MONASH University

MONASH LAW

CASTAN CENTRE FOR HUMAN RIGHTS LAW

Attorney-General's Department Review of the Privacy Act 1988

Submission in relation to the Exposure Draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 ('Online Privacy Bill')

Prepared by
Prof. Moira Paterson and Assoc. Prof. Normann Witzleb

On behalf of the Castan Centre for Human Rights Law
Faculty of Law, Monash University

6 December 2021

I. Introduction

1. The Castan Centre for Human Rights Law of Monash University's Faculty of Law is a world-renowned academic centre using its human rights expertise to create a more just world where human rights are respected and protected, allowing people to pursue their lives in freedom and with dignity. The Castan Centre's mission includes the promotion and protection of human rights, and it is from this perspective that we make this submission.

2. The Castan Centre thanks the Attorney-General's Department for the opportunity to make a submission in relation to the Exposure Draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 ('Online Privacy Bill' or 'draft Bill').

3. We welcome the proposal to introduce a new code of practice about online privacy ('OP code') as a third category of binding privacy codes under the Privacy Act. This is an important step in addressing the many challenges to the protection of individuals' privacy posed by the data handling practices of social media and online platforms.

4. Due to time limitations, this submission will focus only on selected issues arising from the exposure draft of the Online Privacy Bill.

II. Who would the OP Code apply to?

5. We broadly support the definitions in the Online Privacy Bill of 'OP organisations'. However, we are concerned that the definition of social media platforms as 'organisations that provide an electronic service that has the ***sole or primary purpose*** of enabling online social interaction' may leave some unintended gaps.

6. We query whether this definition would apply to educational, gaming and fitness and similar platforms that allow users to interact with one another. Edutech platforms such a ClassDojo or learning management systems such as Blackboard arguably have as their primary purpose the provision of online educational content. However, they also allow users to have online social interaction between users and collect large volumes of personal data from users. This collected data includes both content data (in the form of messages, postings and self-produced educational or assessment content) and metadata about the time, frequency and modes of interaction with the platform. Similarly, gaming platforms can be said to have the provision of games as their primary purpose, but they also often allow users to interact and collect substantial amounts of personal data from users about their interactions or their gaming activity. Similar arguments could also be made for fitness tracking platforms with social media capabilities. We suggest that organisations that run such platforms should be subject to the OP code.

7. We therefore submit that it should be examined further whether the formulation of '***sole or substantive purpose***' should be substituted for *'sole or primary purpose'*. Such a modification might help to clarify that platforms whose primary purpose lies in the provision of (different

kinds of) user services, but who invite and generate substantial social interaction on their platforms, will also be covered by the definition of OP organisation.

III. Requirements of the proposed OP code

8. We support the recommendations for code inclusions in the *Digital Platforms Inquiry Report* of the Australian Competition and Consumer Commission ('DPI Report')[1] and submit that they are justified by the detailed evidence of information asymmetries and potential consumer harms outlined in that report. The latter are of increasing concern in the context of Big Data and the increased use of AI both to target individuals and to make decisions that can impact adversely on them.

9. We note that the Online Privacy Bill does not always fully reflect the recommendations of the DPI Report. **Where there are differences, we recommend a reconsideration of the Online Privacy Bill**.

10. We further note a number of other issues arising from draft provisions concerned with enhancing the privacy protection of children and vulnerable individuals. These issues are discussed further below.

1. Information requirements

11. Clause s26KC(2)(c) of the draft Bill requires that the OP code must 'make provision for, or in relation to, requiring an OP organisation to notify an individual, or to otherwise ensure that the individual is aware, of the purposes for which the organisation collects, uses and discloses personal information'. This current wording in cl. 26KC(2)(c) of the draft Bill fails to address the issue of complexity in privacy notices, identified by the DPI Report, and would benefit from the **inclusion of requirements for multi-layered notices** as outlined in recommendation 18(1) of the DPI Report.

12. We welcome the requirements in s26KC(2)(g), including the requirement in (i) that notifications must be 'clear and understandable' but believe that the legislation should provide **more guidance** as to how OP organisations could achieve this.

    In particular, the DPI Report made various recommendations for strengthening the notice and consent requirements, especially with regard to children. Recommendation 16(b) called for the amendment of notice obligations in APP5 to require notices to consumers to be 'concise, transparent, intelligible and easily accessible, written in clear and plain language, provided free of charge, and clearly set out how the APP entity will collect, use and disclose the consumer's personal information'. It recommended in respect of children that:

[1] Australian Competition and Consumer Commission, *Digital Platforms Inquiry*, Final Report (June 2019) ('DPI Report').

