Dear OAIC,

Thankyou for the opportunity to contribute to the children's online privacy code.

In short, I suggest that additional consideration is given to:

- Clarifying community expectations on what is 'personal information'
- The importance of APP 2 – Anonymity and Pseudonymity, APP 3.5 and APP 12.
    - If the code will be sub-ordinate to the APPs, then that should be made clear. If it is not sub-ordinate, then not including an APP that is relevant risks the code being incomplete.
- Good Practices of many platforms that provide "near real time" access to personal information.

Sincerely,

[redacted]

Part 1 – Initial Response

Background – What is 'personal information' ?

Children, like everyone else want to have control of the information about them held by others ('Information privacy'[1]).

Such rights were incorporated into domestic Australian law in 1988 by the Commonwealth Parliament in Privacy Principles that form part of the Privacy Act 1988 (Cth), this law was significantly amended in 2000 and 2012.

These Privacy Principles are based on the principles in the OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (OECD Guidelines), having been adapted for Australia. They are now known as the Australian Privacy Principles.

Unfortunately, cases like Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4 at [2]; have seen the ambiguity in personal information interpreted in a manner aligned to "Breach of Confidence" actions in Equity; rather than preference being given to interpretations that deliver on Australia's obligations to the international treaty[2] and the parliament's purpose[3] (protecting privacy from erosion by information technology).

For any privacy code to be effective, the OAIC needs to clarify the definition of personal information. The success the OAIC claimed[4] (including the clarity of what is personal information) has been overridden be subsequent case law[5]. While Glass v Cessnock[6] is a welcome improvement in the interpretation of personal information, SM McAteer does not go far enough in his judgment to deliver on the Parliament's intent.

So you need to draw attention back to the intent of the Commonwealth Parliament

Commonwealth Parliament[7]	`Personal information' is widely defined to include anything-act, true or false, or opinion-that reasonably identifies an individual. Given the Explanatory Memoranda, I would suggest "act" is incorrectly reported and should be read as "fact".
ALRC Report 22[8]	Commission's Approach. For present purposes, there are three aspects of the definition of 'personal information' that need to be

[1] Australian Law Reform Commission, 'ALRC Report 22 - Privacy' [46], Volume 1.
[2] *Plaintiff S157/2002 v Commonwealth [2003] HCA 2* [29].
[3] 'Commonwealth, Parliamentary Debates, House of Representatives, Nov 1988, Lionel Bowen)' <URL Unavailable>.
[4] 'Update on the Federal Court Decision' <https://web.archive.org/web/20170306182506/https://www.oaic.gov.au/media-and-speeches/statements/privacy-commissioner-v-telstra-corporation-limited-federal-court-decision>.
[5] *GMW v Victoria Legal Aid (Human Rights) [2022] VCAT 922*.
[6] *Glass v Cessnock City Council [2024] NSWCATAD 292* [92-100].
[7] 'Commonwealth, Parliamentary Debates, House of Representatives, Nov 1988, Lionel Bowen)' (n 3).
[8] Australian Law Reform Commission (n 1) [1198], Volume 1.

	considered. The first concerns the relationship of the information in question with a natural person. (For reasons given in Chapter 1 ls, information about bodies corporate is not treated in this report as raising privacy issues.) Information about the credit rating of a sole trader is of as much concern to that trader as information about an ordinary individual's credit rating is to that individual. To limit the definition of 'personal information' to information relating to the 'personal affairs' of a person is too restrictive. There is room for doubt about the precise scope of that phrase? Any information about a natural person should be regarded as being personal information. Secondly, the link between the person and the information need not be explicit. If the information can be easily combined with other known information, so that the person's identity becomes apparent, the information should be regarded as personal information." Information should be regarded as being 'personal information' if it is information about a natural person from which, or by use of which, the person can be identified. Lastly, the Commission has reconsidered the question whether its proposals should be restricted to personal information kept in a systematic fashion, i.e. in a record system. It is true that most of the dangers to information privacy will come from the systematic processing of personal information. But not all will. In particular, the Commission's recommendations about the law of breach of confidence'* should not be so restricted. It would not be appropriate to restrict the class of personal information to which the Commission's general recommendations apply in the way the scope of the Commission's Discussion Paper was limited", although particular principles and controls may need to be so limited.
OECD Guidelines	The principles encompass all media for the computerised processing of data on individuals (from local computers to networks with complex national and international ramifications), all types of personal data processing (from personnel administration to the compilation of consumer profiles) and all categories of data (from traffic data to content data, from the most mundane to the most sensitive).

