AUSTRALIAN COUNCIL ON CHILDREN AND THE MEDIA

PO Box 1240, Glenelg South SA 5045
ABN: 16 005 214 531
Phone: (08) 8376 2111 **Fax:** (08) 8376 2122

Web: www.childrenandmedia.org.au **E-mail:** info@childrenandmedia.org.au

REVIEW OF THE PRIVACY ACT 1988:

COMMENTS ON DISCUSSION PAPER JANUARY 2022

Thank you for the opportunity to provide a submission to the timely and important review into Australian privacy law.

ACCM is the national peak not-for profit body representing the interests of children as media consumers. Its mission is to support families, industry and decision makers in building and maintaining an enjoyable media environment that fosters the health, safety and wellbeing of Australian children. Its membership includes major national and state education, welfare and parent organisations and individuals.

ACCM's core business is to collect and review research and information related to children and the media; to provide information and advice on the impact on children of print, electronic and screen-based media; to provide reviews of current movies and apps from a child development perspective; to advocate for the needs and interests of children in relation to the media; and to conduct and act as a catalyst for relevant research.

The chief aim of the ACCM submission to the Issues Paper is to provide input as to how this review of Australian privacy law and principles can best address the special privacy rights and needs of children (as expressed in UN *General Comment 25 on Children's Rights in Relation to the Digital Environment* (2021)).

In particular, ACCM's comments are informed and motivated by what we have learnt about popular apps used by children and their overt and covert tracking behaviours and consequent invasions of children's privacy. The findings of ACCM's 2021 project *Apps can trap: privacy tips and checks* can be found here https://childrenandmedia.org.au/app-reviews/apps-can-trap-tracking.

This submission can be posted on the review website.

Further information about this submission can be obtained from

ACCM Hon CEO Barbara Biggins OAM CF 08 83762111, bbiggins@ozemail.com.au or ACCM President Prof Elizabeth Handsley FAAL. handsley.elizabeth@gmail.com

This submission sets out

a) short-answer responses to the Proposals outlined in the Issues Paper and
b) fuller responses to the issues outlined in Chapter 13 *Children and vulnerable individuals*

Section 1 Complete list of proposals

Part 1: Scope and application of the Act

1. Objects of the Act

1.1 Amend the objects in section 2A, to clarify the Act's scope and introduce the concept of public interest, as follows:

(a) to promote the protection of the privacy of individuals *with regard to their personal information*, and

(b) to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities *undertaken in the public interest*.

ACCM supports these proposals.

2. Definition of personal information

2.1 Change the word 'about' in the definition of personal information to 'relates to'.

2.2 Include a non-exhaustive list of the types of information capable of being covered by the definition of personal information.

2.3 Define 'reasonably identifiable' to cover circumstances in which an individual could be identified, directly or indirectly. Include a list of factors to support this assessment.

2.4 Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.

2.5 Require personal information to be anonymous before it is no longer protected by the Act.

2.6 Re-introduce the Privacy Amendment (Re-identification) Offence Bill 2016 with appropriate amendments.

ACCM supports all these proposals given that children spend many hours in technical environments, including apps, which collect overtly or covertly a range of information which can be used to target children commercially. (See https://childrenandmedia.org.au/app-reviews/apps-can-trap-tracking.)

3. Flexibility of the APPs

3.1 Amend the Act to allow the IC to make an APP code on the direction or approval of the Attorney-General:

- where it is in the public interest to do so without first having to seek an industry code developer, and
- where there is unlikely to be an appropriate industry representative to develop the code

ACCM's view is that the IC should be mandated to make all APP Codes that apply to children. The industry's track record in making Codes that put the interests of children first does not inspire confidence.

3.2 Amend the Act to allow the IC to issue a temporary APP code on the direction or approval of the Attorney-General if it is urgently required and where it is in the public interest to do so.

3.3 Amend Part VIA of the Act to allow Emergency Declarations to be more targeted by prescribing their application in relation to:

- entities, or classes of entity
- classes of personal information, and
- acts and practices, or types of acts and practices.

3.4 Amend the Act to permit organisations to disclose personal information to state and territory authorities when an Emergency Declaration is in force.

ACCM supports Proposals 3.2 to 3.4.

Part 2: Protections

8. Notice of collection of personal information

8.1 Introduce an express requirement in APP 5 that privacy notices must be clear, current and understandable.

ACCM submits that such notices should be required to be understandable to people of the likely age of the users of the product. See further in comment on Chapter 13.