'Where the personal information of children is collected, the notice should be written at a level that can be readily understood by the minimum age of the permitted digital platform user'.[2]

However, given that it is proposed that consent needs to be provided by a parent or guardian of a child if the child is under 16 years of age, any notice given to that child does not serve directly to inform consent. Nonetheless, the thrust of this recommendation is commendable as it enhances transparency and the opportunities for children to learn about the uses their data is put to and to become informed agents in privacy matters. We submit that OP organisations should therefore be **required to set out how they will comply with the notice standards recommended by the DPI Report**.

2. Consent

13. We welcome the requirements in s26KC(2)(e) of the draft Bill that the OP code should specify what is required for consent to qualify as voluntary, informed, unambiguous and specific – and also to deal with the issue of currency of consent, including in relation to sensitive information.

14. However, in view of the power asymmetries between OP organisations and consumers as well as the extent and breadth of potential harms that can arise from inappropriate uses of consumers' personal data, we submit that the legislation should go further and **require 'opt-in controls for any data collection that is for a purpose other than the purpose of supplying the core consumer-facing service**', as recommended by the DPI Report,[3] at least in relation to children and other vulnerable individuals but preferably across the board.

    We recommend that

    - **in the case of personal information that does not qualify as 'sensitive information', the limitation in APP 3.2 that limits solicitation and collection of personal information to what is reasonably necessary for one or more of its functions or activities should be applied so that solicitation or collection is limited to what is directly necessary for the OP organisation's consumer-facing activities in absence of specific and informed opt-in to such further solicitation or collection**.
    - **In the case of the collection of sensitive information, the OP organisation should be required clearly to distinguish between the information that is required for the direct provision of the consumer-facing activity and the information that is required for other purposes and to obtain separate consent for each of these**.

15. Furthermore, we would recommend in relation to both our proposed opt-in and in respect of consent that **the notice should make clear where the information collected includes geolocation information and information to be used for the purposes of profiling.**

[2] Ibid, p 461.
[3] Ibid, rec 18(2).

3. Ceasing to use or disclose personal information upon request

16. In principle, we welcome the new requirement in s26KC(2)(h) to 'take such steps (if any) as are reasonable in the circumstances to not use or disclose, or to not further use or disclose' an individual's personal information upon request from that individual. However, as the Early Assessment – Regulation Impact Statement makes clear,[4] this requirement is not intended to amount to a 'right to erasure' of the personal information and will not prevented permitted secondary uses.

17. We submit that this requirement falls behind international best practice. Under the California Consumer Privacy Act, consumers have a qualified right to request deletion of their data. This permits a consumer to request a business or service provider to delete personal information collected by the business from the consumer if it is no longer necessary for the business or service provider to maintain that information for one of more specified purposes.[5] Allowing individuals to retrieve volunteered personal information once it is no longer required, is especially important in relation to children who may have volunteered their information without fully understanding the full implications of doing so. The EU General Data Protection Regulation likewise has a more expansive right to erasure in its art. 17. We submit that the protections under Australian law should be **strengthened to allow a request of deletion of personal data**, rather than merely a requirement on OP organisations to take reasonable steps to no longer use and disclose data.[6]

4. Children

18. We **support** the Online Privacy Bill's approach of elevating the protections for children from guidance given by the Office of the Australian Information Commissioner to requirements under the OP code.

19. We **support** the definition of a 'child' as an 'individual who has not reached 18 years' because it is in line with the approach under UN Convention on the Rights of the Child.

5. Age verification

20. We note the proposed requirement in cl. 26KC(6)(a) that an OP organisation must 'take all reasonable steps to verify the age of individuals to whom the OP organisation provides an electronic service'.

21. We have concerns that this provision requires an OP organisation to verify the age of all users, including its adult users. In our view this is overly broad, likely to be burdensome, and unnecessarily privacy invasive. There is also no such requirement in comparable overseas

[4] Australian Government, Attorney-General's Department, *Enhancing online privacy and other measures*, Early Assessment – Regulation Impact Statement (October 2021), p 15.
[5] California Civil Code § 1798.105(a).
[6] See also DPI Report, rec. 16(d), which proposed to give a consumer a qualified right to request APP entities to erase the personal information of that consumer.

legislation, such as the US COPPA[7] or the EU GDPR.[8] It is sufficient to identify which users are children and to which age brackets they belong to.

22. In our view it would be preferable instead to establish a requirement to take all reasonable steps to **verify**
    (1) whether an individual is below or above the age of 18 years; and
    (2) if below or likely to be below the age of 18 years, to verify
        a. whether the individual is above or below the of 16 years; and
        b. if below or likely to below the age of 16 years, to determine the age bracket.

23. This modified approach would better express the legislative policy that an OP organisation take reasonable steps to verify which of their users are children and therefore enjoy special protections under the proposed changes to the Privacy Act and under the proposed OP code. It would also clarify that there is no need for OP organisation to take reasonable steps to verify the age of adult users.

