REVIEW OF THE PRIVACY ACT 1988 ISSUES PAPER SUMBSISSION

Felix Harvey

29 November 2020

Introduction

I would like to thank the Attorney-General for the opportunity to provide a submission in relation to the review of the *Privacy Act 1988*.

The ever-increasing collection, processing and sharing of personal data in conjunction with shifting societal attitudes and awareness of privacy issues clearly demonstrates the need to have strong and robust privacy legislation.

I feel Australia is well posistioned to become a global leader in privacy legislation and I welcome the ongoing consultation and feedback from the general public to guide and provide input into possible reforms for the *Privacy Act 1988*.

This submission will focus on issues primarily from the perspective of a user, customer or consumer and not from the point of view of a business or other stakeholder.

This submission will narrowly address a select few questions posed by the Issues Paper. Specifically, this submission will provide responses and recommendations in relation to question 5, 25, 27, 32, 39 & 46.

Individuation

The Issues Paper asks the following question:

> 5. Are any other changes required to the Act to provide greater clarity around what information is 'personal information'?

I will submit that the definition of 'personal information' within the *Privacy Act 1988* should be ammended to extend beyond 'identifiability' and include 'individuation'. The notion that an individual cannot be be harmed simply because they cannot be identified is an outdated perspective on protecting privacy.

In their submission to the *Privacy Act 1998 Review – Issues Paper,* Salinger Privacy describe 'individuation' as the ability "to disambiguate or 'single out' a person in the crowd, such that they can be tracked, profiled, targeted, contacted, or subject to a decision or action which impacts them, even if that individual's 'identity' is not known". [1]

It is clear that individuation has the potential to cause harm to individuals. A contemporary example within Australia was the relase of myki data for a datathon. The myki card type is different for children and thus although the specific identity of an individual was unable to be ascertained, an adevesary could determine the travel patterns of unaccompanied minors. [2] This is clearly a breach of their privacy, regardless of whether their identity was able to be ascertained.

[1] See https://www.salingerprivacy.com.au/wp-content/uploads/2020/11/20-11-20_Privacy-Act-review_Salinger-Privacy_Submission.pdf

[2] See https://www.oaic.gov.au/assets/about-us/access-our-information/foi-disclosure-log/foireq20-00110.pdf

Protections

Notice

The Issues Paper puts forth the following question:

> 25. Would a standardised framework of notice, such as standard words or icons, be effective in assisting consumers to understand how entities are using their personal information?

I would suggest that the development of a standardised framework of notice would be valuable and effective at assisting the widest possible range of consumers as to the methods that APP entities are using their personal information.

Personally, I'm relatively privacy conscious, however, I rarely take the time to read a privacy policy in full. Primarily this is because the key information is often buried within lengthy documents compromised of legal jargon, which obfuscate how entities are using personal information.

Although there are inherent costs associated with implementing a standard framework such as the loss of nuance, detail and higher compliance costs, I believe that these limitations would be significantly outweighed by the benefits of implementing a standard set of icons or words.

There would be numerous benefits from the creation of a standardised framework including making comparisons between services much easier, reducing the time taken to glean the key uses of personal data and a greater awareness from consumers as to how their personal information is being used. This scheme would be particularly valuable for those less familiar with technical privacy jargon.

The need to interpret and understand privacy policies in a relatively short amount of time is crucial and extremely pertinent at the moment. As a consumer and as a current example, it is simply not feasible to read an entire privacy policy as you check into a restaurant and scan a QR code. However, the implementation of a standard framework with icons or a similar alternative would allow consumers to quickly digest and understand the 'why', 'what' and 'how' of an entity's personal information collection. For a consistent framework to be implemented successfully, widespread testing, consultation and feedback would be required to ensure that the right balance between specificity and understandability is obtained.

Recently, I tested out the CDR scheme by authorising the use of my financial data by a data recipient. The reasons why the data was needed, the specific data required, and the processes used to aggregate and transform the data were clearly explained, while simultaneously not overwhelming me.

Consent

The Deloitte Privacy Index 2020 highlights the role that meaningful consent plays in increasing consumer trust and also as the importance as a critical component of privacy in general. [3] The Issues Paper asks the following questions:

> 27. What approaches should be considered to ensure that consent to the collection, use and disclosure of information is freely given and informed?
>
> 39. Should entities be required to expressly provide individuals with the option of withdrawing consent?

For consent to be valid, freely given and informed I would expect that the following conditions must be met at an absolute minimum:

1. Explicit – the individual giving consent should have to 'opt-in'. The user should have to take action rather than a default option already selected for them.
2. Unbundled – the act of giving consent should not involve other consenting to other collection, use and disclosure methods. However, most importantly, consent should also not be bundled with accepting to terms and conditions.
3. Revocable – at any time a user should have the option of freely withdrawing the consent. If an entity provides a number of services for which the user has consented to, the options to withdraw should all be available in a single place.

Privacy by Design

> 32. Should entities collecting, using and disclosing personal information be required to implement pro-privacy defaults for certain uses and disclosures of personal information?

Yes, I think that similar to GDPR, 'Privacy by Design' & 'Privacy by Default' should be integrated within the *Privacy Act 1988*.

As Salinger Privacy describe in their submission, the responsibility for privacy protections should be placed with regulators and the organisations that hold personal information. It should not be the responsibility of an individual to determine if an entity's data practices are responsible or safe.

Right to Erasure

The right to erasure is also explored within the issues paper, specifically question 46 asks:

> 46. Should a 'right to erasure' be introduced into the Act? If so, what should be the key features of such a right? What would be the financial impact on entities?

I would recommend the 'right to erasure' or 'right to be forgotten' be introduced into the Act. The features of such a right would likely be similar to those found in the equivalent right contained within the GDPR.

---

[3] See https://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-australian-privacy-index-2020.pdf