24 January 2022

Attorney-General's Department

4 National Circuit

BARTON ACT 2600

By email: PrivacyActReview@ag.gov.au

Dear Attorney-General,

RE: Review of the Privacy Act 1988

Please find attached the response from the Centre for Artificial Intelligence and Digital Ethics to the Privacy Act Review Discussion Paper (October 2021), with contributions from Dr Shaanan Cohney (Faculty of Engineering and Information Technology), Professor Lars Kulik (Faculty of Engineering and Information Technology), Liam Harding (CAIDE). Thank you for the extension in submitting this response until 24 January 2022.

Overall, we are supportive of the far-reaching reforms proposed in the discussion paper. We provide in our submission comments on some aspects of those proposed reforms in the aim of strengthening their protective impact.

We have no objection to this submission being published. We do not require any part of this submission to be redacted.

Kind regards,

Jeannie Paterson

Jeannie Marie Paterson | Professor of Law | Melbourne Law School | The University of Melbourne

Co-Director of the Centre for AI and Digital Ethics (CAIDE)

Response to the Review of the Privacy Act - Discussion Paper (October 2021)

Centre for Artificial Intelligence and Digital Ethics | The University of Melbourne

Professor Jeannie Paterson, with Dr Shaanan Cohney, Professor Lars Kulik, Liam Harding

24 January 2022

Part 1: Scope and Application of the Privacy Act

2. Definition of personal information

2.1 Change the word 'about' in the definition of personal information to 'relates to'.

2.2 Include a non-exhaustive list of the types of information capable of being covered by the definition of personal information.

2.3 Define 'reasonably identifiable' to cover circumstances in which an individual could be identified, directly or indirectly. Include a list of factors to support this assessment.

2.4 Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.

2.5 Require personal information to be anonymous before it is no longer protected by the Act.

We are broadly in support of the recommendations made by Salinger Privacy in their submission dated 3 January 2022.

2.6 Re-introduce the Privacy Amendment (Re-identification) Offence Bill 2016 with appropriate amendments.

The discussion paper proposes reintroducing the Privacy Amendment (Re-identification) Offence Bill 2016 with appropriate amendments. (The original bill lapsed in 2019: see Discussion paper p 24). The government should not reintroduce these, or similar, amendments.

We share the concern raised by researchers and NGOs over the lack of exceptions for good-faith defensive research. To assess the effectiveness of deidentification techniques and develop improvements, researchers attempt to reverse the process. If the reidentification is successful, they can identify the problems with the original scheme and suggest ways to improve the process. Criminalising this form of research short-circuits the process of strengthening dataset privacy. If the law were to criminalize research with good intentions, not only will the risk of deidentification attacks persist, but when data is ultimately deanonymized, it will be by parties willing to abuse their findings.

Part 2: Protections

8. Notice of collection of personal information

8.1 Introduce an express requirement in APP 5 that privacy notices must be clear, current, and understandable.

8.2 APP 5 notices limited to the following matters under APP 5.2:

1. *the identity and contact details of the entity collecting the personal information*
2. *the types of personal information collected*
3. *the purpose(s) for which the entity is collecting and may use or disclose the personal information*
4. *the types of third parties to whom the entity may disclose the personal information*
5. *if the collection occurred via a third party, the entity from which the personal information was received and the circumstances of that collection*
6. *the fact that the individual may complain or lodge a privacy request (access, correction, objection, or erasure), and*
7. *the location of the entity's privacy policy which sets out further information.*

8.3 Standardised privacy notices could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording, and icons. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised notices.

8.4 Strengthen the requirement for when an APP 5 collection notice is required – that is, require notification at or before the time of collection, or if that is not practicable as soon as possible after collection, unless:

- *the individual has already been made aware of the APP 5 matters, or*
- *notification would be impossible or would involve disproportionate effort.*

Notice is important in giving individuals the opportunity to be informed about data collection, processing, and use. However, as recognised in the Issues and the Discussion papers even 'clear, current and understandable' notice procedures do not overcome the considerable information asymmetry between individuals and firms.[1]

This is a lesson that has already been learnt in consumer protection and financial services law. Mandatory disclosure of the information deemed relevant to consumers was long relied upon as a way of correcting the imperfections of the market by empowering consumers to themselves manifest better choices.[2] However, these fields of law have now supplemented disclosure as a policy tool with strong substantive protections for consumers and investors. This is because it is now well recognised that individuals are subject to what is sometimes termed 'bounded rationality' in decision making. Bounded rationality means that individuals are influenced by heuristics, rules of thumb and information overload which limits their ability to make optionally welfare enhancing decisions.[3]

