Making privacy core business

Submission:

Privacy Act Review – Discussion Paper

For:

Attorney-General's Department

7 January 2022

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

Attorney-General's Department
4 National Circuit
BARTON ACT 2600

Via email to: PrivacyActReview@ag.gov.au

7 January 2022

Dear Attorney-General

Submission: Privacy Act Review – Discussion Paper

Introduction

Thank you for the opportunity to participate in the consultation regarding the Attorney-General's Department Review of the Privacy Act Discussion Paper (the Discussion Paper). This submission follows on from Privcore's submissions to the ACCC's Final Report in 2019 and in response to the Attorney-General's Department Privacy Act Review Issues Paper in late 2020. Privcore will not repeat what it has already submitted in earlier submissions, which also cover some of the questions raised in the Discussion Paper.

Whilst the Discussion Paper highlights 67 proposals for change to the *Privacy Act 1988* (Cth) (the Privacy Act), Privcore has focused this submission on five key areas. Overall, Privcore considers that each of those 67 proposals for change should be considered carefully from the perspective of the individual consumer and citizen. Where proposals increase regulatory burden or complexity on regulated entities without commensurate increases in privacy protections for consumers and citizens, then those proposals should be reconsidered with a view to understanding the benefit to those the Privacy Act is designed to protect (ie consumers and citizens). For example, increasing regulatory complexity regarding potential controller and processor distinctions has limited, if any, benefit to consumers and citizens' privacy.

Further issues to consider

This submission further focuses on five key areas. They are based on Privcore's experience of issues that contribute to getting privacy right in practice. The five key areas (with the closest corresponding Discussion Paper page numbers) relate to:

- APP 11 – Reasonable steps to take under the security principle [pages 146-147]
- Proposed transparency around the OAIC's complaint handling [page 182]
- APP 5 – Information that should form part of a privacy notice [page 70]
- Proposed fair and reasonable test [pages 80-91]
- Small business and employee records exemption [pages 40-57]

1) APP 11 – Reasonable steps to take under the security principle

Based on Privcore's experience, APP 11 is one of the most commonly breached APPs, either through failing to destroy or de-identify personal information no longer required or not taking reasonable steps to secure personal information, as commonly seen through preventable data breaches.

Regulated entities do not commonly understand what are reasonable steps to take to comply with APP 11. For example, many regulated entities still engage in extensive collection of personal information without adopting multi-factor authentication to better secure access to that personal information. This includes entities that store and collect personal information on behalf of other regulated entities.

As such, Privcore welcomes the opportunity the review of the Privacy Act and the Department of Home Affair's work on strengthening Australia's cybersecurity regulation provide to codify what are reasonable steps to take under APP 11. Such steps will need to have enough flexibility to cater for technological developments.

In particular, consideration should be given to harmonising requirements with the Australian Cyber Security Centre's Essential 8 as a starting point and any other appropriate and effective security standards when developing the proposed code under the Privacy Act's code making powers.

2) Proposed transparency around the OAIC's complaint handling

The Discussion Paper proposes amending the *Australian Information Commissioner Act 2010* (Cth) to increase the annual reporting requirements of the OAIC to include the outcome of all complaints lodged including the number dismissed under each ground of section 41 of the Privacy Act.

Privcore welcomes increased transparency around complaint handling, including reporting reasons for closure of investigations and the number of preliminary enquiries under section 42 that lead to the opening of investigations. There should be enough meaning and granularity in reporting rather than merely stipulating the closure ground under section 41. For example, closing an investigation on the basis that it has been adequately dealt with under section 41(2)(a) does not provide any indication as to whether the complainant accepted the matter as having been adequately dealt with.

Whilst the OAIC also publishes determinations, it does not commonly publish the outcomes of privacy complaints and common everyday scenarios raised by complaints. In Privcore's experience many regulated entities don't appreciate what ordinary and common privacy complaint scenarios arise. It would be helpful for not just unusual or outlier cases to be published through determinations, but also everyday common privacy complaint scenarios, so that regulated entities can focus on getting common and ordinary privacy issues resolved.

3) APP 5 – Information that should form part of a privacy notice

In Privcore's experience, few regulated entities fully understand the distinction between an APP 1 Privacy Policy and an APP 5 Privacy Notice. The latter is particularly valuable as it is the information required to be given to consumers and citizens generally at the touchpoint at which their personal information is collected. As such, there is immediate context and meaning for the consumer and citizen. A Privacy Policy, in contrast, is generally significantly longer and designed to cover the entire entity's personal information handling practices and is less likely to be read by the consumer and citizen.

The Discussion Paper proposes the removal of certain aspects from an APP 5 Privacy Notice, namely:

- Whether the collection of the personal information is authorised or required by an Australian law or court/tribunal
- The main consequences (if any) if the personal information is not provided
- Whether the personal information is likely to be disclosed to overseas entities
- If it is likely to be disclosed to overseas entities, the relevant countries those recipients are located

All of the above, should they be relocated to a Privacy Policy as proposed, would likely have less meaning to the consumer and citizen, as well as being less likely to be read by the consumer and citizen, as Privacy Policies are not frequently accessed. This can be seen by numerous surveys and research studies on the low-level of readership of Privacy Policies, some of which are also referenced in the Discussion Paper.

