Submission on the Exposure Draft of the Privacy (Children's Online Privacy Code) 2026

[redacted], 5 June 2026

I am a data scientist by profession, and this submission is made in a personal capacity. Outside my job, I use freedom of information and data access requests to document how organisations actually handle personal information.

The submission uses a case study drawn from that work to examine whether the protections in the draft Children's Online Privacy Code will hold when tested against the way organisations actually handle personal information. It identifies two structural failure modes, and examines the enforcement conditions necessary for the Code to function in practice.

Case study: The Office of the eSafety Commissioner's Social Media Minimum Age evaluation study

To illustrate the likely failure modes of the draft Code, I draw on the Office of the eSafety Commissioner's evaluation study of the Social Media Minimum Age (SMMA) legislation.

I note that eSafety would not be covered by the Code and is in fact covered by its own Code (the Australian Government Agencies Privacy Code). The example nonetheless demonstrates how gaps in the current draft Code are likely to play out.

The eSafety Commissioner has commissioned a two-year evaluation study of the SMMA legislation, which is currently underway.[1] The study is designed to follow approximately 4,000 children and their families, combining survey data, passive smartphone usage tracking, and linked administrative records from Medicare Benefits Schedule (MBS), Pharmaceutical Benefits Scheme (PBS), and NAPLAN datasets. Participants include children as young as ten.[2]

The study involves complex data flows across multiple entities, with the collection, linkage, and storage of participants' data fragmented across at least six parties.[3] The Social Research Centre (fieldwork provider) directly collects participants' survey responses and personal identifiers, including names, contact details, and Medicare numbers. Wakoopa (third-party technology provider) collects passive smartphone usage data, which is stored in Ireland. Services Australia and state education departments provide linked administrative records from the MBS, PBS, and NAPLAN datasets to the Australian

1 eSafety Commissioner, 'eSafety begins evaluation of Australia's world-first social media minimum age', media release, 26 February 2026. https://www.esafety.gov.au/newsroom/media-releases/esafety-begins-evaluation-of-australias-world-first-social-media-minimum-age.

2 Stevic, A. et al., 'Evaluation of the Social Media Minimum Age on Australian Young People: A Study Protocol', *PsyArXiv*, 2025. https://osf.io/preprints/psyarxiv/u5zn6_v2.

3 The description of the study's data flows draws on the published study protocol (Stevic et al., 2025), documents released by the Office of the eSafety Commissioner under FOI (Log 185, https://www.esafety.gov.au/about-us/corporate-documents/freedom-of-information/disclosure-log), and documents released by the Australian Institute of Family Studies under FOI (FOI26-002, https://aifs.gov.au/compliance-reporting/freedom-of-information).

Institute of Family Studies (AIFS), which de-identifies the administrative data and provides it to eSafety. eSafety holds the linked dataset and manages access for domestic and international researchers. The fieldwork provider also subcontracts components of data collection to further third parties.

In February 2026, I made a freedom of information request to eSafety seeking, among other things, any privacy impact assessment (PIA) or equivalent privacy risk assessment conducted for the study. The FOI decision of 27 March 2026 confirmed that no privacy impact assessment or privacy threshold assessment had been conducted by eSafety, on the basis that the study "was not deemed to be a high privacy risk project, with the study only collecting de-identified information and no personal information."[4]

Nine documents were released under the same decision, including consent forms for administrative data linkage and participant information sheets for passive smartphone tracking. These documents show that names, contact details, and Medicare numbers are collected, as well as health and education records, and usage data from children's smartphones.

In subsequent correspondence, eSafety clarified that personal information is in fact collected and that a privacy threshold assessment was conducted, but by the fieldwork contractor commissioned by eSafety rather than by eSafety itself.[5] As the fieldwork provider handles only the survey and smartphone tracking data, it appears doubtful that such an assessment would apply to the study as a whole. eSafety also stated that the study “ultimately produces de-identified data outputs" and that "neither eSafety nor the passive tracking provider will receive any identifiable information."

I note that AIFS will be assessing the linked administrative data for re-identification risk before providing the data to eSafety.[6] However, as AIFS does not receive either the survey or smartphone data, they are unable to assess the re-identification risk of the final linked dataset. In any case, this assessment will be performed after the study has already commenced and after participants consented on the basis that their data would be de-identified.

