



Phone: 1300 00 6842
Email: enquiries@ovic.vic.gov.au
PO Box 24274
Melbourne Victoria 3001

29 March 2023

Attorney-General's Department

By email only: privacyactreview@ag.gov.au

Dear Review team,

Submission in response to the Attorney-General's Department's Privacy Act Review Report

I am pleased to make a submission in response to the Attorney-General's Department's *Privacy Act Review Report (Report)*.

My office, the Office of the Victorian Information Commissioner (**OVIC**), is the primary regulator for information privacy, information security and freedom of information in Victoria, administering both the *Privacy and Data Protection Act 2014 (PDP Act)* and the *Freedom of Information Act 1982 (Vic)*. As such, I have a strong interest in matters that impact information rights.

I commend the Attorney-General for the breadth of work that has gone into conducting the review of the *Privacy Act 1988 (the Act)* and releasing this report. My office considers that many of the proposal put forward in this report will strengthen Australia's privacy framework, offering stronger protections for individuals' privacy rights and holding entities more accountable for their information handling practices.

Definition of personal information

Replacing 'about' with 'relates to'

1. OVIC supports the proposal to broaden the definition of personal information in the Act by replacing the word 'about' with the phrase 'relating to'.¹
2. The amended definition would capture the wider range of information which can be used to identify an individual such as inferred information and technical data such as location data and IP addresses. The proposal would also bring the Act into closer alignment with global privacy frameworks such as the General Data Protection Regulation (**GDPR**).

¹ Report, page 27, proposal 4.1.

Meaning of 'collection'

3. OVIC is pleased to see the proposal to amend the definition of 'collection' to expressly include information 'obtained from any source and by any means, including inferred or generated information'.² As discussed in OVIC's submission to the Privacy Act Review Discussion paper (**previous submission**)³, this expansion will further align the protection of personal information with both community expectations and leading global privacy law.

De-identified information

4. OVIC supports the proposal to amend the definition of de-identified information to make it clear that de-identification of personal information is not a permanent state but rather a process applied to personal information that involves treating it in such a way that no individual is identifiable or reasonably identifiable in the current context.
5. Further, given the inherent risk of re-identification, OVIC also supports the proposal to extend specific protections in the Act to de-identified information. This includes the requirement for APP entities to take reasonable steps to protect de-identified information from misuse, loss, unauthorised access, modification and reidentification among others. It also includes the requirement to ensure an overseas recipient of de-identified information does not breach the APPs.
6. Finally, OVIC is pleased to see the proposal to extend the protections applied to the use of personal information for targeting purposes, to the use of de-identified information for targeting purposes.

Definition of sensitive information

7. OVIC supports the proposal to broaden the definition of sensitive information by, among other things, replacing the word 'about' with 'relates to' and clarifying that sensitive information can be inferred from information that is not sensitive information. As discussed in our previous submission, information such as location or transaction information can reveal sensitive attributes about individuals.⁴ It is positive to see proposed measures to adequately protect this type of information.

Emergency declarations

Proposal for targeted emergency declarations

8. OVIC supports the proposal to amend Part VIA of the Act to make an emergency declaration (ED) more targeted by restricting its application to specific entities, or classes of entity,

² Report, page 30, proposal 4.3.

³ OVIC *Submission in response to the Attorney-General's Discussion Paper*, (December 2021), pages 1-2 available at: <https://ovic.vic.gov.au/wp-content/uploads/2022/01/Submission-Privacy-Act-Review-Discussion-Paper-December-2021.pdf>.

⁴ *Ibid*, page 2, paragraph 8 – 9.

types of personal information, and particular types of acts and practices.⁵ In OVIC's view, this amendment would allow entities regulated under the Privacy Act (**APP entities**) to better strike a balance between being responsive to an emergency and protecting individuals' privacy.

Responsibility for making emergency declarations

9. OVIC understands that Part VIA of the Act allows the Prime Minister or a Minister to make an ED if they are satisfied that an emergency or disaster has occurred, it is of national significance, and it has affected one or more Australian citizens.⁶
10. As noted in OVIC's previous submission, given the Australian Information Commissioner (**the Commissioner**) has oversight over the Act and given the privacy impacts of EDs on individuals, it may be more appropriate for the Commissioner to hold the power to make EDs or alternatively require that EDs only be made in consultation with the Commissioner.