Similar considerations apply equally in the context of privacy and data protection. Consumers cannot meaningfully be asked to give up their data without some understanding of what may be done with that data, the inferences that may be drawn about them, the ways in which their data may be combined with other sources and the consequences for their market interactions. Yet it seems likely that consumers are currently largely unaware of these processes[4], and commonly misunderstand the purpose of privacy policies.[5] Some form of consumer education strategy might assist in narrowing the information gap. However, ultimately, problems of information overload and inaccessibility, along with the pressures of time, limit the use that most consumers can make of privacy policies in providing informed consent to data collection and processing practices they deal with on a daily basis.[6]

Responsibility for reasonable and fair data collection, processing and use should be placed on firms, rather than individuals, who are better placed to manage the inherent risks to autonomy and well-being inherent in these practices.

---

[1] See further Paterson, J., Chang, S., Cheong, M., Culnane, C., Dreyfus, S. & McKay, D. (2021). The Hidden Harms of Targeted Advertising by Algorithm and Interventions from the Consumer Protection Toolkit. *International Journal on Consumer Law and Practice*, 9 pp. 1-24.

[2] Daniel J Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880.

[3] Also, generally J M Paterson, 'From Disclosure to Design: The Australian Regulatory Response to Mis-selling to Consumer Investors by Financial Services Providers' in Sandra Booysen, *Financial Advice and Investor Protection* (Elgar, 2021)

[4] Lina M Khan and David E Pozen, 'A Skeptical View of Information Fiduciaries' (2019) 133 Harvard Law Review 497, 519–520.

[5] See, e.g., ACCC, 'Digital Platforms Inquiry: Preliminary Report' (December 2018) 174; Policy and Research Group, Office of the Privacy Commissioner of Canada, 'Consent and Privacy: A Discussion Paper Exploring Potential Enhancements to Consent under the Personal Information Protection and Electronic Documents Act' (Discussion Paper, 2016) 9; Competition and Markets Authority, United Kingdom, 'Online Platforms and Digital Advertising: Market Study Final Report' (2020) 166–72: generally reporting consumers assume privacy policies are about restricting use of data.

[6] See, e.g., Russell Korobkin, 'Bounded Rationality, Standard Form Contracts, and Unconscionability' (2003) 70 University of Chicago Law Review 1203; Australian Securities and Investments Commission, *Financial Literacy and Behavioural Change* (Report REP 230, March 2011).

9. Consent to the collection, use and disclosure of personal information

9.1 Consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.

This is a desirable reform that brings the Privacy Act into alignment with the GDPR and the Consumer Data Right.

However, even a requirement for consent that is 'voluntary, informed, current, specific, and unambiguous' will not ensure individuals will be enabled to act in a way that protects their best interests in relation to personal data, for the reasons discussed above in relation to notice.

Notice and consent regimes have clear downsides. When requests for consumer consent are as frequent as they already are, it becomes impracticable for individuals to meaningfully consider the substance of the requests. This remains true, even when the requests are conspicuous and written in plain language.[7]

Given the potential harms arising from extensive use of data analytics, targeting and profiling, reform to the Privacy Act should:

- require firms to implement pro-privacy defaults
- provide substantive protections for the interests of individuals.
- adopt the use of black and grey lists to respond to disproportionately harmful data practices.

Such protections will compliment those existing generally in consumer protections law.[7]

9.2 Standardised consents could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording, icons, or consent taxonomies. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised consents.

Standardised consents will assist individuals by reducing consent fatigue and improving opportunities for understanding. Consumer comprehension testing is also desirable. Such testing is likely to show many notice and consent provisions are written at a reading level well beyond the capacity of average consumers.[8] However we reiterate, as explained above, even standardised, comprehensive, tested notice and consent processes to not adequately protect individuals' rights and interests. The additional protections outlined above should be adopted.

10. Additional protections for collection, use and disclosure of personal information

10.1 A collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.

A statutory obligation for collection, use or disclosure of personal information to be fair and reasonable would be a desirable and appropriate response to the information asymmetry between individuals and firms. Firms, not individuals, are best placed to respond to societal expectations of fair data practices.