8.2 APP 5 notices limited to the following matters under APP 5.2:

- the identity and contact details of the entity collecting the personal information
- the types of personal information collected
- the purpose(s) for which the entity is collecting and may use or disclose the personal information
- the types of third parties to whom the entity may disclose the personal information
- if the collection occurred via a third party, the entity from which the personal information was received and the circumstances of that collection

- the fact that the individual may complain or lodge a privacy request (access, correction, objection or erasure), and
- the location of the entity's privacy policy which sets out further information.

ACCM supports these proposals, especially with the insertion in dot point 4, of the requirement for the entity to supply a list of such third party entities.

8.3 Standardised privacy notices could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording and icons. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised notices.

ACCM supports this proposal and discusses it further in comments on Chapter 13.

8.4 Strengthen the requirement for when an APP 5 collection notice is required – that is, require notification at or before the time of collection, or if that is not practicable as soon as possible after collection, unless:
- the individual has already been made aware of the APP 5 matters; or
- notification would be *impossible* or would involve *disproportionate effort*.

ACCM supports this proposal.

9. Consent to the collection, use and disclosure of personal information

9.1 Consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.

9.2 Standardised consents could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording, icons or consent taxonomies. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised consents.

ACCM supports these proposals.

10. Additional protections for collection, use and disclosure of personal information

10.1 A collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.

ACCM would add "and necessary for the function of the product".

10.2 Legislated factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances could include:

- Whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances
- The sensitivity and amount of personal information being collected, used or disclosed
- Whether an individual is at foreseeable risk of unjustified adverse impacts or harm as a result of the collection, use or disclosure of their personal information
- Whether the collection, use or disclosure is reasonably necessary to achieve the functions and activities of the entity
- Whether the individual's loss of privacy is proportionate to the benefits
- The transparency of the collection, use or disclosure of the personal information, and
- If the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child.

ACCM supports these proposals.

10.3 Include an additional requirement in APP 3.6 to the effect that that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3.

Commissioner-issued guidelines could provide examples of reasonable steps that could be taken, including making reasonable enquiries regarding the collecting entities' notice and consent procedures or seeking contractual warranties that the information was collected in accordance with APP 3.

10.4 Define a 'primary purpose' as the purpose for the original collection, as notified to the individual. Define a 'secondary purpose' as a purpose that is directly related to, and reasonably necessary to support the primary purpose.

ACCM supports these proposals.

11. Restricted and prohibited acts and practices

11.1 **Option 1**: APP entities that engage in the following restricted practices must take reasonable steps to identify privacy risks and implement measures to mitigate those risks:

- Direct marketing, including online targeted advertising on a large scale
- The collection, use or disclosure of sensitive information on a large scale
- The collection, use or disclosure of children's personal information on a large scale
- The collection, use or disclosure of location data on a large scale
- The collection, use or disclosure of biometric or genetic data, including the use of facial recognition software
- The sale of personal information on a large scale
- The collection, use or disclosure of personal information for the purposes of influencing individuals' behaviour or decisions on a large scale
- The collection use or disclosure of personal information for the purposes of automated decision making with legal or significant effects, or

- Any collection, use or disclosure that is likely to result in a high privacy risk or **risk of harm to an individual.**

ACCM supports this option, subject to replacing “a large” with “any” in dot point 3.

Option 2: In relation to the specified restricted practices, increase an individual’s capacity to self-manage their privacy in relation to that practice.

Possible measures include consent (by expanding the definition of sensitive information), granting absolute opt-out rights in relation to restricted practices (see Chapter 14), or by ensuring that explicit notice for restricted practices is mandatory.

12. Pro-privacy default settings

12.1 Introduce pro-privacy defaults on a sectoral or other specified basis.

- **Option 1** – Pro-privacy settings enabled by default: Where an entity offers a product or service that contains multiple levels of privacy settings, an entity must pre-select those privacy settings to be the most restrictive. This could apply to personal information handling that is not strictly necessary for the provision of the service, or specific practices identified through further consultation.
- **Option 2** – Require easily accessible privacy settings: Entities must provide individuals with an obvious and clear way to set all privacy controls to the most restrictive, such as through a single click mechanism.

ACCM supports Option 1, as this offers better protection for children.

13. Children and vulnerable individuals

13.1 Amend the Act to require consent to be provided by a parent or guardian where a child is under the age of 16. The Review is seeking additional feedback on whether APP entities should be permitted to assess capacity on an individualised basis where it is practical to do so. The Review is also seeking feedback on the circumstances in which parent or guardian consent must be obtained:

- **Option 1** - Parent or guardian consent to be required before collecting, using or disclosing personal information of the child under the age of 16.
- **Option 2** - In situations where the Act currently requires consent, including before the collection of sensitive information or as an available mechanism to undertake a secondary use or disclosure of personal information.

