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: D21/21844

1 December 2021

Attorney-General's Department

By email only: OnlinePrivacyBill@ag.gov.au

Dear Review team,

Submission in response to the Online Privacy Bill Exposure Draft and Explanatory Paper

I am pleased to make a submission in response to the Attorney-General's Department's Exposure Draft of the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* (**Online Privacy Bill**) and the corresponding Explanatory 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* (Vic) (**PDP Act**) and the *Freedom of Information Act 1982* (Vic). As Information Commissioner, I have a strong interest in matters that impact individuals' privacy, and one of my functions under the PDP Act is to make public statements in relation to such matters.

General comments

1. OVIC supports the introduction of a binding Online Privacy Code (**OP Code**) to address the challenges and privacy risks posed by social media platforms, data brokerage services and other large online platforms.[1] An OP Code will assist to bring the *Privacy Act 1988* (**Privacy Act**) in line with current community expectations, by ensuring that individuals' privacy is given appropriate consideration and better protected in online settings.[2]

2. It is positive to see the Online Privacy Bill proposes to enhance the Australian Information Commissioner's (**the Commissioner's**) investigative and enforcement powers under the Privacy Act, particularly in relation to organisations that repeatedly interfere with individuals' privacy.[3]

3. OVIC is pleased to see the Online Privacy Bill defines the term 'OP organisation' and includes detailed descriptions of the types of organisations that are included within the scope of the term and thus subject to the OP Code.[4] Additionally, the Explanatory Paper contains useful plain English descriptions of the categories of OP organisations and practical examples for each category. OVIC recommends similar descriptions and examples be included in guidance published by the Office of the Australian Information Commissioner (**OAIC**) on the OP Code as it will allow organisations to easily determine whether they will be subject to the OP Code.

[1] *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* (Cth) sections 26KB and 26KC(2)(a) (**Online Privacy Bill**).
[2] Explanatory Paper, Online Privacy Bill page 4.
[3] Ibid, pages 15 – 22.
[4] Online Privacy Bill section 6W.

Development of the OP Code

4. The Explanatory Paper notes the OP Code may be developed by the Commissioner, but that OP organisations will have the first opportunity to act as 'OP code developer'.[5] OVIC acknowledges that codes under the Privacy Act are typically developed by the organisations that will be subject to the codes.

5. However, given many OP organisations use business models that depend upon the harvesting of information, personal or otherwise, and have a history of misrepresenting how they use and disclose information,[6] OVIC is concerned about the moral hazard in permitting OP organisations to develop the OP Code themselves. In OVIC's view, it will be difficult for OP organisations to develop a sufficiently robust code that meets community expectations, where the eventual code will curtail elements of their business and profit models. OVIC strongly suggests the responsibility for developing the OP Code rest with an independent party, for example the Commissioner only, with a requirement to consult with OP organisations during the development process.

Requirement to cease use and disclosure of personal information upon request

6. OVIC generally considers that the proposed requirement for OP organisations to cease further use and disclosure of an individual's personal information upon request will allow individuals increased control over their personal information and takes a positive step towards strengthening individuals' privacy online. However, the proposed requirement also raises issues that may need further consideration.

'Cease use and disclosure' versus a 'right to erasure'

7. The Explanatory Paper notes that the right of an individual to request an OP organisation to cease using and disclosing their personal information is not intended to amount to a 'right to erasure'.[7] The Explanatory Paper indicates that this new requirement will provide individuals with a mechanism to limit how OP organisations use and disclose, or further use and disclose their personal information. OVIC generally supports the introduction of this mechanism on the basis that it provides individuals with additional control over how their personal information is used and disclosed by OP organisations.

8. However, OVIC queries whether section 26KC(2)(h) of the Online Privacy Bill could be expanded to include a right to erasure similar to that included in the European Union's General Data Protection Regulation[8] to minimise the risks to privacy. In addition, this would bring the Privacy Act more in line with international jurisdictions and be consistent with the approach taken in domestic legislative frameworks such as the Consumer Data Right and My Health records systems.[9] OVIC acknowledges there may be a range of challenges associated with a right to erasure including implementation, technical, cost and other resource challenges which would need to be taken into account when determining the appropriate scope of the right.