Reasonableness would seem to require a considered approach to data handling, looking to industry practices and the reasonable expectations of the individual. Fairness in this context would seem to require the interests of both parties to be considered and for any action taken in the interests of the firm to be proportionate to the interests being protected having regard to the risks of harm to the individual.[9]

[7] See further Clifford, Damian, and Paterson, Jeannie. "Consumer Privacy and Consent: Reform in the Light of Contract and Consumer Protection Law". *Australian Law Journal*, vol.94, no.10, 2020, pp. 741-751.

[8] See Benoliel, Uri and Becher, Shmuel I., The Duty to Read the Unreadable (January 11, 2019). 60 Boston College Law Review 2255 (2019), Available at SSRN: https://ssrn.com/abstract=3313837 or http://dx.doi.org/10.2139/ssrn.3313837.

[9] See e.g., *ASIC v AGM Markets Pty Ltd (in liq) (No 3)* [2020] FCA 208, [521].

10.2 Legislated factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances could include:

1. *Whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances*
2. *The sensitivity and amount of personal information being collected, used or disclosed*
3. *Whether an individual is at foreseeable risk of unjustified adverse impacts or harm as a result of the collection, use or disclosure of their personal information*
4. *Whether the collection, use or disclosure is reasonably necessary to achieve the functions and activities of the entity*
5. *Whether the individual's loss of privacy is proportionate to the benefits*
6. *The transparency of the collection, use or disclosure of the personal information, and*
7. *If the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child.*

In drafting amendments to the Privacy Act, it will be important to think about legislative design. Drafting that is overly dense, complicated, or prescriptive can create uncertainty, increase compliance costs, and creates the opportunity of regulatory arbitrage by firms in reducing their obligations.[10] A list of considerations is not strictly necessary as it reduces the flexibility and reasonableness of the principle based primary obligations. It would be possible instead to place these considerations in regulatory guidance from the OAIC. 'Soft law' approaches such as regulatory guidance can provide some increased certainty to industry without constricting the flexibility of the regime by overly prescriptive statutory drafting.[11]

11. Restricted and prohibited acts and practices

11.1 Option 1: APP entities that engage in the following restricted practices must take reasonable steps to identify privacy risks and implement measures to mitigate those risks:

1. *Direct marketing, including online targeted advertising on a large scale*
2. *The collection, use or disclosure of sensitive information on a large scale*
3. *The collection, use or disclosure of children's personal information on a large scale*
4. *The collection, use or disclosure of location data on a large scale*
5. *The collection, use or disclosure of biometric or genetic data, including the use of facial recognition software*
6. *The sale of personal information on a large scale*
7. *The collection, use or disclosure of personal information for the purposes of influencing individuals' behaviour or decisions on a large scale*
8. *The collection use or disclosure of personal information for the purposes of automated decision making with legal or significant effects, or*
9. *Any collection, use or disclosure that is likely to result in a high privacy risk or risk of harm to an individual.*

[10] See further *Financial Services Legislation: Interim Report A (ALRC Report 137)(2021)*: https://www.alrc.gov.au/publication/fsl-report-137/. Also Becher, Shmuel I., The Puzzle of Effective Consumer Protection Legislation: Challenges, Key Lessons and Design Principles (March 14, 2020). The Law and Economics of Regulation, pp. 73-99 (Mathis & Torr eds.) (Springer, 2021), Available at SSRN: https://ssrn.com/abstract=3565532.

[11] See Bant, E. and Paterson, J 2017. 'Statutory Interpretation and the Critical Role of Soft Law Guidelines in Developing a Coherent Law of Remedies in Australia,' in Levy, R., O'Brien, M., Rice, S., Ridge, P. and Thornton, M (ed.), New Directions for Law in Australia: Essays in Contemporary Law Reform, 1 edn, ANU Press. pp. 301-309. doi:10.22459/ndla.09.2017.27.

Option 2: In relation to the specified restricted practices, increase an individual's capacity to self-manage their privacy in relation to that practice.

Possible measures include consent (by expanding the definition of sensitive information), granting absolute opt-out rights in relation to restricted practices (see Chapter 14), or by ensuring that explicit notice for restricted practices is mandatory.

It is desirable to have a grey list of practices that require a privacy impact statement. Additionally, thought should be given to a 'black-list' approach. There is no justification for conduct that seeks to influence an individual's behaviour or decisions on a large scale. Such practices should be banned as contrary to ideals of individual autonomy and agency. A similar position may be reached with other high-risk activities.

