Office of the Victorian Information Commissioner

t 1300 00 6842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D19/208

15 February 2019

Digital Platforms Inquiry
Australian Competition & Consumer Commission
GPO Box 3131
CANBERRA ACT 2601

By email only: platforminquiry@accc.gov.au

Dear Sir/Madam

Submission in response to the Digital Platforms Inquiry preliminary report

The Office of the Victorian Information Commissioner (**OVIC**) is pleased to provide a submission to the Australian Competition & Consumer Commission (**ACCC**) in relation to the *Digital Platforms Inquiry preliminary report* (**the report**).

OVIC is the primary regulator for information privacy, data security, and freedom of information in Victoria, and administers the *Privacy and Data Protection Act 2014* (**PDP Act**) and the *Freedom of Information Act 1982* (Vic). As the Information Commissioner, I have a strong interest in matters that impact on individuals' privacy, and one of my functions under the PDP Act is to make public statements in relation to such matters.

This submission is made from a Victorian perspective and through the lens of the PDP Act. It outlines my office's views on some of the issues identified in Chapter 5 of the report which relate to consumers' privacy and personal information, namely consent and the deletion of user data.

Consent

1. The report contains a number of proposed amendments to the Commonwealth *Privacy Act 1988* (**Privacy Act**) in relation to consent, including that the definition of consent under the Privacy Act be amended to only include express consent (rather than express *or* implied). Further, the report recommends that the Australian Privacy Principles (**APPs**) establish binding criteria for valid consent – that it is current and specific, provided voluntarily, and by an individual who is adequately informed and has the capacity to understand and communicate their consent.[1]

2. While OVIC recognises the value of consent to provide consumers with a greater ability to control the collection, use, and disclosure of their personal information, OVIC is also mindful that relying on consent as a means to protect consumers' privacy may be problematic in some cases. The traditional (or transactional) approach to consent, which involves a consumer providing their consent to the collection, use or disclosure of their personal information in exchange for a product or service, places the responsibility on the consumer to inform themselves of the way in which

[1] See, pages 13, 225 and 229 of the report.

their personal information will be handled, prior to making the decision to access that particular product or service.

3. However, as the report highlights, privacy policies and terms of use are often long, complex, vague, difficult to navigate, and do not provide sufficient detail for informed consent. Further, privacy policies (and the explanations that accompany them) often include language that indicates user data is used for targeted advertising purposes.[2] While this may be true, and allows advertising on digital platforms to be more effective than traditional media, it is arguable whether more targeted advertising is in fact what consumers want, and yet it is often stated as the reason for the collection of the data.[3] Recent research in the United States suggests that this assumption is not based on users' actual opinions, at least in the context of political advertising.[4] This is also consistent with the Office of the Australian Information Commissioner's survey and the ACCC consumer survey referenced in the report.[5]

4. The length, complexity, and difficulty in navigating privacy policies and terms of use mean that often, consumers may not read these documents, and few engage meaningfully with them.[6] Moreover, the provision of express consent may not necessarily indicate that the consumer has read or understood the terms and conditions regarding the collection, use, or disclosure of their personal information. Consequently, the consent provided – while express – is often not meaningful.

5. The UK Information Commissioner's Office has previously highlighted that even where consumers are informed and do understand the inherent privacy risks of providing their personal information, it is possible they may feel resigned to consenting to the use of their information in order to access online services, as they do not consider there is any alternative.[7] In addition, consumers can rarely negotiate terms of use in an online environment.[8] As a result, consent may not necessarily be given voluntarily, which is a fundamental element of meaningful consent.

6. The use of notice and consent mechanisms as a means to protect privacy is further challenged by technological advances and developments in areas such as machine learning, artificial intelligence, and big data analytics. In a digital landscape, consumers' personal information can be used in exponentially new and unexpected ways, and at times these processes and outcomes can be unclear to those developing the algorithms, let alone the consumer whose information is being used. The increasing complexity of networks, systems, and information flows, along with the widening variety of data collection methods, renders the traditional consent model less and less meaningful (and practicable) in the modern world.[9]

7. While consent does not always form the legal basis for collecting personal information, organisations are still generally required to provide notice of collection to individuals. Improved notification practices to encourage more user-friendly communication, such as those proposed by Preliminary recommendation 8(a) of the report, would therefore provide value to consumers even where their consent is not sought for the collection, use or disclosure of their personal information.

---

[2] On page 182 of the report.

[3] See: Zuckerberg, Mark, "The Facts About Facebook," *The Wall Street Journal*, 24th January 2019, https://www.wsj.com/articles/the-facts-about-facebook-11548374613, accessed 14th February 2019.