24. This modified approach would also ensure that an OP organisation take reasonable steps to identify which of their users are above and below the age of 16 years, respectively. This knowledge is necessary because of the requirements in cl. 26KC(6)(b) and (c) to seek the consent of a parent or guardian of a child who has not reached 16 years.

25. This modified approach would furthermore ensure that an OP organisation takes reasonable steps to identify the age bracket to which a child user under the age of 16 years belongs. This knowledge is necessary to identify what further protections of the child's data are necessary having regard to the requirement in cl. 26KC(6)(f) of adopting 'fair and reasonable' data practices that 'have the best interest of the child as the primary consideration'. Ideally, this provision should be complemented elsewhere in the legislation by a requirement to fashion protections for children by reference to their age-specific needs, interest and capacities. Relevant overseas design codes also rely on age brackets to identify children's vulnerabilities and need for protection.[9]

6. Age limit for parental/guardian consent

26. We note that the specified age of 16 is higher than that currently provided for under the OAIC's guidance, which creates a presumption that child aged 15 and above has capacity to consent. We **welcome** setting a general age limit of 16 years.

27. However, we have some concern that the requirement for parental/guardian consent is now so rigid. In our view, there should be some recognition of children's increasing agency in line

[7] COPPA requires that requires that operators provide notice to parents, and get their verifiable consent, where operators 'have actual knowledge that they are collecting personal information online from a child under 13 years of age'.
[8] The GDPR art. 8 has a requirement that 'controller shall make reasonable efforts to verify [where consent is the legal basis of data processing in relation to information society services directly offered to a child and a child is under 16 years or other age between 13 and 15 years, as Member States prescribe] that consent is given or authorised by the holder of parental responsibility over the child'.
[9] See, eg., Information Commissioner's Office (UK), *Age appropriate design: a code of practice for online services*, Annex B.

with child rights standards which call for respect for the evolving capacities of children. As we noted previously:[10]

> While recognising the special vulnerabilities of children arising from their physical and mental development is important, viewing children entirely as vulnerable can lead to unintended consequences of eroding children's rights. The idea that parental consent is an appropriate substitute for a child's consent until they turn 18 is indeed difficult to reconcile with the premise that data protection and privacy laws safeguard personal autonomy. […]

28. The Online Privacy Bill substitutes the age of 16 years as the relevant age of consent. However, there may still be data practices that are straightforward to understand or of limited risk or significance, such that children even under the age of 16 years have the capacity to consent.

29. We therefore submit that the consent of the parent or guardian of a child is not required, **if**
(i) the child has reached the age of 14 years of age but is under 16 years;
(ii) the child consents; and
(iii) the child has demonstrably developed the required capacity to consent, having regard to
    a. **the child's age, experience and understanding,**
    b. **the type and complexity of the data practice in question,**
    c. **the notice provided to the child, and**
    d. **the consequences that the practice has for the child.**

7. Circumstances in which parent or guardian consent must be obtained

30. In our view, the current wording of the draft Bill does not make clear the circumstances and effect of the consent obtained from a parent or guardian. In particular, it is unclear whether such consent needs to be obtained only once (other than in cases of cl. 26KC(2)(e)(ii)) and then potentially provides a lawful basis of all collections, uses and disclosures of personal information identified in the notice or whether it has a more limited effect.

31. We note that the Privacy Act review seeks feedback on the circumstances in which parent or guardian consent must be obtained. It identifies two options, as follows:

    - 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.

32. We assume that it will be the Privacy Act in its amended form – rather than the OP code – that will spell out what consent is required for and what effect (if any) it will have. However,

[10] Lisa Archbold, Damian Clifford, Moira Paterson, Megan Richardson and Normann Witzleb, 'Adtech and Children's Data Rights' (2021) 44(3) *UNSW Law Journal* 857, 869.

if this is not the case, we submit that the Online Privacy Bill needs to **make clearer the context in which consent will operate** and its proposed effect.

8. Data processing must be 'fair and reasonable'

33. We support the approach adopted in cl. 26KC(6)(e) and (f) that requires OP organisations to ensure that the collection, use and disclosure of personal information of children must be 'fair and reasonable in the circumstances', and that the 'best interest of the children [is] the primary consideration'.

34. Indeed, we submit that this requirement that data processing must be 'fair and reasonable in the circumstances' should **be extended to all data subjects, whether children or adults**.

9. Child rights impact assessment and participation of children in design

35. It has been noted in General Comment No 25 to the UN Convention on the Rights of the Child that the digital environment provides crucial opportunities for children to participate in society and to 'be effective advocates for their rights, individually and as a group'.[11] This includes the policy level where 'data privacy' regulation affecting children is formulated, but should also extend to requiring organisations to conduct children's rights impact assessments and seek input from children in relation to how they view specific practices.

