Making privacy core business

Submission:

Consultation on the Privacy Act Review

For:

Attorney-General's Department

27 November 2020

Privcore Pty Ltd

ACN: 167 388 178

ABN: 46 167 388 178

Email: operations@privcore.com

Website: www.privcore.com

Address: Level 14, 5 Martin Place, Sydney NSW 2000

Andrew Walter
First Assistant Secretary
Integrity and Security Division
Attorney-General's Department

Via email to: PrivacyActReview@ag.gov.au

27 November 2020

Dear Mr Walter,

Submission: Consultation on the Privacy Act Review

Introduction

Thank you for the opportunity to participate in the consultation regarding the Australian Government's Review of the Privacy Act (the Review) arising out of the ACCC's Digital Platforms Inquiry Final Report (the ACCC's Final Report). This submission follows on from Privcore's submission to the ACCC's Final Report in 2019.

Privcore supports the review of the Privacy Act. Many of the issues in the Review have been raised before through other extensive consultation processes, including the previous Privacy Act law reform process, which resulted in some changes to the Privacy Act which came into effect in 2014.

Privcore notes that technology neutral principles based legislation supported by detailed regulatory guidance is most effective in rapidly changing digital and work environments. Unnecessary complexity, piecemeal approaches where some APPs apply and not others, and non-streamlined approaches should be avoided. Understanding where incentives lie to comply or not to comply with the Privacy Act are also essential in developing effective amendments to the Privacy Act. This is also particularly useful to consider when developing codes or certification mechanisms which by their nature tend to be voluntary and therefore require commercial appeal or other incentives to be effective and have uptake. For example, to date, there is only one voluntarily (not-regulator imposed) created code under the code-making provisions of the Privacy Act, the Privacy (Market and Social Research) Code 2014.

In today's digital era, it appears difficult for the Australian government to continue to support exemptions of substantial and key parts of the economy which process personal information. Comparable jurisdictions do not support similar exemptions. Rather areas that are currently exempt from the Privacy Act that may no longer remain exempt depending on the outcome of this review (such as employee records, small business and political parties) should be supported through appropriate and well-funded regulatory guidance with a grace period for compliance.

Further issues to consider

In addition to Privcore's submission to Treasury regarding the ACCC's Final Report, this submission further focuses on six additional issues that would be helpful to consider as part of this Review. They are based on Privcore's experience of issues that contribute to getting privacy right in practice. The six additional issues (with the closest corresponding Issues Paper question numbers) relate to:

- Expand APP 1 - Organisations knowing what data they hold and process [Q29]
- Focus on data minimisation and default "opt-ins" (express consent rather than implied consent) as a way to mitigate on flow privacy risks to go hand in hand with an individual deletion (or right to erasure) right [Q26, 27, 29, 32, 44, 46, 47]
- Leverage the insight from data breaches to educate regulated entities and sectors on prevention and mitigation steps to improve the effectiveness and impact of the NDB scheme [Q43, 63, 64]
- Introduce privacy impact assessments for high risk processing for regulated private sector entities [Q67, 68]
- Allow appeals from privacy complaint cases the OAIC closes (whether or not formally investigated by the OAIC) [Q54, 56]
- Points to consider - CBPR in Australia [Q50, 51]

1) Expand APP 1 - Organisations knowing what data they hold and process

If you don't know what personal information you have, why, how it is processed, where it is and where it goes to, you can't protect it. As such, one of the fundamental tasks for any organisation wanting to implement privacy in practice is undertaking an inventory of its personal information holdings and processing activities. Only then can you see whether data collections may be redundant, unnecessary, out of date, where they reside and the security controls that may or may not be in place. It is legislated to some extent in Article 30 of the GDPR as a "records of processing activities" requirement, but no similar requirement exists in the Privacy Act. Such a requirement could usefully be added to APP 1.

Recommendation: Consider expanding APP 1 to include ensuring that regulated entities know what data they hold and process.

2) Focus on data minimisation and default "opt-ins" (express consent rather than implied consent) as a way to mitigate on flow privacy risks to go hand in hand with individual deletion (or right to erasure) right

Many privacy risks, such as inappropriate use or disclosure, poor security, access and correction obligations can be reduced or avoided when a data minimisation approach is adopted. This first consideration is often overlooked and often consent is sought for the collection of personal information that is actually not required for the collectors' purposes. This is discussed in Privcore's submission in 2019 to the Consultation on Artificial Intelligence, Australia's Ethics Framework.