The assumed age of capacity would also determine when a child may exercise privacy requests independently of their parents, including access, correction or erasure requests.

ACCM supports Option 1, and strongly opposes the use of assessing capacity of children on an individual basis. We discuss these issues further in our comments on Chapter 13.

13.2 Require APP 5 notices to be clear, current and understandable, *in particular for any information addressed specifically to a child*.

ACCM supports this proposal and discusses it further in our Chapter 13 comments.

14. Right to object and portability

14.1 An individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information.

On receiving notice of an objection, an entity must take reasonable steps to stop collecting, using or disclosing the individual's personal information and must inform the individual of the consequences of the objection.

ACCM supports this proposal.

15. Right to erasure of personal information

15.1 An individual may only request erasure of personal information where one of the following grounds applies, and subject to exceptions:

- the personal information must be destroyed or de-identified under APP 11.2
- the personal information is sensitive information
- an individual has successfully objected to personal information handling through the right to object (see Chapter 14)
- the personal information has been collected, used or disclosed unlawfully
- the entity is required by or under an Australian law, or a court/tribunal order, to destroy the information, and
- the personal information relates to a child and erasure is requested by a child, parent or authorised guardian.

ACCM supports these proposals.

15.2 Provide for exceptions to an individual's right to erasure of personal information. An APP entity could refuse a request to erase personal information to the extent that an exception applied to either *all or some* of the personal information held by an APP entity.

15.3 An APP entity must respond to an erasure request within a reasonable period. If an APP entity refuses to erase the personal information because an exception applies, the APP entity must give the individual a written notice that sets out the reasons for refusal and mechanisms available to complain about the refusal, unless unreasonable to do so.

ACCM supports proposal 15.3 but in regard to 15.2, ACCM believes there should be no exceptions to children's right to erasure.

16. Direct marketing, targeted advertising and profiling

16.1 The right to object, discussed at Chapter 14, would include an unqualified right to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing. An individual could still request not to receive direct marketing communications from an organisation. If an organisation provides marketing materials to an individual, it must notify the individual of their right to object in relation to each marketing product provided.

On receiving notice of an objection, an entity must stop collecting, using or disclosing the individual's personal information for the purpose of direct marketing and must inform the individual of the consequences of the objection.

16.2 The use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions must be a primary purpose notified to the individual when their personal information is collected.

16.3 APP entities would be required to include the following additional information in their privacy policy:

- whether the entity is likely to use personal information, alone or in combination with any other information, for the purpose of influencing an individual's behaviour or decisions and if so, the types of information that will be used, generated or inferred to influence the individual, and
- whether the entity uses third parties in the provision of online marketing materials and if so, the details of those parties and information regarding the appropriate method of opting-out of those materials.

ACCM broadly supports these proposals, but notes that such objections from users can only occur if the entity has made a clear and conspicuous statement in its privacy policy / website/ other communication that such activity occurs.

16.4 Repeal APP 7 in light of existing protections in the Act and other proposals for reform.

ACCM supports this proposal only if elsewhere it is stated clearly that "if an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing". This is of importance in light of the practice (used by the developers of apps) of collecting and transferring children's data to advertising-linked companies. See

https://www.comparitech.com/blog/vpn-privacy/app-coppa-study/

and https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf

and refer to ACCM's 2021 project *Apps can trap: privacy checks of top 50 android apps for children* https://childrenandmedia.org.au/app-reviews/privacy-check/all

Proposals 17-19

No comment.

20. Organisational accountability

20.1 Introduce further organisational accountability requirements into the Act, targeting measures to where there is the greatest privacy risk:

- Amend APP 6 to expressly require APP entities to determine, at or before using or disclosing personal information for a secondary purpose, each of the secondary purposes for which the information is to be used or disclosed and to record those purposes.

ACCM supports this proposal.

22. Overseas data flows

22.1 Amend the Act to introduce a mechanism to prescribe countries and certification schemes under APP 8.2(a).

22.2 Standard Contractual Clauses for transferring personal information overseas be made available to APP entities to facilitate overseas disclosures of personal information.

22.3 Remove the informed consent exception in APP 8.2(b).

22.4 Strengthen the transparency requirements in relation to potential overseas disclosures to include the countries that personal information may be disclosed to, as well as the specific personal information that may be disclosed overseas in entity's up-to-date APP privacy policy required to be kept under APP 1.3.

22.5 Introduce a definition of 'disclosure' that is consistent with the current definition in the APP Guidelines.

22.6 Amend the Act to clarify what circumstances are relevant to determining what 'reasonable steps' are for the purpose of APP 8.1.