I am not a lawyer, but the study would appear to meet any reasonable definition of a high privacy risk project, as it involves collecting and linking sensitive information, children as young as ten, offshore data processing, and a data retention period of at least twenty years. The Australian Government Agencies Privacy Code requires a PIA for all high privacy risk projects, and the OAIC's own guidance recommends a threshold assessment

4 FOI request to the Office of the eSafety Commissioner, decision dated 27 March 2026 (eSafety reference FOI 26038). Copy of the decision letter available from the author on request. I notified the OAIC of the absence of a PIA for the study on 7 April 2026, with further information provided on 9 April 2026 (OAIC reference APP-PI26/0053).

5 Correspondence from the Office of the eSafety Commissioner, 7 April 2026. Copy available from the author on request.

6 Correspondence from the Australian Institute of Family Studies, 18 May 2026. Copy available from the author on request.

for any project involving new or changed ways of handling personal information as the screening step for that determination.[7]

The structural concern this submission raises is not that eSafety acted carelessly or in bad faith. Part of eSafety's statutory mission is the protection of children from online harms, so their commitment to children's privacy is not in question. The Privacy Officer's involvement in procurement, the contracting arrangements with an Accredited Data Service Provider, and the substantive response to follow-up questions all reflect good-faith engagement with children's privacy.[8]

However, the concern remains that despite eSafety's mission being closely aligned with protecting children's privacy and the absence of commercial incentives, the agency was able to characterise its activities in a way that led it to conclude that its privacy obligations were not engaged. I note that the Code will be applied to entities whose operating conditions are substantially less favourable.

Implications for the Children's Online Privacy Code

As noted above, eSafety will not itself be subject to the Code. The SMMA evaluation study is used here to identify structural features that the Code will need to address, not to make a submission about eSafety's conduct.

The SMMA evaluation study is operating under conditions far more favourable than those that will apply to entities within scope of the Code: a published protocol, an ethics committee process, an accredited data service provider, a small defined cohort, no commercial interest in collecting more data than necessary, and public scrutiny. If these conditions did not produce a whole-of-study privacy assessment prior to recruitment, the reasons are structural rather than institutional. The two failure modes identified below explain how this occurred.

The first failure mode: calling data de-identified takes it outside the Code

Information that is de-identified is not personal information, so describing data as de-identified effectively removes it from privacy obligations. The Code inherits this from the Privacy Act, which sets a single test: personal information "is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable."[9]

The eSafety case study demonstrates how this operates in practice. The conclusion that no privacy assessment was required rested on its characterisation of the study as collecting only de-identified information. Given that the data is to be retained for at least twenty years and re-identification risk will only increase over time, this was a significant assumption. Whether a study that links multiple longitudinal datasets produces data in which no child is reasonably identifiable is precisely the question the de-identification test

7 Privacy (Australian Government Agencies — Governance) APP Code 2017, s 12(1); OAIC, 'When do agencies need to conduct a privacy impact assessment?', https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/government-agencies/australian-government-agencies-privacy-code/when-do-agencies-need-to-conduct-a-privacy-impact-assessment.

8 Correspondence from the Office of the eSafety Commissioner, 7 April 2026. Copy available from the author on request.

9 Privacy Act 1988 (Cth), s 6(1).

exists to answer.[10] It cannot be settled by asserting that the outputs are de-identified. The dataset includes MBS and PBS records of the kind that Culnane, Rubinstein, and Teague demonstrated could be re-identified,[11] combined with additional data sources that would increase rather than reduce that risk. The assumption that the dataset is de-identified therefore appears contestable. Despite this, the assertion that the study's outputs would ultimately be de-identified was used to class the study as a whole as not high privacy risk and therefore not requiring a PIA.

For entities within scope of the Code, re-identification is not a hypothetical risk. Identity resolution and data enrichment products exist specifically to match records back to known individuals.[12] In the ecosystem in which the Code will operate, re-identifying data linked to device and online identifiers is a routine commercial activity.

The entities this Code covers hold precisely the data most exposed to this risk. A child's engagement history, social connections, location data, and inferred interests are rich, linked, and longitudinal. Device and advertising identifiers, cookies, hashed emails, and the behavioural and engagement data keyed to them are routinely treated as de-identified as a matter of standard industry practice, despite the OAIC's guidance that all of these can be personal information depending on context.[13] Under the Code, classifying this data as de-identified removes it from any protections.

