Office of the Victorian Information Commissioner

t 1300 006 842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D21/21968

21 December 2021

Attorney-General's Department

By email only: PrivacyActReview@ag.gov.au

Dear Review team,

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

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

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).

I have broadly organised my comments around each theme and the related questions contained in the Discussion Paper.

Definition of personal information

Replacing 'about' with 'relates to'

1. OVIC supports the proposal to broaden the definition of personal information in the *Privacy Act 1988* (**Privacy Act**) by replacing the word 'about' with the phrase 'relating to' so that personal information is defined as 'information or an opinion *relating to* an identified individual, or an individual who is reasonably identifiable'.

2. This alternative wording captures a wider range of information including technical data such as location data, online identifiers, and inferred information. In OVIC's view, this proposal avoids the need to list types of information capable of being considered personal information, retaining a technology neutral definition. It would also align the Privacy Act more closely with global privacy frameworks like the General Data Protection Regulation (**GDPR**), the California Consumer Privacy Act and Canada's Personal Information Protection and Electronic Documents Act.

3. OVIC acknowledges that updating the definition of personal information will likely result in increased compliance costs for entities regulated under the Privacy Act (**APP entities**) as they may need to modify their systems and information handling practices. However, OVIC is of the view that the public interest in providing more comprehensive and meaningful privacy protection by amending the definition of personal information outweighs concerns about compliance costs.

Meaning of collection

4. OVIC notes the proposal to amend the definition of collection to include circumstances where an APP entity 'infers, derives, generates or otherwise creates personal information, whether or not

this is done by or on behalf of an individual'.[1] This complements the proposed expansion to the definition of personal information and will further align the protection of personal information with community expectations and leading global privacy law.

5. Crucially, while it is important to ensure clarity around the types of personal information covered by the Act, and to enhance protections around the collection of personal information, OVIC considers it is the uses of personal information which pose the most significant risks to the privacy of individuals. For example, it is appropriate for APP entities to collect and use IP addresses for fraud and crime prevention purposes. However, APP entities that use IP addresses for commercial purposes such as micro-targeting pose serious risks to individuals' privacy. This is discussed in detail further below.

6. Introducing this alternative wording may also help to deal with the emerging problem of inferences derived by artificial intelligence (**AI**) from otherwise de-identified data. While this problem is emerging, OVIC suggests it would be useful to guide government and industry toward acceptable uses of AI rather than relying only on further legislation to deal with this issue.

Definition of sensitive information

7. Sensitive information is a subset of personal information that covers specific categories of information set out in the Privacy Act.[2] OVIC notes the proposed amendment to the definition of personal information to include inferred personal information would also apply to inferred sensitive information.

8. OVIC notes the comments in the discussion paper regarding the intrusive nature of information such as location or transactional data, and its capacity to reveal sensitive attributes about individuals such as religious beliefs and health information.[3] In many instances this data can be collected without an individual's knowledge or consent,[4] and contrary to community expectations.

9. Given this, OVIC sees benefit in expanding the definition of sensitive information to include information capable of being used as a proxy for sensitive information. Information capable of exposing or revealing sensitive attributes are equally deserving of stronger protections on collection, use and disclosure. For instance, location information, regularly collected by numerous mobile applications, wearable devices, and by platforms such as Google, Amazon, and Facebook, can reveal an individual's gender, political affiliations, health conditions and other intimate details about their life.[5]

Emergency declarations

Proposal for targeted emergency declarations

10. It is pleasing to see the proposal to amend Part VIA of the Privacy Act to make an emergency declaration (**ED**) more targeted by restricting its application to specific entities, or classes of entity, types of personal information, and particular types of acts and practices. As noted by the Australian

[1] Attorney-General's Department, *Privacy Act Review Discussion Paper* (October 2021) page 28.
[2] *Privacy Act 1988* (Cth) s 6.
[3] Attorney-General's Department, *Privacy Act Review Discussion Paper* (October 2021) 42; See also Salinger Privacy's *Submission to the Privacy Act Review Issues Paper* (December 2020) 24.
[4] See for example, Scott Ikeda, '*Facebook's Use of Alternative Location Tracking Methods to Circumvent Apple Privacy Protections Expands to Accelerometer Data*', CPO Magazine (5 November 2021) https://www.cpomagazine.com/data-privacy/facebooks-use-of-alternate-location-tracking-methods-to-circumvent-apple-privacy-protections-expands-to-accelerometer-data/.
[5] Anna Johnston '*Location, location, location: online or offline, privacy matters*' SalingerPrivacy (12 November 2020) https://www.salingerprivacy.com.au/2020/11/12/geo-location-blog/; Jennifer Valentino-DeVries, Natasha Singer, Michael Keller and Aaron Krolik, '*Your apps know where you were last night, and they're not keeping it secret* ' NY Times (10 December 2018) https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