ACCM supports these proposals.

Proposal 23.

No comment.

Part 3: Regulation and enforcement

24. Enforcement

24.1 Create tiers of civil penalty provisions to give the OAIC more options so they can better target regulatory responses including:

- A new mid-tier civil penalty provision for any interference with privacy, with a lesser maximum penalty than for a serious and repeated interference with privacy.

- A series of new low-level and clearly defined breaches of certain APPs with an attached infringement notice regime.

24.2 Clarify what is a 'serious' or 'repeated' interference with privacy.

24.3 The powers in Part 3 of the Regulatory Powers (Standard Provisions) Act 2014 (Regulatory Powers Act) would apply to investigations of civil penalty provisions in addition to the IC's current investigation powers.

24.4 Amend the Act to provide the IC the power to undertake public inquiries and reviews into specified matters.

24.5 *Amend paragraph 52(1)(b)(ii) and 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss. The current provision could be amended to insert the underlined:*

- a declaration that the respondent must perform any reasonable act or course of conduct to identify, mitigate and redress any actual or reasonably foreseeable loss or damage suffered by the complainant/those individuals.

24.6 *Give the Federal Court the power to make any order it sees fit after a section 13G civil penalty provision has been established.*

24.7 Introduce an industry funding model similar to ASIC's incorporating two different levies:

- A cost recovery levy to help fund the OAIC's provision of guidance, advice and assessments, and
- A statutory levy to fund the OAIC's investigation and prosecution of entities which operate in a high privacy risk environment.

24.8 *Amend the annual reporting requirements in the AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground.*

24.9 Alternative regulatory models

- **Option 1** - Encourage greater recognition and use of EDRs. APP entities that handle personal information could be required to participate in an EDR scheme. APP entities that are not part of a recognised EDR scheme could be required to pay a fee for service to the OAIC as the default complaint handling provider if a complaint is made against them.
- **Option 2** - Create a Federal Privacy Ombudsman that would have responsibility for conciliating privacy complaints in conjunction with relevant EDR schemes.
- **Option 3** - Establish a Deputy Information Commissioner – Enforcement within the OAIC.

ACCM supports 24.1 to 24.6, and 24.8 and 24.9. It has no view on the options.

However we oppose 24.7. For a regulatory system to operate genuinely in the public interest it should be funded from the public purse. So-called 'cost recovery' systems tend to create conflicts of interest, and also risk engendering a client-type relationship with the regulator.

Proposal 25

ACCM has no comment.

26. A statutory tort of privacy

26.1 **Option 1**: Introduce a statutory tort for invasion of privacy as recommended by the ALRC Report 123.

26.2 **Option 2**: Introduce a minimalist statutory tort that recognises the existence of the cause of action but leaves the scope and application of the tort to be developed by the courts.

26.3 **Option 3**: Do not introduce a statutory tort and allow the common law to develop as required. However, extend the application of the Act to individuals in a non-business capacity for collection, use or disclosure of personal information which would be highly offensive to an objective reasonable person.

26.4 **Option 4:** In light of the development of the equitable duty of confidence in Australia, states could consider legislating that damages for emotional distress are available in equitable breach of confidence.

ACCM supports Option 1.

Proposals 27-28

ACCM has no comment.

Section 2: Chapter 13 Children and vulnerable individuals

ACCM strongly supports measures to address the need for enhanced privacy protections for children, noting the absence to date of effective protections and the significant harms for children that continue to result from their frequent interactions with social media and with apps that gather their data and transfer to others, all too often covertly.

1. The development of an OP Code.

ACCM notes that the new Act will require the development of an OP Code, and that such a Code will need to set out how all OP organisations will meet privacy requirements in relation to children.

The Code, or section of it, which deals with children must be developed by the OAIC in consultation with Australian children's organisations with expertise in this area.

The development of the Code should not be given to industry, which has an inherent conflict of interests when it comes to the kind of restraint needed to protect children's interests. ACCM's experience over many years, with codes developed by the advertising and free-to-air television industries in Australia, provides strong support for scepticism as to whether the industry is likely to bring to the task an understanding of likely harms to children, and a recognition of the need to word such codes carefully so that they offer real and effective protections.

1.1 Defining a child

ACCM notes that the new Bill will define a child as a person under the age of 18. We support this approach as it is consistent with the Convention on the Rights of the Child.

1.2 Consent and capacity

In ACCM's submission, the ideal position would be that informed parental consent be required before an entity collects, uses or discloses personal information relating to any child under the age of 16 years. This should apply to all collections of children's personal information and to all APP entities. Any request for parents to give consent must be accompanied by clear and precise information about the types of information that will be collected and how it will be used.