Making EDs in relation to ongoing emergencies

11. OVIC acknowledges the importance and benefits of information collection, use and disclosure in facilitating government responses to emergencies, including ongoing emergencies such as pandemics. In relation to the proposal to ensure EDs can be made in relation to ongoing emergencies,⁷ OVIC is of the view that periodic review of the ED would be important to ensure individuals' right to privacy is protected through the duration of the declaration.

Employee records exemption

12. OVIC is pleased to see the intention to enhance privacy protections afforded to employees.⁸ However, OVIC considers that the proposed protections may not afford a sufficient level of privacy protection for employees given the sheer volume and variety of personal information employers often collect from employees.⁹ As noted in OVIC's previous submission, removing this exemption would align the Act with community and employee expectations, whilst also improving public trust and confidence in employers' information handling practices.¹⁰

⁵ Report, page 51, proposal 5.3.

⁶ *Privacy Act 1988* (Cth), s 80J.

⁷ Report, page 51, proposal 5.4.

⁸ Report, page 71, proposal 7.1.

⁹ For examples of harms arising from interferences with employees' records, see OVIC's *Submission in response to the Privacy Act Review Issues Paper*, (20 November 2020), available at <https://ovic.vic.gov.au/wp-content/uploads/2021/08/Privacy-Act-review-Submission.pdf>.

¹⁰ OVIC *Submission in response to the Attorney-General's Discussion Paper*, (December 2021), page 3, paragraph 13-14 available at: <https://ovic.vic.gov.au/wp-content/uploads/2022/01/Submission-Privacy-Act-Review-Discussion-Paper-December-2021.pdf>.

Political parties' exemption

13. OVIC recognises the political parties' exemption under the Act is intended to encourage freedom of political communication and enhance the operation of electoral and political processes in Australia. However as noted in the Report, the exemption is instead serving to undermine the integrity of the democratic electoral process.¹¹
14. The exemption currently enables political parties to avoid being transparent in their information handling practices. This raises significant concerns around the handling of voters' personal information, particularly given the documented history of political parties misusing voters' personal information for targeted campaigning.¹² There are also concerns around the security of personal information held by political parties, and the possibility for cyber-attacks or foreign interference in elections, as political parties are not currently required to implement robust information security measures to protect that information.
15. OVIC strongly recommends the political parties' exemption be removed entirely. Its removal would not inherently limit any freedom of political communication and political parties could still communicate with constituents within the framework of the Act, but it would require them to become more transparent and accountable for their information handling practices. The removal of the exemption would also more closely align the Act with comparable global privacy frameworks.
16. However, should the exemption be retained, OVIC considers it important that it is narrowed in scope and operation to strengthen the protection of individuals' personal information.
17. To that end, OVIC supports the proposal to include registered political parties within the scope of the Act and within the scope of the exemption in section 7C of the Act.¹³ This would ensure they are required to comply with the APPs when handling personal information for purposes other than purposes covered by the exemption. While the proposal does not fully address the concerns with the ways in which registered political parties handle voters' information, it would require them to be accountable for the collection, use and disclosure of personal information for non-political purposes which is a positive.
18. OVIC supports the proposal to require political entities to publish a privacy policy which provides transparency in relation to acts or practices covered by the exemption.¹⁴ Additionally, OVIC supports the proposal to apply the fair and reasonable test to political acts and practices covered by the exemption.¹⁵ This proposal would compel political parties

¹¹ Report, page 73.

¹² Ben Grubb, 'Craig Kelly texts show need for spam, privacy reform: experts', InnovationAus (1 September 2021) available at <https://www.innovationaus.com/craig-kelly-texts-show-need-for-spam-privacy-reform-experts/>; Lucy Gray, 'Craig Kelly backs bill to stop unsolicited political texts', Nine News (25 October 2021) <https://www.9news.com.au/national/unsolicited-text-messages-craig-kelly-will-support-legislationbanning/8a642933-75fa-47e3-a28d-65c7b6c734fe>.

¹³ Report, page 74, proposal 8.1.

¹⁴ Report, page 75, proposal 8.2.

¹⁵ Report, page 79, proposal 8.3(a).

to turn their minds to the impact that their information handling practices may have on individuals.