(Div 2) Consent

The division is useful, as it provides clarity on the operation of APP3.5; which from my experience appears to be very poorly understood; expecting non legal practitioners to apply the legal process of statutory interpretation (e.g. the principle of legality) means the benefits of the legislation are unlikely to be realised and the general public is likely to be confused. This is certainly what has happened so far, and it goes well beyond the general public being confused.

While the Privacy Act states that consent is explicitly required for the collection of sensitive personal information; the operation of APP3.5 requires that the method of collection is lawful and fair; and APP3.6 that requires that information is collected from the person.

Typically, the method of collection requires consent (express or implied); the Commonwealth and State Parliaments' considered how consent is obtained in online environments with the enactment of the Electronic Transactions Acts (e.g. Electronic Transactions Act 1999 (Cth), and in particular s15B (and equivalent in sections in the state based acts).

APP 3.6 requires that information must be collected from the person with their knowledge and not from their device in the background (or covertly). This APP has seen limited consideration in any complaints.

When recording personal information using a "device", the community's attitudes (dislike) with regards to recording what people are doing is reflected in statutes that deal with recording what people are doing – typically these are the state based Surveillance Devices acts. It is important here to note gaps in coverage across states, as some states sill only have listening device statutes that do not include optical, location (trackers), or data surveillance devices.

When recording personal information using a person's computer in the background (aka covertly), it is necessary to consider the rights of the person in possession of the device to have control over its operation. The common law offers 'tresspass to chattles' and there are criminal statutes, which again lack of uniformity in relation to offences involving computers and extremely limited prosecution of such offences hampers an understanding of this in online environments.

It is recommended that you make reference to these in children's online privacy code, and/or check it for consistency with relevant acts.

(Div 4/s30) Requests for Access

This section is incredibly weak and not aligned to 'good practices'.

Many applications include the ability for you to download a copy of your information. This is quite a reasonable practice in 2026; and far better for consumers and children that having to manually request it and wait up to 60 days.

I would suggest that you undertake some research on the general availability of such mechanisms consider what is offered by platforms like Facebook, LinkedIn.

This would enable you to strengthen this section so that it is better suited to consumer needs, including responsiveness requirements.

(Div 4/s31) Requests for Correction

Again, this section is incredibly week, 30 to 60 days is far too slow a response time.

(Div 5/s32) Requests to Destroy

Requests to Destroy, are closely linked with APP11.2 and APP2.

By virtue of recording information about a person, you are eroding their privacy.

As noted, many applications offer no real privacy choices and the information about what does or doesn't work if personal information isn't provided, or cookies are disabled or javascript is turned off is so vague that it provides no value to the child using a platform.

So requests to destroy must be considered in this light; again 30 to 60 days is far too slow a response time.

(Div 6/s33) Geolocation Data

Geolocation data can be particularly problematic for vulnerable children with complex parenting arrangements and for example various orders of the family court.

I would suggest further consideration is given to this section, including leveraging APP 2 to protect children with complex parenting arrangements.

(Div 7/s35) Information about children's privacy rights

Again, you should be clear here, these are 'information privacy rights' and you should not restrict or narrow these rights to collect, use and disclose.

People should have access to information about how their personal information is secured; how it is deleted when it is no longer required, et al.

(Div 8) Privacy impact assessments and privacy education and training.

For this section, I think it would be reasonable to require the providers of platforms to have appropriate security and risk management systems and training for the software developers, ICT staff and management.

You should also consider staff with incidental access; which is included in many Child Safe Standards, the Child Safe Standards[9] developed by the Commission for Children and Young People and especially Standard 9[10].

---

[9] 'Child Safe Standards' <https://ccyp.vic.gov.au/child-safe-standards/the-11-child-safe-standards/>.
[10] 'Child Safe Standards - Standard 9: Physical and Online Environments Promote Safety and Wellbeing While Minimising the Opportunity for Children and Young People to Be Harmed.' <https://ccyp.vic.gov.au/child-safe-standards/the-11-child-safe-standards/standard-9/>.

Part 2 - Roundtable Questions

Opening Queston – Clarification

- Are there any aspects of the exposure draft you would like us to walk through or clarify before we begin?

What is personal information and what is information privacy are not consistently understood in legal circles, let alone the community. This was demonstrated with the Grubb Matters that culminated in the Full Federal Court[11]. Glass v Cessnock[12] has adopted some of the Full Federal Court's obiter.

Q0 – Scope – What is the purpose of information privacy ?

To protect privacy from erosion by IT.

Q1 - Scope - What is personal information ?

OECD Guidelines: Personal Data (equivalent to personal information) any information about a person.