It would seem, however, that some other information contained in the APP 5 Privacy Notice requirements could comfortably be removed to shorten them and a link provided to the Privacy Policy containing information outlined in APP 5.2(g) and (h), namely:

- That the APP privacy policy contains information on how to access and correct personal information
- That the APP privacy policy contains information on how to lodge a privacy complaint

In Privcore's experience, as outlined above, APP 11 is one of the most commonly breached APPs, particularly around retaining personal information longer than for the purposes it was initially collected. As such, it would be useful to include a requirement in the APP 5 Privacy Notice that the maximum period of retention be outlined and/or information on when the collected personal information will be destroyed/de-identified or anonymised. This would assist in the operationalisation of APP 11.2 in practice, as it would require regulated entities to turn their mind to this more routinely.

4) Proposed fair and reasonable test

The Discussion Paper proposes a new test that personal information must not only be collected lawfully and by fair means under APP 3, but also its use or disclosure under APP 6 (and collection under APP 3) must be fair and reasonable in the circumstances.

There is very limited information regarding the existing operation of the lawful and fair means requirement for the collection of personal information under APP 3, as it is not a commonly complained about provision. Based on complaints lodged with the OAIC in 2020-2021 fewer than 13% of complaints related to APP 3 (see page 126 of the OAIC's 2020-2021 Annual Report). That percentage would encompass a broad range of collection issues, not just lawful and fair means of collection issues. So, the actual percentage of complaints dealing with unlawful or unfair means of collection would be extremely small.

Introducing a 'fair and reasonable' test has the potential to introduce significant grey areas into the interpretation of the Privacy Act, even where guidance is provided and/or criteria are included in

legislation, as what is fair and reasonable to one person is not to another. It may also be difficult to determine community expectations which may have a bearing on what is 'fair and reasonable'. As such, the proposed test may be complex to apply in practice with a wide latitude for interpretation.

It is also not clear that the introduction of such a test would fully resolve the identified problem the proposed test is seeking to resolve, namely shifting "the growing burden of maintaining privacy protections from consumers to APP entities" (p.478 ACCC Digital Platform Final Report). Indeed, the ACCC in its Final Report stated that such a test "could mitigate **some** of the information asymmetries, bargaining power imbalances and behavioural biases identified in this chapter that lead to consumer harm from unfair uses of personal information such as discriminatory targeting" [emphasis added].

The Discussion Paper also proposes amending the objectives of the Privacy Act, with a change to make it clear "that the subjective interests of entities are not relevant if their functions and activities are not in the public interest" in relation to balancing their interests with privacy (see p.20-21 Discussion Paper). This proposed change to the objectives would be a significant addition to the Privacy Act to potentially help determine appropriate boundaries and purposes for processing personal information.

5) Small business and employee records exemption

Employee records exemption

There are three key circumstances in which the employee records exemption does not currently apply, namely to:

1) government entities regulated by the Privacy Act;

2) entities that store and process current and former employees' personal information on behalf of their customers, for example suppliers of payroll and human resource platforms;

3) the handling of Tax File Numbers in employee records, so for example, if a private sector entity were to experience a notifiable data breach involving Tax File Numbers of its employees it would not be able to rely upon the exemption not to notify.

The application of the APPs and the notifiable data breach scheme in the above three contexts to employees' personal information is clearly workable in practice. Extending it to all regulated private sector entities with a direct relationship to their employees would appear to be a small leap. Having some employees' personal information protected in some contexts and not others as outlined above appears to create an unequal playing field for non-insurmountable policy reasons. Other jurisdictions with equivalent privacy laws do not see the need to have an equivalent employee records exemption.

Small business exemption

There has been a strong instinct in the Australian context over the last two decades to ensure that small businesses are not regulated by the Privacy Act, largely due to the perceived compliance burden it may have on small businesses.

Small businesses represent around 95% of all businesses in Australia, based on the turnover definition in the Privacy Act. As such, removing the exemption would have significant impact (not necessarily negative impact) in Australia.

Considering the current digital and data driven economy and the increasing levels of ransomware and other data breaches occurring, the question to ask is whether it remains sensible to exclude such an enormous portion of the Australian economy from privacy regulation? Businesses, governments, consumers and citizens work and live in an ecosystem where risk has unlimited boundaries. The lack of sufficient privacy protections of one entity can impact many other businesses, governments, consumers and citizens. For example, credential stuffing attacks on business and government due to poor privacy practices of small businesses. Why leave such a large gap to be exploited by those seeking to cause havoc in Australia's ecosystem? It would appear timely for the small business exemption to be seriously reconsidered and small businesses to be supported to achieve baseline privacy protections to serve all interests, including those of small business.

Conclusion

As 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.

Privcore's submission may be made publicly available.

Yours sincerely

Annelies Moens

Annelies Moens

Managing Director

About Privcore

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. Privcore conducts privacy impact assessments, privacy health checks or audits, data breach prevention and recovery, privacy by design, builds privacy programs, provides advice, policies and conducts research into privacy and cybersecurity.

Annelies Moens, CIPP/E, CIPT, FIP, FAICD, CMgr FIML, a Superstar of STEM in 2021-2022 and a privacy professional practising since 2001 founded Privcore. She has led and conducted hundreds of privacy consulting deliverables globally. She is a former President of the International Association of Privacy Professionals which she co-founded in Australia and New Zealand in 2008. She has been instrumental in shaping and building the privacy profession in Australia and New Zealand and influencing privacy developments in APEC. She also has extensive privacy regulatory experience and resolved hundreds of privacy complaints whilst working at the Australian privacy regulator.