19. OVIC is supportive of the proposal to explicitly prohibit political entities from engaging in targeted campaigning based on sensitive information or traits relating to an individual.¹⁶ The practice of targeting individuals based on their personal and sensitive information negatively impacts democracy by inhibiting informed political debate and potentially restricting voters' ability to make informed decisions, so OVIC welcomes any proposal aimed at addressing this issue.
20. OVIC notes the proposal to require political entities to provide a mechanism for individuals to opt-out of their personal information being used or disclosed for direct marketing, and receiving targeted advertising.¹⁷ This proposal takes a positive step towards reducing the misuse of voters' personal information for targeted campaigning.
21. OVIC supports the proposal to extend the data security obligations in APP 11 to personal information held for the purpose of the exemption. Given the amount of personal information held by political entities, it is crucial they be required to implement adequate measures to protect it.¹⁸
22. However, rather than requiring political entities to only comply with some of the obligations in the APPs, OVIC considers individuals' privacy would be better protected if they were required to comply with all the APPs in relation to all their information handling practices. OVIC considers that the political parties' exemption does not serve any valid public interest.

Notice of collection of personal information

23. OVIC is pleased to see the proposed introduction of an express requirement in APP 5 that collection notices be 'clear, up-to-date, concise, and understandable'.¹⁹ As outlined in OVIC's previous submission, providing notice plays an essential role in individuals' ability to make informed choices and provide consent by enabling individuals to understand how their personal information will be collected, used and disclosed.²⁰

Consent to collection, use and disclosure of personal information

24. OVIC supports the proposal to amend the definition of consent so that it specifies the elements that must be met for consent to be valid. The proposed definition would set the standard of consent required for APP entities to collect, use and disclose information thereby requiring them to be more transparent about their information handling practices. This would enable individuals to exercise more meaningful choice and control over how

¹⁶ Report, page 79, proposal 8.3(b).

¹⁷ Report, page 81, proposal 8.4.

¹⁸ Report, page 83, proposal 8.5.

¹⁹ Report, page 97, proposal 10.1.

²⁰ See *OVIC's Submission to the Privacy Act Review Discussion paper* (21 December 2021), page 4, available at: <https://ovic.vic.gov.au/wp-content/uploads/2022/01/Submission-Privacy-Act-Review-Discussion-Paper-December-2021.pdf>.

their personal information is handled by organisations which would help address the power imbalance between individuals and APP entities.

25. OVIC also supports the proposal to recognise an individual's right to withdraw consent to the collection, use or disclosure of their information. This is discussed further below.
26. Importantly, consent should not be the primary basis for authorising information handling practices. While strengthened consent requirements would address some of the limitations of the current consent model, it should be supported by additional obligations on entities to have fair and reasonable information handling practices.

Fair and reasonable information handling practices

27. OVIC supports the proposal to introduce a requirement in the Act that the collection, use and disclosure of personal information by APP entities be fair and reasonable in the circumstances.²¹ OVIC also supports the proposal that this requirement apply irrespective of whether the APP entity has obtained consent for the collection, use or disclosure.²²
28. While there are proposed reforms to improve the quality of privacy policies, collection notices and consent, this is not enough to address the current and emerging risks of the digital age. As noted in OVIC's previous submission and in the Report, the APPs do not adequately protect against APP entities collecting, using or disclosing information in a way that harms an individual's privacy.²³
29. Amongst other things, this proposal would serve as a check to APP entities engaging in practices such as inappropriate personalised targeted advertising, marketing to children or other vulnerable groups and discriminatory algorithmic decision-making.
30. Further, the proposal would help shift the burden of protecting privacy to APP entities. Individuals should not bear the main responsibility of determining whether an APP entity's information handling practices pose a risk to privacy, as they currently do.

Rights of the individual

31. OVIC supports the proposal to introduce enhanced rights for individuals including the right to access and explanation, to object or withdraw consent to collection, use and disclosure, and to erasure.
32. As the Report notes, the current obligations on APP entities provide individuals limited transparency and control over their personal information.²⁴ The current notice and consent model is not an effective way for individuals to control how APP entities handle their

²¹ Report, page 116, proposal 12.1.

²² Report, page 121, proposal 12.3.

²³ See *OVIC's Submission to the Privacy Act Review Discussion paper* (21 December 2021), page 6, available at: <https://ovic.vic.gov.au/wp-content/uploads/2022/01/Submission-Privacy-Act-Review-Discussion-Paper-December-2021.pdf>.