ALRC Report 22: Any information related to a person, from which the person can be identified or which can be combined with other information to identify the person.

Cth Parliament - Any information related to a person.

Online – Williams and Roxon.

Adequate for Trade with Europe – Williams.

Vic Parliament – Saw personal information as a superset of personal data.

Full Federal Court – Narrow, 'about' interpreted similar to 'personal affairs', breach of confidence actions in equity, akin to 'delicate information'.

NSWCATAD – Interpreted liberally.

Q2 - Scope - What is information privacy ?

Information Privacy are the rights of a person to control the information about them help by others. These are defined by the Parliament in the APPs, and not to be defined by the courts; other than interpreting the parliament's intent.

Q3 – Scope - What about other APPs (incl Security) ?

---

[11] *Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4*.
[12] *Glass v Cessnock City Council [2024] NSWCATAD 292* (n 6).

General Response

Does it achieve the Right Balance while remaining workable ?

Given that very limited impact that I have seen privacy legislation have due to the scope issues mentioned earlier, additionally privacy requires organisations to go out of their way for their customers.

The Bunnings case illustrates this – the failure to provide notice was a breach of privacy as well as Surveillance Devices Acts which have far harsher penalties.

As there has been little to no enforcement action by the OAIC, organisations are unprepared for this.

They are well and truly capable of solving any issues; however it will take time and effort to upskill.

My interactions with the OAIC over the OAIC's own website illustrate the problems – the OAIC is unwilling to forego "user experience" data, is unwilling to offer an "opt out" or "opt in", like the UK ICO is.

In short, this is too little too late – by over 26 years.

Unworkable

There will be "push back" from industry; however as the purpose of this Privacy Act was to regulate IT (w.r.t personal information/personal data).

As the Privacy Act has never been used to this effect, there will be culture shock.

Integration with other laws – Surveillance Devices Act and lack of uniformity, Crimes Acts (OPD and Computer Crimes).

Lack of awareness of the issues; and lack of interest by regulators. Despite the Victorian Parliament's work and ALRC Reports 22, 108, 112, 123.

Gaps

A number of APPs (e.g. Security, Anonymity, Collecting from the person, rather than (covertly from) the device) are not covered, it is unclear how the Code operates with respect to the broader act.

In general, it lacks an understanding of the origins of the Act, ALRC Report 22, the OECD Guidelines, and Parliament's intent including updates in 2000 and 2012.

There is no requirement to provide people with access to a copy of their personal information in a automated fashion (e.g. self service, per Facebook and other platforms).

It doesn't address the requirements for Collection Notices to be "good faith"; rather than the current efforts which seek to bury information about what is being done because people may not like it; or the organisation itself does not understand.

No consideration of "privacy of attention" – annoying pop ups or choices that don't offer good privacy defaults (see privacy by design), poor user experience/user interface design.

Certainty

Some organisations will "push back" that it is not prescriptive and/or does not tell them exactly what to do.

In general, I also expect "push back" from Privacy Officers and Legal Practitioners over workload.

In general, there is also a lack of legal understanding of the application of the law to online platforms, including models where the client device (and associated property rights are taken into account).

This requires consideration of property rights (trespass to chattles, computer crimes, obtaining property by deception (Vic) – issuing unauthorised instructions to a computer).

Specific Obligations

It is all implementable; however as this requires organisations to do something for their customers benefit, I don't see organisations being motivated to do much at all – other than complain about red tape that is finally starting to be enforced.

Commencement and Implementation

I'd expect a handful of companies that this applies to are aware of these developments.

The OAIC has never delivered on the Parliament's intention' and as such information privacy remains a curiosity; rather than something to be complied with and taken seriously.

A key challenge that many organisations will face, is that there development road maps are full and until this is registered, organisations are unlikely to commit to doing anything based on a draft – without significant awareness and promotion.

Regulatory Coherence

The Privacy Act is intended to operate alongside other acts, particularly with the method of collection, that is required to be lawful.

While consent isn't required to collect ordinary personal information; most methods of collection require consent – ask a question, if I answer it – that is implied consent. Again, this is very poorly understood in the community.

Few commercial organisations have legal authority to compel answers, like law enforcement. However, typically if you want the service, you have to give up your personal information (and substantially more than you would think).

The APP that requires collection via fair and lawful means, is akin to the Legality Principle of Statutory Interpretation. The Privacy Act doesn't explicitly require consent; however it doesn't authorise anything illegal.

In terms of regulatory coherence, any work that you are doing is not going to be co-herent unless you consider:

Electronic Transactions Acts

Computer Crimes in the Crimes Acts

Surveillance Devices Acts.