36. We therefore submit that OP organisations should be required to engage in **child rights impacts assessments**, where such entities are likely process to a substantial amount process personal information of children.

37. We also encourage the Office of the Australian Information Commissioner to engage with children during the process of developing and approving the OP code to ensure that children's views are considered and **recommend that the draft Bill should lay down such a requirement**.

10. Protection of vulnerable individuals

38. The Discussion Paper states that the OP code will require 'organisations to follow stricter rules about handling the personal information of children and other vulnerable groups'. However, the draft Bill makes no explicit reference to vulnerable groups. The only exception to this is cl. 26KC(5)(a)(ii), which requires OP organisations to address the 'specific protections for individuals physically or legally incapable of giving consent to the collection, use of disclosure of personal information'.

[11] United Nations, Committee on the Rights of the Child, *General Comment No. 25 (2021) on children's rights in relation to the digital environment*, para. 16 (p 3).

39. We are concerned that this is likely to provide only very limited protection to vulnerable individuals.

40. First, individuals may be vulnerable also in circumstances where they are not physically or legally incapable of giving consent. We submit that the current very narrow focus and definition of vulnerability fails to protect a large number of individuals who may be capable of giving consent but are nonetheless vulnerable to harm from inappropriate or exploitative data practices. We would accordingly recommend that the OP code should adopt a factor-based definition of vulnerability that relies on a non-exhaustive list of risk factors, modelled on approaches adopted by the eSafety Commissioner, in the Banking Code of Practice and the General Insurance Code of Practice 2020.[12]

41. Second, the Online Privacy Bill does not seem to establish, or require, any substantive protection of individuals in vulnerable circumstances. This differs from the situation of children. Children are also considered vulnerable and are protected through the requirement that the handling of their personal data must be 'fair and reasonable', having regard to their best interest as the primary consideration.

42. We note that the Discussion Paper suggests that '[f]urther consideration of how the Act and APPs should apply to particular groups of people, including any additional or different protections for vulnerable adults, could be undertaken as part of developing the OP code'.[13]

43. However, we submit that the Online Privacy Bill should itself contain further measures to protect vulnerable adults. The approach of 'principles-based' regulation in the Privacy Act allows for vulnerability to be considered as an aspect of fairness. For example, APP 3.5 imposes a requirement on APP entities to solicit and collect personal information only by 'fair and lawful means'.[14] It could be considered unfair if an entity collect data from vulnerable individuals through exploitation of their vulnerability. This is implicitly recognised in the APP Guidelines, which give as examples of unfair collection practices that personal information is collected 'from an individual who is traumatised, in a state of shock or intoxicated' or 'in a way that disrespects cultural differences'.[15]

44. Following on from our proposal above (see para 33 and 34) that the 'fair and reasonable' requirement should be extended to the handling of all personal information, including that of adults, we submit further that the Online Privacy Bill for the OP Code should include **the following factors to be considered in determining whether a collection, use or disclosure is fair and reasonable in the circumstances:**
    - **Any information the OP organisation has, or ought to have, about the likely vulnerabilities of their users**.

[12] For detail, see Monash University and elevenM Consulting, *Privacy risks and harms for children and other vulnerable groups in the online environment: Research paper commissioned by the Office of the Australian Information Commissioner* (December 2020).
[13] Discussion Paper, p 110.
[14] *Privacy Act* 1988 (Cth), Australian Privacy Principle 3.5.
[15] Office of the Australian Information Commissioner, *APP Guidelines* (July 2019), para 3.63.

- **The appropriateness in the circumstances of enquiring about or verifying whether a user is vulnerable in a particular way before processing their information.**
- **Any privacy harms that could result from processing and any measures that could be taken to prevent them**.

45. We would also recommend inclusion in the draft Bill of the following further measures which are drawn from our detailed report into the area, *Privacy risks and harms for children and other vulnerable groups in the online environment: Research paper commissioned by the Office of the Australian Information Commissioner* by Monash University and elevenM Consulting, December 2020:[16]
    - **The Code should require that any privacy notices required to be provided to an individual who is known to have limited capacity also be provided to a nominated supporter or decision maker, where one exists.**
    - **The Code should require that privacy policies and privacy controls be provided in formats that are accessible, according to current, generally accepted accessibility standards or guidelines.**

46. Finally, we would also stress that the best way of ensuring protection for vulnerable individuals is to provide for robust privacy standards and that our recommendations above would be an important step in this direction.

[16] This report is published on the OAIC website at https://www.oaic.gov.au/__data/assets/pdf_file/0012/11136/Report-Privacy-risks-and-harms-for-children-and-other-vulnerable-groups-online.pdf.