²⁴ Report, page 166.

personal information, particularly given the complexities of new and emerging technologies and the evolving ways in which personal information is used.²⁵

33. The right of access and explanation will require APP entities to give individuals more meaningful information about the entities' information handling practices. This will enable individuals to make well informed decisions about the handling of their information, including enabling individuals to properly exercise the right to object or withdraw consent to an information handling practice.
34. OVIC notes the exercise of these rights would be subject to exceptions such as where there is a competing public interest, where exercising the rights would be contrary to law or where it would be technically impossible, frivolous or vexatious. OVIC is broadly supportive of this proposal to ensure the protection of individuals' privacy is balanced against the interests of APP entities in carrying out their functions and activities.
35. OVIC is pleased to see the proposed requirement for APP entities to notify individuals about these rights and how to exercise them, including providing reasonable assistance to individuals to assist in the exercise of their rights.²⁶

Automated decision making

36. OVIC supports the proposals aimed at increasing transparency about the use of automated decision making. As discussed in OVIC's previous submission, Artificial Intelligence can provide a range of benefits for the public, but it can also pose significant risks to privacy including perpetuating biases and augmenting existing inequalities.²⁷
37. Thus, the proposed requirement for privacy policies to set out the types of information that will be used in substantially automated decisions which have a legal, or similarly significant effect on an individual's rights is positive. So too is the proposed introduction of a right for individuals to request meaningful information about how substantially automated decisions which have a legal, or similarly significant effect are made.

Children's privacy

38. It is pleasing to see the Report recognise the lack of specific privacy protections for children and make multiple proposals to strengthen the protection of children's privacy in Australia.

²⁵ For discussion on the limitations of the current notice and consent model, see *OVIC Submission to the Privacy Act Review Discussion paper* (21 December 2021), page 5, available at: <https://ovic.vic.gov.au/wp-content/uploads/2022/01/Submission-Privacy-Act-Review-Discussion-Paper-December-2021.pdf>.

²⁶ Report, pages 183-184, proposal 18.8 and 18.9.

²⁷ See *OVIC Submission to the Privacy Act Review Discussion paper* (21 December 2021), page 8, available at: <https://ovic.vic.gov.au/wp-content/uploads/2022/01/Submission-Privacy-Act-Review-Discussion-Paper-December-2021.pdf>. See also Rebecca Heilweil, 'Why algorithms can be racist and sexist', *Vox* (online, February 18 2020) available at: <https://www.vox.com/recode/2020/2/18/21121286/algorithms-bias-discrimination-facial-recognition-transparency>; Annie Brown, 'Biased algorithms learn from biased data: 3 kinds of biases found in AI datasets', *Forbes* (online, February 7 2020) available at: <https://www.forbes.com/sites/cognitiveworld/2020/02/07/biased-algorithms/?sh=47aeadc476fc>.

As stated in OVIC's previous submission, OVIC broadly supports the introduction of measures to strengthen privacy protections for children and young people.²⁸

39. OVIC supports Proposal 16.2 requiring APP entities to rely on the OAIC's guidance in relation to children and young people and their capacity to consent to the collection, use and disclosure of information.²⁹ Whether the assumed age of capacity is 15 or 16, OVIC considers that it should be consistent for all APP entities, which this proposal should ensure.
40. However, OVIC notes that the assumed age of capacity may not necessarily be adequate in the eyes of young people. For example, members of OVIC's Youth Advisory Group (YAG)³⁰ have expressed concern that Australia's current primary and secondary curriculums do not provide enough privacy education to ensure young people have a sufficient understanding of the possible privacy impacts of the collection, use and disclosure of their personal information. Consequently young people may not develop sufficient capacity to provide valid consent by the age of 15 or 16.
41. OVIC is pleased to see the proposal to expressly require collection notices and privacy policies be clear and understandable, particularly when they are targeted to children.³¹ YAG members have stated on multiple occasions that privacy policies and collection notices, particularly in relation to online services such as social media, are written at a difficulty level that is almost impossible for young people to understand and makes them particularly vulnerable to the inappropriate collection, use and disclosure of their personal information.
42. It is pleasing to see the Report discusses the use of visual communication and infographics as possible tools to increase the accessibility of collection notices and privacy policies for young people.³² YAG members have stated that tools such as infographics and animated videos have the potential to increase both the accessibility of collection notices and privacy policies and the likelihood of young people taking time to read them rather than simply ticking the 'I agree' box.
43. OVIC supports the proposal to require APP entities to take into account the best interests of the child when considering whether the collection, use and disclosure of a child's personal information is fair and reasonable.³³ Not only would this place the needs of the children at the forefront, but it would also assist in aligning Australia's privacy protection for children with international frameworks such as the UK Age Appropriate Design Code.