In one place, the Code already correctly treats de-identification as inadequate. Section 32 requires that, on request, an entity destroy a child's personal information. Unlike APP 11.2, it does not offer de-identification as an alternative. The Explanatory Statement explains that this is deliberate: de-identification "will not be sufficient" for a destruction request, given the risk of re-identification. However, that treatment is confined to section 32. Everywhere else in the Code, de-identification serves as a complete exit from scope. The reasoning that supports the approach in section 32 applies equally to the Code's other provisions.

The second failure mode: no entity is responsible for the whole

A second failure mode emerges when children's personal information moves across several entities. The Privacy Act structures obligations around discrete acts: what each entity collects, holds, uses, or discloses, and what it transfers to overseas recipients. The

10 On the question of re-identification standards more broadly, the standard commonly applied to assess re-identification risk asks whether a reasonably competent, motivated person with no specialist skills could re-identify the data (OAIC, 'De-identification and the Privacy Act', https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/de-identification-and-the-privacy-act). This standard depends on the skill of the re-identifier rather than the consequence of re-identification, and is arguably miscalibrated for an environment in which re-identification capabilities are commercially available. If a child is re-identified, it does not matter who did it or how skilled they were. The harm is the same.

11 Culnane, C., Rubinstein, B.I.P. & Teague, V., 'Health Data in an Open World', arXiv:1712.05627, 2017. https://arxiv.org/abs/1712.05627.

12 See, for example, LiveRamp, 'What is Identity Resolution?', https://liveramp.com/blog/what-is-identity-resolution; Experian Australia, 'Identity Resolution and Data Management', https://www.experian.com.au/insights-au/data-quality/what-is-identity-resolution-and-how-data-management-can-help.

13 OAIC, 'Tracking pixels and privacy obligations', https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/tracking-pixels-and-privacy-obligations.

Code inherits this, binding each entity in relation to its own handling of children's personal information. These provisions govern individual handoffs between entities but do not require any entity to assess the privacy implications of an activity involving multiple parties as a whole.

The SMMA evaluation study illustrates how this plays out. The study involves at minimum six entities across multiple jurisdictions in activities that include the collection of direct identifiers, passive behavioural monitoring, and administrative data linkage. Each entity's obligations attach to its own portion of this arrangement. eSafety assessed its privacy obligations by reference to the data it was itself to receive, not by reference to the data collected, used, and disclosed in the study it had commissioned. The fieldwork provider conducted a privacy threshold assessment of its own activities. On the evidence available, no entity assessed the privacy implications of the study as a whole before recruitment began. The problem is that data linkage across multiple entities creates privacy risks that do not belong to any single entity. The risks can only be assessed for the study as a whole, but each entity could plausibly treat itself as responsible only for its own piece. That this was possible is clearly undesirable.

The privacy impact assessment provision in the draft Code is the clearest illustration of the gap. Section 38 requires that an entity conduct a privacy impact assessment that includes a description of data flows, an assessment of whether the handling is consistent with the best interests of the child, and an assessment of the risk of harm to children. But nothing in section 38 requires that these assessments extend beyond the entity's own handling. The Code does not specify that an entity that commissions or designs an activity must assess the whole of that activity, even where it determines its scope and purpose. It fails to provide that a third-party assessment cannot discharge the entity's obligation. It does not require that the data flows described extend to every party in the arrangement, including downstream recipients, linkage partners, and offshore processors. Nor does it require an entity to assess whether children's personal information it obtains from third parties was collected in compliance with the Code. In a distributed activity, privacy impact assessments can therefore be conducted piecemeal while the whole activity goes unassessed. For the entities that will be subject to the Code, this is not the exception but the norm.[14]

The PIA provision is the most visible instance of this problem, but the gap is not limited to it. The Code's structure means that wherever an activity is distributed across parties, no entity is clearly responsible for the whole.