Department of Health,[6] providing the flexibility for EDs to be more targeted would better balance the need to protect individuals' privacy with the need to collect, use and disclose personal information to coordinate effective responses to emergencies and disasters.

Responsibility for making emergency declarations

11. Part VIA of the Privacy Act allows the Prime Minister or a Minister may 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.[7] Given the Information Commissioner has oversight over the Privacy Act, and the impacts of EDs on individuals' privacy, the Review may wish to consider whether it would be more appropriate to vest the power to make EDs with the Commissioner, or alternatively ensure EDs are only made in consultation with the Commissioner.

12. Further, given the ability to undertake public consultation prior to making an ED is limited, it may be beneficial to implement mechanisms to ensure the decision to declare an ED can be reviewed as soon as practicable after the declaration.

Employee records exemption

13. With the volume and variety of personal information employers often collect from their employees, there is a significant risk of harm to employees if their personal information is used or disclosed inappropriately.[8] OVIC recommends removing the employee records exemption from the Privacy Act to ensure privacy protections apply to employee information. This would also ensure employees have appropriate avenues to make privacy complaints where necessary. Removing this exemption would align the Privacy Act with community and employee expectations[9] and improve public trust and confidence in employers' information handling practices.[10]

14. While the removal of the employee records exemption would result in increased compliance costs for employers, OVIC considers the increase would not be significant, as employers have existing obligations under the Privacy Act in relation to other personal information they collect, use or disclose in the course of their business. Further, any increase in costs would not outweigh the public interest in providing individuals with adequate privacy protections within the workplace.

Political parties' exemption

15. While the Privacy Act exemption for political parties is intended to encourage freedom of political communication and enhance the operation of the electoral and political process in Australia, it raises significant concerns around the information handling practices of political parties and the impact on individuals' privacy. As noted by OVIC,[11] political parties collect personal information about voters from a variety of sources such as media and data brokerage services. When combined with personal information contained in electoral rolls, political parties can build large databases with detailed information about voters without their knowledge or consent.

16. Such databases enable political parties to target political campaigning at individual voters based on the detailed voter profiles. This practice negatively impacts democracy by inhibiting informed political debate and restricting voters' ability to make informed decisions. There are several

[6] See paragraph 10 of the Australian Department of Health's submission in response to the Privacy Act Review Issues Paper, December 2020, https://www.ag.gov.au/sites/default/files/2020-12/australian-department-of-health.PDF.
[7] *Privacy Act 1988* (Cth) s 80J.
[8] 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.
[9] Australian Community Attitudes to Privacy Survey (Lonergan, September 2020) 60.
[10] See OAIC's *Submission in response to the Privacy Act Review Issues Paper* (11 December 2020) https://www.ag.gov.au/sites/default/files/2021-01/office-of-the-australian-information-commissioner.PDF.
[11] 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.

examples of political parties misusing voters' personal information to undertake targeted campaigning in previous elections, which has resulted in calls for restrictions on political advertising.[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.

17. OVIC notes the introduction of the *Spam Amendment (Unsolicited Political Communications) Bill 2021* which, if passed by the Parliament of Australia, will require political parties to provide an unsubscribe function for unsolicited electronic political communications[13] is taking a positive step towards reducing the misuse of voters' personal information for targeted campaigning. However, OVIC's concern is the Bill is reactive in nature and only enables voters to unsubscribe from further use of their personal information for targeted campaigning by the relevant political party. The Bill does not protect the collection, use and disclosure of voters' personal information in the first instance.

18. Given the abovementioned risks to individuals personal information, and the limits of the protection proposed by *Spam Amendment (Unsolicited Political Communications) Bill 2021*, OVIC strongly recommends the removal of the political parties' exemption. This would require political parties to be more transparent and accountable for their information handling practices and improve public trust in the democratic process. The removal of the exemption would not inherently limit any freedom of political communication. Political parties could still communicate with constituents as they do now.