In circumstances where organisations need to rely on consent as a basis for using or disclosing personal information, it can be done in ways that are implied under the current Privacy Act. Consent is defined in section 6 as meaning "express consent or implied consent". OAIC guidance explains that consent (whether implied or express) constitutes the following elements:

- Informed
- Voluntary
- Current and specific
- Have capacity to give consent

It would be more difficult to show the above elements have been met where consent is implied. Strengthening the definition of consent, so that it can no longer be implied, and thus more aligned with OAIC guidance, as well as international definitions of consent, including GDPR (Recital 32) would tighten data practices that rely on inaction. Should the definition of consent remain unchanged, the right to erasure for individuals would become even more important as a counter-balancing measure to manage privacy risk.

Recommendation: Remove "implied" from the definition of consent in the Privacy Act.

3) Leverage the insight from data breaches to educate regulated entities and sectors on prevention and mitigation steps to improve the effectiveness and impact of the NDB scheme

To date, the OAIC has published nine reports on the NDB scheme which provide statistics on the types of data breaches, the sectors responsible and the type of personal information impacted. These statistics have been similar each reporting period, with no obvious improvements seen in terms of fewer data breaches or sectors changing practices to prevent data breaches. Consistently about two-thirds of data breaches relate to malicious or criminal activity (mostly to do with phishing or stolen credentials), a third are caused by human error and approximately 5% relate to system issues. Consistently the two main sectors which report data breaches are the health and finance sectors.

The OAIC is privy to a significant amount of insight that could be used to educate data breach prone sectors on better ways to manage personal information and prevent data breaches. For the NDB scheme to be more effective going forward, it would appear that the same problems should not keep showing up each reporting period, as it would suggest no lessons are being learnt by impacted sectors or privacy/security practices are not sufficiently changing.

Recommendation: Use the information obtained through the NDB scheme to drive changes to practices in impacted sectors to reduce known data breach risks.

4) Introduce privacy impact assessments for high risk processing for regulated private sector entities

With the increasing amount of artificial intelligence (AI) and automated decision making processes becoming embedded in personal information handling processes, it is becoming crucial that not only the government sector, but also the private sector assesses privacy impact of high risk processes. High risk processes are not just limited to AI or automated decision making processes, but could include any high risk processing involving personal information. The OAIC's guidance on "When do agencies need to conduct a privacy impact assessment?" outlines factors that lead to high risk processing activities which require a privacy impact assessment.

Recommendation: Introduce privacy impact assessments for regulated private sector entities, similar to requirements in the Privacy (Australian Government Agencies – Governance) APP Code 2017 for agencies

5) Allow appeals from privacy complaint cases the OAIC closes (whether or not formally investigated by the OAIC)

Under section 96 of the Privacy Act and as outlined in the OAIC's Guide to privacy regulatory action only determinations are appealable decisions. The Commissioner makes a determination in less than 0.1% of all privacy complaint cases lodged with the OAIC (since 1 November 2010, 40 determinations have been published on the OAIC's website). The bulk of complaints are closed without the use of determination making powers or use of investigation powers and are generally conciliated. In cases where a complainant believes their privacy has been interfered with and believes the respondent has not provided an adequate remedy and the OAIC closes the complaint (on the basis of it having been adequately dealt with for example), there are no pathways of redress for the complainant. This issue becomes increasingly important in circumstances where the OAIC has reduced resources to conduct investigations and has pressures to close cases quickly due to the volume of complaints it receives. As such, this issue should be taken into account in considering the introduction of a direct right of action.

Recommendation: Introduce direct right of action or allow appeals from closed OAIC complaint cases.

6) Points to consider - CBPR System in Australia

The Australian Government successfully applied to have Australia included as a participating economy in the Cross Border Privacy Rules System (CBPR System) and was endorsed by APEC in November 2018. There are some further steps to make it fully operational in the Australian market as outlined in a paper the author drafted in her previous role and APEC published. This most likely includes developing a code to ensure the OAIC can enforce the CBPR System, should a certified entity be in breach of a CBPR System requirement that is not otherwise resolved. APEC also published a paper on the benefits of the CBPR System for which the author was the Lead Author in her previous role.

Conclusion

As issues are fully crystallised, impacts are assessed and drafting strategies are explored, Privcore would be pleased to contribute to these further discussions in targeted consultation meetings and to assist in the privacy reform agenda.

Our submission is able to be made publicly available.

Yours sincerely

Annelies Moens

Annelies Moens

Managing Director

About Us

Privcore's team with 40 years' combined experience helps business and government make privacy core business, so they can deliver services with the trust and confidence of customers and citizens.

Annelies Moens, CIPP/E, CIPT, FIP, FAICD, CMgr FIML, a privacy professional practising since 2001 founded Privcore and is a former President of the International Association of Privacy Professionals which she co-founded in Australia and New Zealand. She has been instrumental in shaping and building the privacy profession in Australia and New Zealand and influencing privacy developments in APEC. She had the benefit of resolving hundreds of privacy complaints whilst working at the Australian privacy regulator and consults globally on privacy. Her bio is available at: www.privcore.com/bios.