What is needed for effective enforcement

The Code creates substantial new individual privacy rights for children. Those rights are only meaningful if there is a remedy when they are not respected. Under the Act, a breach of the Code is an interference with privacy, enforced through the Commissioner's

14 Federal Trade Commission, *A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services*, September 2024, https://www.ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services; Pimienta, J. et al., 'Mobile apps and children's privacy: a traffic analysis of data sharing practices among children's mobile iOS apps', *Archives of Disease in Childhood* 108(11), 2023, 943–945, doi:10.1136/archdischild-2023-325960.

complaint-handling and investigation functions. The Code is, however, being introduced at a time when the OAIC has announced it will decline to investigate a larger number of privacy complaints, due in part to the growing volume it receives.[15] While the rationale of focusing resources where they can deliver broader change is defensible, the problem remains that the Code creates new privacy rights without a clear pathway for their enforcement. There is no general right of action except for serious interferences with privacy, and a refusal to investigate is reviewable on legality grounds only.

This raises a question the OAIC should address before the Code commences: what is the intended remedy for a child whose rights under this Code are not respected if the OAIC declines to investigate? The OAIC should set out clearly how the individual rights created by the Code will be enforced under its current model.

Effective enforcement also requires applying a consistent definition of personal information. Much of the data held by entities covered by the Code will be inferred data: behavioural profiles, interest categories, and algorithmic classifications derived from a child's activity. The OAIC's own published guidance is clear that such data is personal information where the individual is reasonably identifiable.[16] The Act itself defines personal information as information or an opinion about an identified individual, or an individual who is reasonably identifiable.[17] The information need not identify the child by itself; it is enough that the data is about the child and that the child is reasonably identifiable. In correspondence on privacy complaints, the OAIC has instead asked whether the information itself identifies the person, framing the question as "whether the requested information is about you, and could identify you or reasonably identify you," and on that basis treated inferred data as falling outside the definition.[18] If the same approach were applied to the data held by entities covered by the Code, the rights the Code creates would be significantly reduced before enforcement began.

Even where the definition is applied consistently, enforcement requires that non-compliance be visible. Section 39 requires entities to publish a register of privacy impact assessments, but transparency functions as a governance mechanism only if someone is looking. The eSafety example illustrates this. The agency already maintains a published PIA register, but until recently it contained a single entry, dated 2021, and the absence of

15 Carly Kind, 'Handling privacy complaints – a new approach for a new era', OAIC Blog, 2 March 2026, https://www.oaic.gov.au/news/blog/handling-privacy-complaints-a-new-approach-for-a-new-era.

16 OAIC, 'What is personal information?', https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/what-is-personal-information; OAIC, *Guide to data analytics and the Australian Privacy Principles*, https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/more-guidance/guide-to-data-analytics-and-the-australian-privacy-principles; OAIC, 'Guidance on privacy and the use of commercially available AI products', https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products; OAIC, 'Tracking pixels and privacy obligations', https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/tracking-pixels-and-privacy-obligations; OAIC, *Privacy Guidance on Part 4A (Social Media Minimum Age) of the Online Safety Act 2021*, https://www.oaic.gov.au/privacy/privacy-legislation/related-legislation/social-media-minimum-age.

17 Privacy Act 1988 (Cth), s 6(1).

18 OAIC, closure letters for complaints CP25/01766 (16 December 2025), CP25/01918 (17 December 2025), CP25/02442 (18 December 2025), and CP25/02490 (19 December 2025). Copies of the closure letters are available from the author on request.

any later entry prompted no apparent scrutiny.[19] Publication, in other words, does not by itself produce oversight. The OAIC must commit to auditing PIA registers proactively, contacting entities that appear not to be meeting their obligations, and exercising its powers where entities are potentially non-compliant.

The OAIC has committed to increasing transparency in its own decision-making processes, consistent with regulator best practice.[20] The recommendations in this section are consistent with that commitment and ask the OAIC to operationalise it specifically in the context of Code administration. The OAIC should publish annual data on complaints received under the Code by type and outcome, investigations initiated including own-motion investigations, determinations made, proactive monitoring activities undertaken including PIA register reviews, and use of compulsory information-gathering powers. Without this, the Code's protections are unverifiable from the outside. The OAIC should not ask children, parents, and the public to trust an enforcement architecture that is not visible to them.

19 Office of the eSafety Commissioner, 'Privacy Impact Assessment Register', archived 9 March 2026, https://webarchive.nla.gov.au/awa/20260309025908/https://www.esafety.gov.au/about-us/corporate-documents/privacy/privacy-impact-assessment-register.

20 OAIC, *Corporate Plan 2025–26*, https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/corporate-plans/corporate-plan-2025-26.