19. However, to the extent they use personal information about individuals in doing so, they would need to comply with the Australian Privacy Principles. Removing the exemption would also more closely align the Privacy Act with multiple comparable international jurisdictions.[14]

Notice of collection of personal information

20. OVIC supports the proposed introduction of an express requirement in Australian Privacy Principle (**APP**) 5 that collection notices must be 'clear, current and understandable'.[15] Providing notice enables individuals to understand how their personal information will be collected, used and disclosed, and plays an essential role in individuals' ability to make informed choices and provide consent.

21. However, OVIC is concerned that the proposal to strengthen the requirement for when a collection notice is required[16] is unlikely to result in any practical difference when compared with the existing requirement for APP entities to take reasonable steps to notify individuals.

22. The proposed amended wording of APP 5 is largely identical to the existing wording in the Privacy Act. The primary difference is that, where an individual is not already aware of the APP 5 matters, APP entities would still be required to provide a collection notice unless notification 'would be impossible or would involve disproportionate effort'.[17]

---

[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-legislation-banning/8a642933-75fa-47e3-a28d-65c7b6c734fe;

[13] Spam Amendment (Unsolicited Political Communications) Bill 2021 (Cth) Schedule 1 Part 2A; Explanatory Memorandum, Spam Amendment (Unsolicited Political Communications) Bill 2021.

[14] Australian Law Reform Commission, *For your Information: Australian Privacy Law and Practice* (Report No 108, May 2008) vol 2, page 1319, https://www.alrc.gov.au/wp-content/uploads/2019/08/108_vol2.pdf.

[15] See OAIC's *Submission in response to the Privacy Act Review Issues Paper* (11 December 2020) 69 [8.1] at https://www.ag.gov.au/sites/default/files/2021-01/office-of-the-australian-information-commissioner.PDF.

[16] Ibid 73, Proposal 8.4.

[17] Ibid.

23. OVIC considers the amended wording would likely be interpreted by APP entities as indicating that in some circumstances, providing a collection notice to an individual may not be practicable or feasible. That interpretation would have the same or similar effect as the existing requirements in practice.

Consent to collection, use and disclosure of personal information

24. While consent has long been an important element of privacy regulation, in today's digital environment the traditional binary approach to consent is no longer an effective way for individuals to control how entities collect, use, and disclose their personal information.

25. There are a range of matters that affect the utility of consent. The complexities of new and emerging technologies such as AI and Internet of Things challenge an individual's ability to meaningfully consent to how their personal information is handled. For instance, in addition to not fully understanding how an AI system works, an entity may not know how an AI system will use personal information in future, and this impacts the entity's ability to provide notice sufficient to enable individuals to give informed and specific consent.[18]

26. The power imbalance between individuals and entities means individuals often do not have real choice over how their personal information is managed as they are compelled to consent to the collection, use and disclosure of their information to access services.

27. It is difficult, if not impossible, for individuals to identify the privacy risks associated with each transaction they enter with entities, especially future risks. Daniel Solove[19] points out that many privacy harms are the result of an aggregation of pieces of data over a period of time by different entities. He argues that the 'types of new information that can be gleaned from analysing existing information and the kinds of predictions that can be made from this data are far too vast and complex, and are evolving too quickly, for people to fully assess the risks and benefits involved'. Linked to this is the fact that practices such as micro-targeted advertising, profiling and tracking involve the collection, use and disclosure of information without the knowledge or consent of individuals.

28. A new approach to consent is necessary to enable individuals to exercise meaningful consent. To that end, OVIC supports the proposal to introduce an enhanced definition of consent in the Privacy Act. The proposal would also more closely align the Privacy Act with global jurisdictions such as the GDPR.

29. Importantly, entities should not rely on consent to as the primary means of authorising collections, uses and disclosures of individuals' personal information. The current privacy self-management model places an unrealistic, unfair burden on individuals to protect their privacy. Entities need to be more transparent and accountable for their information handling practices and bear more responsibility for protecting the privacy of individuals.

30. The Review raises the question whether entities should be required to refresh or renew an individual's consent on a periodic basis where consent is obtained for the collection, use or disclosure of sensitive information. Understandably, additional protections are applied to sensitive information under the Privacy Act as it carries inherent risks to individuals' privacy. It may be appropriate to periodically renew or refresh consent in specific circumstances, but it is important to ensure this practice does not cause consent fatigue.