Regarding children's own consent, they have varying abilities to know and understand risks associated with their use of social media and apps, and, more importantly, varying capacity to apply such knowledge effectively when presented with a specific scenario. ACCM questions the suggestion that the *Gillick* competency test could be used to determine which children have the capacity to consent to the collection of their data and which not, especially in an online context. This test was developed for use in in medical contexts where a professional has direct dealings with an individual child. This is how the professional is able to form the requisite judgment as to the child's maturity and understanding. In social media and online app environments there is no analogous relationship, and therefore no judgment-forming capacity. Indeed, the 'judgment' is likely to be made by an algorithm.

1.3 Age and consent verification

ACCM recommends the following paper as providing a useful discussion of methods of effectively verifying the age of child users, and of parental consent. https://euconsent.eu/project-deliverables/ see 5th paper September 21

ACCM also suggests that the conditions for obtaining effective consent should include:

- That it is sought before any use commences
- The accompanying provision of clear and unambiguous information is lacking any deception about what such consent allows
- The consent being limited in application to, say, one year
- Being subject to the right of withdrawal
- Being accompanied by a right of refusal

1.4 Notification of the collection of personal information

ACCM supports the proposed requirement for APP 5 notices to be clear, current and understandable to all and especially to children.

ACCM also supports a requirement that such notices incorporate diagrams, cartoons, graphics, video and audio content which can make such information to support understanding by all.

With regard to the above, ACCM notes the success of the long-time use of such symbols to signal particular types of content in the National Classification Scheme. The Netherlands classification system uses a combination of symbols for classification categories and content pictograms to signal types of risks https://www.kijkwijzer.nl/english. This article describes the process of developing such privacy icons https://edpl.lexxion.eu/data/article/14703/pdf/edpl_2019_03-010.pdf

ACCM recommends the uses of content pictograms in privacy policy statements to signal the types of privacy data to be collected, and how they are to be used, if consent granted.

2. Limits on the collection, uses and disclosure of children's personal information

2.1 ACCM calls for limits on the collection of children's data where such collection is detrimental to the best interests of children. The protection of children's best interests should not only rely on parents'

willingness/abilities to use or understand privacy policies: some content and practices should not be collected/ used with children.

ACCM recommends that the OAIC issue a list of acts and practices which would not meet the test of "fair and reasonable". Such excluded acts and practices should include:

- online tracking, behavioural monitoring and profiling of children (see ACCM's research on tracking practices at Appendix 1);
- the disclosure of a child's personal information to a third party which exposes the child to potential safety or privacy risks;
- the sale of a child's personal information; and
- the ongoing retention of children's data once their use of a service ceases.

****

APPENDIX 1: PRELIMINARY FINDINGS FROM *Apps can trap* PROJECT

Between June and November 2021, ACCM worked with the US research firm AppCensus to provide to an Australian audience, analyses of the data collection and tracking practices of the Android apps most popular with children.

A total of 175 apps were analysed and the results published on ACCM's website. See https://childrenandmedia.org.au/app-reviews/privacy-check/all

These analyses include whether the app grants "dangerous permissions" and whether used, and also whether the app collects and passes on sensitive data and to whom. For a fuller explanation of the system see https://childrenandmedia.org.au/assets/files/apps-can-trap/A-guide-to-the-AppCensus-system-final.pdf

An example of data collection and transfer can be seen here https://childrenandmedia.org.au/app-reviews/apps/abcmousecom where the user's Android Advertising ID (AAID) was collected and passed on to advertising-linked companies Unity Technologies and Adjust.

The analysis of the app *Icecream cone cupcake* https://childrenandmedia.org.au/app-reviews/apps/icecream-cone-cupcake-baking-maker-chef shows transfer of the user's AAID to 5 ad-linked companies.

ACCM has now analysed the level of tracking found in the list of 175 apps checked so far. The level of data collected and transferred to advertising-linked companies is disturbing.

Of the 175 apps, 68 (39%) transferred Android Advertising Identfiers (AAID) to at least one advertising-related company. Of the 68 apps, 28 apps transferred data to 3 or more such companies, placing children at risk of increased marketing approaches.

Of note, while most of these 68 apps came from a diverse range of developers/distributors, 6 such groups had 3 or more apps that could be classed as risky in relation to transfer of advertising data linked to the child user. Many of these 28 apps were aimed at young children.

As ACCM receives more app analyses, and continues to analyse this growing data base, there will be more findings of note which support ACCM's and community concerns about the business models of Big Tech. Children's privacy is being invaded with little effective action taken to date to prevent it.