A commitment to an obligation of fair and reasonable processing means that consent should not justify potentially harmful or intrusive practices. This provision may suggest the contrary and should not be included.

12. Pro-privacy default settings

12.1 Introduce pro-privacy defaults on a sectoral or other specified basis.

6. *Option 1 – Pro-privacy settings enabled by default: Where an entity offers a product or service that contains multiple levels of privacy settings, an entity must pre-select those privacy settings to be the most restrictive. This could apply to personal information handling that is not strictly necessary for the provision of the service, or specific practices identified through further consultation.*

7. *Option 2 – Require easily accessible privacy settings: Entities must provide individuals with an obvious and clear way to set all privacy controls to the most restrictive, such as through a single click mechanism.*

Option 1 with pro-privacy, or privacy by design, defaults are desirable. It is not sufficient to instruct entities to provide individuals with a way of controlling privacy settings even if clear and accessible. Most individuals are unlikely to pursue these pathways. Moreover, it is possible for firms to use choice architecture or 'dark patterns' to 'nudge' consumers to privacy eroding settings.[12]

16. Direct marketing, targeted advertising, and profiling

16.1 The right to object, discussed at Chapter 14, would include an unqualified right to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing. An individual could still request not to receive direct marketing communications from an organisation. If an organisation provides marketing materials to an individual, it must notify the individual of their right to object in relation to each marketing product provided.

On receiving notice of an objection, an entity must stop collecting, using, or disclosing the individual's personal information for the purpose of direct marketing and must inform the individual of the consequences of the objection.

Such a measure while useful, should be strengthened by an overriding obligation of reasonable and fair data, collection processing and use.[13]

[12] See further Paterson, J. M., Bant, E. and Cooney, H 2021, 'Australian Competition and Consumer Commission v Google: Deterring misleading conduct in digital privacy policies,' Communications Law - Journal of Computer, Media and Telecommunications Law, vol.26, no.3, pp. 136-148.

[13] Clifford, Damian, and Paterson, Jeannie. "Consumer Privacy and Consent: Reform in the Light of Contract and Consumer Protection Law". *Australian Law Journal*, vol.94, no.10, 2020, pp. 741-751; Taylor MJ and Paterson JM 'Protecting Privacy in India: The Roles of Consent and Fairness in Data Protection' (2021) Indian Journal of Law and Technology 16(1).

17. Automated decision-making

17.1 Require 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 people's rights.

Transparency about data use for automated decision-making is desirable, but again subjective protections are also required to protect the interests of individuals.

Part 3: Regulation and Enforcement

24. Enforcement

24.5 Amend paragraph 52(1)(b)(ii) and 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss. The current provision could be amended to insert the underlined:

> 8. *a declaration that the respondent must perform any reasonable act or course of conduct to identify, mitigate and redress any actual or reasonably foreseeable loss or damage suffered by the complainant/those individuals.*

We agree with the above proposal.

24.9 Alternative regulatory models

> 9. ***Option 1** - Encourage greater recognition and use of EDRs. APP entities that handle personal information could be required to participate in an EDR scheme. APP entities that are not part of a recognised EDR scheme could be required to pay a fee for service to the OAIC as the default complaint handling provider if a complaint is made against them.*
>
> 10. ***Option 2** - Create a Federal Privacy Ombudsman that would have responsibility for conciliating privacy complaints in conjunction with relevant EDR schemes.*
>
> 11. ***Option 3** - Establish a Deputy Information Commissioner – Enforcement within the OAIC.*

We prefer option 2. Ombudsman schemes are an accessible and effective way of supporting individuals to assert their rights and protect their interests in respect to personal data in circumstances where they are unlikely to have the resources to pursue a matter in court. A good model for such a service would be the Australian Financial Complaints Authority.[14] Ombudsman services typically both mediation and an inquisitorial model in resolving disputes which addresses the stark inequality of resources and experience as between individual complainants and firms.

An industry funded ombudsman tasked with resolving individual complaints would leave the OAIC to focus on disciplining the market and privacy policy. The work of the ombudsman would complement that of the OAIC, particularly if that ombudsman was subject to an obligation to report systematic contraventions of the Privacy Act.[15]

[14] See e.g., discussion of the Australian Financial Complaints Authority in Bolitho, H., Howell, N. and Paterson, J 2020. Duggan & Lanyon's Consumer Credit Law, 2 edn, LexisNexis Butterworths, ch 22.

[15] As is the case with AFCA.