[18] For further information on how AI challenges consent see OVIC's *Artificial Intelligence and Privacy – Issues and Challenges* available at https://ovic.vic.gov.au/privacy/artificial-intelligence-and-privacy-issues-and-challenges/.
[19] Daniel Solove, 'Privacy self-management and the consent dilemma' (2013) 126 *Harvard Law Review* 1880 – 1903.

Additional protections for collection, use and disclosure of personal information

31. As noted above, it is crucial to shift the burden of protecting privacy to corporate, government or political entities in order to create a more equitable balance between their responsibilities and individual privacy rights. OVIC supports the introduction of fairness-based protections in the Privacy Act by requiring entities to ensure that all collections, uses and disclosures of personal information are fair and reasonable.

32. Although APP 3 in the Privacy Act requires entities to collect personal information by fair and lawful means, this does not prevent entities from engaging in collection practices which may cause harm to individuals or are otherwise unfair or unreasonable. Furthermore, there is no requirement to use and disclose personal information in a fair manner under APP 6.

33. The fairness-based protection would mitigate against entities engaging in unfair or unreasonable practices likely to harm individuals, such as personalised targeted advertising aimed at vulnerable groups of society. Entities would be required to assess whether their information handling practices are fair and reasonable, even in instances in which individuals may have consented to the collection, use and disclosure of their personal information.

34. This proposal would also mirror approaches in other jurisdictions such as Canada, UK and Europe.[20]

Restricted practices (Proceed with caution zones) and prohibited practices (No-Go zones)

35. To complement the introduction of fairness-based protections, OVIC considers it would be appropriate to more tightly regulate practices that pose a higher risk to individual's privacy and are contrary to community expectations. The introduction of restricted and prohibited practices is one way of regulating such activities.

36. The Review considers whether entitles engaging in restricted practices should be required to undertake additional organisational accountability measures to identify and mitigate the privacy risks associated with these practices or increasing individuals' capacity to self-manage their privacy.

37. As mentioned above, entities are currently over-reliant on individuals self-managing their privacy and in the increasingly digital world, it is unrealistic and unreasonable to expect individuals to do so. OVIC is of the view that it would be preferable to require entities to be more accountable for their information handling practices.

38. In determining what practices should be restricted and prohibited, it may be useful to consider the risk of privacy harms and their impact on individuals, entities' legitimate interests, community expectations and public interest in regulating the practices.

Right to object

39. It is OVIC's view that individuals should have the right to object to, and to withdraw consent to the collection, use and disclosure of their personal information. This would enable individuals to exercise ongoing control over their personal information and respond to emerging privacy risks.

40. A right to object would also align the Privacy Act with similar legislation in other jurisdictions such as GDPR, Singapore and Canada.[21]

Right to erasure

[20] *Personal Information Protection and Electronics Documents Act*, C 2000, s5(3); *General Data Protection Regulation* (United Kingdom) art 5(1).
[21] See *General Data Protection Regulation* (United Kingdom) art 21; *Personal Data Protection Act (*Singapore) s16; *Personal Information Protection and Electronics Documents Act*, sch 1, principle 3 (4.3.8).

41. OVIC supports the inclusion of a limited right to erasure be included in the Privacy Act.[22] There is a strong public interest in providing individuals with the ability to make a request to an APP entity for the deletion of their personal information, particularly given the increasing community support for such a right.[23]

42. However, this right would need to be appropriately limited and would require the careful consideration of the potential implementation challenges and regulatory impact when determining the scope for a right to erasure, particularly in relation to public sector APP entities. OVIC suggests that a right to erasure be largely modelled on Article 17 of the GDPR.

43. Further, OVIC queries whether it may be appropriate for a new right to erasure to be applicable primarily to private sector entities, particularly given the nature of public sector entities' activities likely means there would be limited circumstances in which an exception to a right to erasure would not be available to public sector entities.

Children's privacy

44. As noted in OVIC's submission in response to the exposure draft of the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* (**Online Privacy Bill**), OVIC broadly supports the introduction of further privacy protections for children and vulnerable groups.[24]

45. However, OVIC is concerned that the proposed requirement to verify an individual's age or to obtain a parent or guardian's consent for the collection, use and disclosure of the personal information of a child under the age of 16, may encourage or result in the over-collection of personal information. If the Privacy Act were to require additional privacy protections for children, such as age verification processes, in addition to those proposed under the Online Privacy Bill, OVIC suggests the additional personal information collected to verify an individual's age should be destroyed once age has been verified.

