apps. *New Media & Society*, 14614448241262805. https://doi.org/10.1177/14614448241262805
Hollonds, A. (2021, July 27). Protect children from data surveillance. *Australian Human Rights Commission*. https://humanrights.gov.au/about/news/opinions/protect-children-data-surveillance
Holloway, D. (2019). Surveillance capitalism and children's data: The Internet of toys and things for children. *Media International Australia*, *170*(1), 27–36. https://doi.org/10.1177/1329878x19828205
Huckleberry Labs. (2025). *Sleep experts for every family*. Huckleberry. https://huckleberrycare.com/
Huckleberry Labs. (2022, October 11). *Huckleberry Labs Privacy Policy and Your Privacy Rights*. Huckleberry Labs. https://huckleberrycare.com/privacy-policy
Kemp, K. (2023, March 22). Fertility apps and your privacy. *Choice*. https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/fertility-apps-comparison
Langton, K. (2024a). *Baby Apps: Mapping the Issues*. ARC Centre of Excellence for the Digital Child. https://doi.org/10.26187/ABR3-9Y10
Langton, K. (2024b). *Constructing contemporary parenthood in digital spaces: Infant feeding and baby-tracking applications and the mediation of Australian parenthood* [Queensland University of Technology]. https://eprints.qut.edu.au/248729/
Leaver, T. (2015). *Born Digital? Presence, Privacy, and Intimate Surveillance*. https://doi.org/10.31235/osf.io/ay43e
Mascheroni, G., & Siibak, A. (2021). *Datafied Childhoods: Data Practices and Imaginaries in Children's Lives*. Peter Lang.
Moretti, V., & Maturo, A. (2018). *Digital Health and the Gamification of Life: How Apps Can Promote a Positive Medicalization*. Emerald Publishing Limited. http://ebookcentral.proquest.com/lib/qut/detail.action?docID=5543347
Murgia, M. (2019, April 13). Personal data on new mothers and babies sold to third parties. *FINANCIAL TIMES*. https://www.ft.com/content/6954971e-5d3a-11e9-939a-341f5ada9d40
Okoyomon, E., Samarin, N., Wijesekera, P., On, A. E. B., Vallina-Rodriguez, N., Reyes, I., Feal, Á., & Egelman, S. (2019). *On The Ridiculousness of Notice and Consent: Contradictions in App Privacy Policies* (Master of Science UCB/EECS-2019-76; pp. 1–13). Berkeley, CA. http://www2.eecs.berkeley.edu/Pubs/TechRpts/2019/EECS-2019-76.html

Toler, S. (2021, November 9). Clue Pregnancy Mode. *Clue*. https://helloclue.com/articles/fertility/clue-pregnancy-mode

United Nations (Convention on the Rights of the Child). (2021, February 3). *General comment No. 25 (2021) on children's rights in relation to the digital environment*. United Nations Human Rights Treaty Bodies. https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en

Virani, A., Duffett-Leger, L., & Letourneau, N. (2021). Parents' use of mobile applications in the first year of parenthood: A narrative review of the literature. *Health Technology*, *5*, 14–14. https://doi.org/10.21037/ht-20-28