[4] Turow, J., Delli Carpini, M. X., Draper, N. A., & Howard-Williams, R. (2012). *Americans Roundly Reject Tailored Political Advertising*. Annenberg School for Communication, University of Pennsylvania, Retrieved from http://repository.upenn.edu/asc_papers/398

[5] See page 191 of the report.

[6] On pages 182 – 183 of the report.

[7] In their report, *Big Data, artificial intelligence, machine learning and data protection*, 2017, p 24.

[8] As highlighted by the Consumer Policy Research Centre in their report, *Consumer data and the digital economy - Emerging issues in data collection, use and sharing*, 2018, p 9.

[9] Office of the Victorian Information Commissioner, *Artificial intelligence and privacy issues paper*, 2018, p 12.

8. My office has previously noted these concerns with the traditional notice and consent model and its ability to adequately and effectively protect consumers' privacy.[10] The viability of consent to protect individuals' privacy in a digital world has also been considered in other jurisdictions, along with possible alternatives to supplement consent in order to better protect consumers' privacy.[11] For example, establishing a minimum standard of protection for the treatment of consumers' personal information – regardless of whether or not consent is sought or obtained – may reduce the burden consumers face in understanding and consenting to often complex information flows and practices.[12]

9. My office is of the view that, given the challenges for consumers to be able to understand the full range of contexts in which their data may be used, the use of a consent model for the collection of user data in the context of digital platforms has substantial limitations and may be inappropriate.

10. Accordingly, a minimum standard of protection that limits digital platforms' collection of user data, potentially with a carefully conceived and limited ability to waive that protection, may be a more prudent regulatory strategy. This would need to be balanced with genuine needs to collect user data for services that are not advertising-related. For example, there are substantial benefits to location tracking in some applications such as mapping – it is the extension of that data for use in other contexts and applications that, based on the ACCC survey, concerns consumers.[13]

Deletion of user data

11. OVIC considers it best practice to destroy personal information if it is no longer necessary for any purpose, while having regard to any applicable recordkeeping requirements (noting that compliance with recordkeeping or archiving obligations is itself a purpose for retaining personal information).[14] This is consistent with the principles of necessity highlighted in Information Privacy Principles (**IPPs**) 1 and 4 of the PDP Act which state, respectively, that personal information should only be collected if it is necessary to fulfil an organisation's function, and that personal information should be destroyed if it is no longer needed for any purpose. This can help prevent the open-ended retention of personal information, and mitigate the risk of unauthorised use, disclosure or modification, or misuse and loss.

12. Notwithstanding that the comments expressed above relate specifically to the IPPs under the PDP Act, OVIC supports, in principle, the proposed recommendation to amend the Privacy Act to enable consumers to require the erasure of their personal information where they have 'withdrawn their consent and the personal information is no longer necessary to provide the consumer with a service'.[15]

13. Additionally, OVIC generally supports the suggestion for an explicit obligation for digital platforms or third parties to either delete all user data once a user ceases to use the services, or that user data 'be automatically deleted after a set period of time'.[16] Such an obligation may serve to enhance privacy protections, particularly where the need to request the deletion of their personal information may pose a burden to some consumers who may not actively take the steps to make such a request, or who may not have even been a customer of that platform.[17]

---

[10] See the OVIC Submission to the Australian Competition & Consumer Commission on the Consumer Data Right Rules Framework, available at www.ovic.vic.gov.au/privacy/submissions-and-reports/submissions.

[11] See *Consent and privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act*, Policy and Research Group, Office of the Privacy Commissioner of Canada, 2016.

[12] See paragraph 2 of OVIC's submission, op.cit., pp 1-2.

[13] See page 188 of the report.

[14] In line with Information Privacy Principle 4.2 of the PDP Act.

[15] Preliminary recommendation 8(d), on page 13 of the report.

[16] On page 231 of the report.

[17] See page 193 of the Preliminary Report.

14. OVIC would welcome more information regarding the timeframe for the automatic deletion of user data (presumably after a user has ceased using a service), and how this would apply in practice. Regardless, the deletion of user data should still be balanced with the need to maintain personal information if it is necessary for an organisation's functions or activities, including for recordkeeping purposes.

Thank you for the opportunity to comment on the report. OVIC will continue to follow the progress of the ACCC's Digital Platforms Inquiry with interest.

I have no objection to this submission being published by the ACCC 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 ACCC to collate and publish submissions proactively.

If you have any questions about this submission, please contact Emily Arians, Senior Policy Officer at emily.arians@ovic.vic.gov.au.

Yours sincerely

Sven Bluemmel
Information Commissioner