²⁸ See OVIC *Submission to the Privacy Act Review Discussion paper* (21 December 2021), page 7, available at: <https://ovic.vic.gov.au/wp-content/uploads/2022/01/Submission-Privacy-Act-Review-Discussion-Paper-December-2021.pdf>.

²⁹ Report, page 150.

³⁰ OVIC's Youth Advisory Group (YAG) is comprised of 8 to 12 young Victorians aged between 15 and 22. The YAG advises the Information Commissioner on privacy issues affecting young people, assists OVIC in its engagement with children and young people in Victoria, and provides input into the development and delivery of privacy materials targeted towards this cohort. Further information about YAG is available at: <https://ovic.vic.gov.au/privacy/for-the-public/youth-advisory-group/>.

³¹ Report, Page 151, proposal 16.3.

³² Ibid.

³³ Report, page 153, proposal 16.4.

44. Given the significant amount of time children and young people spend online in both their educational and personal lives, it is positive to see the proposal to introduce a Children’s Online Privacy Code (**the Code**) that would prioritise and strengthen the privacy protection of young Australians.³⁴ OVIC supports the proposed requirement for the developer of the Code to consult broadly with relevant stakeholders, including children, parents, child development experts and the eSafety Commissioner. OVIC and the YAG would also welcome the opportunity to be consulted in the development of the Code.

Direct marketing, targeted advertising and profiling

45. As discussed in OVIC’s previous submission, targeted advertising poses a significant risk not just to individuals’ privacy but to society and democracy.³⁵ Amongst other harmful practices, it has normalised online tracking and consumer profiling, facilitated the growth of misinformation and disinformation, and discriminatory algorithmic decision making. Often these practices are driven by the collection and sharing of individuals’ personal information without their knowledge or in ways they would not reasonably expect.

46. Given this, OVIC welcomes proposals to strengthen the regulation of direct marketing, targeting and other related harms.

47. OVIC supports the proposal to give individuals an absolute right to opt out of their personal information being used or disclosed for direct marketing and the proposal to opt-out of receiving targeted advertising.³⁶ This would give individuals more control over the collection, use and disclosure of their personal information and align with community expectations of how APP entities should handle their information.

48. OVIC also supports the proposals to prohibit direct marketing to a child unless the personal information was collected directly from the child and the direct marketing is in the child’s best interests. Further, OVIC supports the proposal to prohibit targeting to a child unless it is in the child’s best interests.

49. OVIC considers that the proposal to require any targeting to be fair and reasonable would further protect individuals’ privacy rights. In addition, the proposal to require entities to be more transparent about targeting, and the use of algorithms and profiling to recommend content to individuals would hold APP entities more accountable for their information handling practices. OVIC supports these proposals.

Interaction with State and Territory regulatory schemes

50. OVIC recognises privacy legislation enacted in states and territories may not always be equivalent to the Act and the disparity may cause confusion and additional compliance burdens where an APP entity may be subject to both the Act and a state privacy law. OVIC is

³⁴ Report, page 157, proposal 16.5.

³⁵ See *OVIC Submission to the Privacy Act Review Discussion paper* (21 December 2021), page 7-8, available at: <https://ovic.vic.gov.au/wp-content/uploads/2022/01/Submission-Privacy-Act-Review-Discussion-Paper-December-2021.pdf>.

³⁶ Report, page 212 - 214, proposal 20.2 and 20.3.

OFFICIAL

therefore broadly supportive of the proposal to establish a Commonwealth, state and territory working group to harmonise privacy legislation, focussing on key areas of concern.³⁷

Thank you once again for the opportunity to provide comment on the Report. My office will continue to watch the progress of the review with interest and looks forward to any further opportunities to provide input into the review.

I have no objection to this submission being published by the Attorney-General's Department without further reference to me. I also propose to publish a copy of this submission on the OVIC website, but would be happy to adjust the timing of this to allow the Department to collate and publish submissions proactively.

If you have any questions about this submission, please do not hesitate to contact me directly or my colleagues Anita Mugo, Senior Policy Officer at anita.mugo@ovic.vic.gov.au or Jenna Daniel, Senior Policy Officer at jenna.daniel@ovic.vic.gov.au.

Yours sincerely



Sven Bluemmel
Information Commissioner

³⁷ Report, page 303, proposal 29.3.