9. OVIC queries how an individual's request to cease use and disclosure of their personal information would operate in circumstances where the individual no longer wishes to engage with or utilise the OP organisation's services (as opposed to limiting secondary uses). In these circumstances, a right to erasure may be more appropriate where there are limited reasons, if any, for which an OP organisation would need to retain personal information. The indefinite retention of personal information poses a risk to individuals' privacy as it increases the risk of misuse, loss, unauthorised access, modification, or

[5] Explanatory Paper, Online Privacy Bill page 12.
[6] See, for example, Federal Trade Commission, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook* (24 July 2019) <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>.
[7] Ibid, page 10.
[8] General Data Protection Regulation Article 17.
[9] Competition and Consumer Act 2010 (Cth) section 56BAA; My Health Records Act 2012(Cth) section 17(3).

disclosure. It also increases the risk that it will be used, whether inadvertently or deliberately, for other purposes often completely unrelated to the original purpose of collection.

Charges for complying with requests from individuals to not use personal information

10. While OVIC acknowledges OP organisations will incur costs for time and resources required to comply with individual requests to cease use and disclosure of personal information, OVIC strongly discourages the proposal to allow OP organisations to charge individuals for complying with a request.[10]

11. The collection of an individual's personal information is often central to the generation of revenue for many OP organisations. OVIC considers it unreasonable to enable OP organisations to further increase their revenue by imposing charges on individuals related to a request to not use personal information.

12. Furthermore, imposing charges on individuals may deter individuals from making a request and limit their ability to control how their personal information is used and disclosed. This may also set a concerning precedent in which 'privacy' becomes a service individuals must pay for and is only available to those with financial means.

Protecting children and vulnerable groups

13. OVIC supports the introduction of further privacy protections for children and vulnerable groups, both generally and online, as OVIC recognises that enhancing privacy protections for these groups is vital to minimising the privacy risks they face.

14. OVIC acknowledges the proposed requirement for social media platforms to take all reasonable steps to verify the age of individuals using the service and 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.[11] However, OVIC is concerned this requirement may encourage or cause the overcollection of information. For example, it would be an adverse outcome if social media platforms started collecting copies of official documents such as driver's licences or birth certificates to verify an individual's age. OVIC suggests it should be made clear that the collection of additional personal information is only for the purpose of age verification and must be destroyed once the individual's age has been verified.

15. In addition, OVIC highlights that Australian Privacy Principle (**APP 2**) provides that individuals must have the option of dealing anonymously or by pseudonym with an APP entity, which would include the proposed OP organisations, unless required by Australian law or court/tribunal order or it would be impracticable for the APP entity to deal with individuals acting anonymously or under a pseudonym.[12] Anonymity and pseudonymity are important concepts as they allow individuals to exercise control over their personal information and decide how much of, or when, their personal information will be disclosed. Noting the manner in which age verification will be achieved is unknown at this stage, the proposal will likely diminish the effectiveness of APP 2, and may consequently lay the foundations for greater interferences in individuals' online privacy in the future.

Extra-territorial application

16. OVIC is pleased to see the Online Privacy Bill clarifies that the scope of the Privacy Act will extend to foreign organisations carrying on business in Australia even where Australians' information is not collected or held directly from a source in Australia.[13]

[10] Online Privacy Bill section 26KC(4)(c).
[11] Online Privacy Bill section 26KC(6).
[12] *Privacy Act 1988* (Cth) schedule 1 part 1 clause 2; Office of the Australian Information Commissioner, *Australian Privacy Principles guidelines* (22 July 2019) chapter 2.
[13] Explanatory Paper, Online Privacy Bill page 23.

17. OVIC notes that this is an important clarification in the context of the increasingly digital and highly connected world we live in, where individuals regularly utilise online products and services that are offered to Australians but are primarily based in a foreign location. For example, many individuals in Australia utilise Facebook, a product operated by a foreign organisation based in the United States of America (**the US**), and their personal information collected while engaging with the platform may be stored in servers in the US or within other foreign countries.

Resources and funding

18. The OAIC will need to be appropriately resourced to effectively fulfil its expanded functions under the Online Privacy Bill. For instance, the new investigation powers permitting the Commissioner to investigate possible interference with privacy of an individual and assess OP organisations' compliance with the OP Code will likely require additional resourcing to be carried out effectively.

19. In addition, to aid the successful development and implementation of the OP Code, the OAIC will need to dedicate resourcing to communications and guidance to raise awareness and understanding of the OP Code once introduced.

Thank you for the opportunity to comment on the Online Privacy Bill. I have no objection to this submission being published without further reference to me. I also propose to publish a copy of this submission on OVIC's website and would be happy to adjust the timing of this to allow you to collate and publish submissions proactively.

If you would like to discuss this submission, please do not hesitate to contact me or my colleague Jenna Daniel, Policy Officer, at Jenna.Daniel@ovic.vic.gov.au.

Yours sincerely

Sven Bluemmel
Information Commissioner