46. Further, OVIC suggests that the assumed age of capacity, whether 15 or 16 years, be consistent for all APP entities. This would provide consistency across the Online Privacy Code (**OP Code**) and Privacy Act, and ensure APP entities subject to both the OP code and Privacy Act have a clear understanding of their obligations in relation to children.

Direct marketing, targeted advertising and profiling

47. OVIC supports strengthening the regulation of direct marketing, and in particular micro targeted advertising, which poses a greater risk to individuals, society, and democracy. Micro-targeted advertising relies on the collection of individual's personal information often through invasive, insidious practices, and the sharing of this information with a range of entities either without the individual's knowledge or in ways that individuals would not reasonably expect. It has normalised tracking and data mining and driven the phenomenon known as 'surveillance capitalism'.[25]

---

[22] See OAIC's *Submission in response to the Privacy Act Review Issues Paper* (11 December 2020) 52 – 55, available at https://www.ag.gov.au/sites/default/files/2021-01/office-of-the-australian-information-commissioner.PDF; See Australian Competition and Consumer Commission's *Digital Platforms Inquiry Final Report* (June 2019) 35, available at: https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf.

[23] Australian Community Attitudes to Privacy Survey (Lonergan, September 2020): https://www.oaic.gov.au/__data/assets/pdf_file/0015/2373/australian-community-attitudes-to-privacy-survey-2020.pdf.

[24] See OVIC's *Submission in response to the Online Privacy Bill 2021 Exposure Draft and Explanatory Paper*, 1 December 2021, https://ovic.vic.gov.au/wp-content/uploads/2021/12/OVIC-Submission-Online-Privacy-Bill-December-2021.pdf.

[25] Shoshana Zuboff. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019. 691 pp.: ISBN: 9781610395694

Furthermore, micro-targeted advertising has facilitated the growth of fake news and as mentioned in the Paper, there are potential harms with targeting misinformation at vulnerable individuals.[26]

48. While APP 7 regulates the use and disclosure of personal information for direct marketing in certain circumstances, it is not broad enough to address the privacy harms associated with targeted advertising. OVIC supports implementation of mechanisms aimed at giving individuals greater control over the use of their information in direct marketing, and aimed at making entities more transparent about the use of individuals' personal information for direct marketing purposes.

49. Specifically, OVIC supports introducing an unqualified right to object to the collection, use and disclosure of personal information for direct marketing purposes, requiring entities to include specific information on direct marketing in their privacy policies, and requiring entities to notify individuals at the point of collection that the primary purpose of use or disclosure will be to influence the individual's behaviour or decisions.

50. Importantly, stronger regulation of direct marketing practices would be consistent with approaches taken in other jurisdictions such as Europe and Canada.

Automated decision making

51. As noted in the Paper, AI is becoming increasingly common across both the public and private sector. While automated decision making can provide numerous benefits, it can also cause significant harms to individuals. One common risk of automated decision making is ability to discriminate, perpetuate biases and augment existing inequalities.[27]

52. The Review proposes requiring privacy policies to include information on whether personal information will be used in automated decision making which has a legal, or similarly significant effect on individual's rights.

53. OVIC supports requiring entities to be more transparent about their information handling practices. Further, OVIC queries whether it would be beneficial to develop a non-exhaustive list of decisions, or types/categories of decisions, that have a legal, or similarly significant effect on people's rights to provide guidance to entities.

Thank you once again for the opportunity to provide comment on the Discussion Paper. My office will 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.

[26] Arwa Mahdawi, 'Targeted ads are one of the world's most destructive trends. Here's why', The Guardian (online, 6 November 2019) available at https://www.theguardian.com/world/2019/nov/05/targeted-ads-fake-news-clickbait-surveillance-capitalism-data-mining-democracy.
[27] 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 biases found in AI datasets', *Forbes* (online, February 7 2020) available at: https://www.forbes.com/sites/cognitiveworld/2020/02/07/biased-algorithms/?sh=3810917376fc. See also OVIC's *Artificial Intelligence and Privacy – Issues and Challenges* available at https://ovic.vic.gov.au/privacy/artificial-intelligence-and-privacy-issues-and-challenges/.

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

Yours sincerely

Sven Bluemmel
Information Commissioner