Making privacy core business

Submission:

Privacy Act Review Report 2022

For:

Attorney-General's Department

27 March 2023

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

27 March 2023

Dear Attorney-General's Department

Submission: Privacy Act Review – Report 2022

Introduction

Thank you for the opportunity to participate in the consultation regarding the Attorney-General's Department Privacy Act Review Report 2022 (Report 2022). This submission follows on from Privcore's submissions to the ACCC's Final Report in 2019, Privcore's response to the Attorney-General's Department Privacy Act Review Issues Paper in late 2020 and Privcore's response to the Attorney-General's Department Discussion Paper in early 2022. Privcore will not repeat what it has already stated in earlier submissions, rather focuses on two new aspects not previously raised as areas considered for change by the Attorney-General's Department.

Overall, Privcore's view is that the vast majority of the 116 proposals for change move privacy regulation in the appropriate direction, clarifying and strengthening privacy protections in a number of areas. It particularly notes the proposed changes to the objects of the Act to clarify that the Act is about the protection of personal information and the public interest in protecting privacy. As such, in making proposals for change, the uplift to consumers/citizens' privacy should be at the centre.

New areas for change not previously raised by the Attorney-General's Department

This submission focuses on two new proposals:

1) Proposal 15.2 – Expressly require that APP entities appoint or designate a senior employee responsible for privacy within the entity. This may be an existing member of staff of the APP entity who also undertakes other duties.

2) Proposal 22.1 – Introduce the concepts of APP entity controllers and APP entity processors into the Act.

1) Proposed introduction of senior employee responsible for privacy

It is not clear from this proposal whether contractors and outsourced privacy officer service providers would be disallowed from being appointed with privacy responsibility of entities. Most organisations don't have the resources to appoint employees responsible for privacy nor do they have staff with privacy expertise, regardless of level. Many organisations would not have privacy officers or senior level chief privacy officers (whether full-time or otherwise). This would be

particularly the case for small businesses which are proposed to come within the purview of the Privacy Act.

The New Zealand Privacy Act 2020 allows agencies to appoint individuals from "outside the agency" as privacy officers. For a discussion of the reasoning behind this and benefits, the former Assistant Commissioner, who worked at the Office of the Privacy Commissioner in New Zealand for 25 years published 'Contracting out privacy officers in new NZ privacy law'.

Likewise, Article 37(6) of the General Data Protection Regulation (GDPR) enables the data protection officer to be either a staff member or the tasks may be fulfilled on the basis of a service contract.

As such, it would appear that this proposal, whilst appropriately requiring a senior level, should be broadened to enable independent expertise from outside the entity to also be able to provide such senior level privacy services. In full transparency, Privcore provides such outsourced privacy services to clients.

2) Proposed introduction of APP entity controllers and APP entity processors

Proposals that increase regulatory burden or complexity on regulated entities, in Privcore's view, need to have a cost/benefit analysis undertaken of the benefit to those the Privacy Act is designed to protect (ie consumers and citizens) and the costs to all stakeholders to inform whether or not the proposal should proceed.

This needs to be considered particularly in the context of the potential introduction of a controller and processor distinction. The proposal appears to increase burden and complexity without commensurate increases in privacy protections for consumers and citizens. The Law Council in its submission on the Discussion Paper stated that "introduction of new definitions of controllers and processors would otherwise interfere with contractual arrangements and descriptions of responsibilities and rights of the parties without a corresponding privacy benefit to individuals". In Privcore's view, the benefit to consumers and citizens of introducing such a distinction needs to be sufficiently strong to outweigh the apparent increase in regulatory burden and complexity on regulated entities and costs that such a distinction would introduce.

Citizens and consumers who are affected by interferences with privacy cannot be expected in all circumstances to understand whether they are dealing with a controller or processor, or attempt to locate that information. It is not uncommon, when multiple stakeholders are involved and wrongdoing is alleged, consumers and citizens are advised to address their complaints to other stakeholders – leading to a "run around" which is of no benefit to a consumer or citizen. It may also impact the timing of complaint lodgement with the OAIC, considering that the 'respondent' needs to have an opportunity to respond to the matter for 30 days, before the OAIC will consider the complaint.

The OAIC may also consider that controllers and processers have incorrectly defined their responsibilities as part of an investigation. This can already be seen in EU decision making under the GDPR (and prior Directive) from where the controller-processor distinction is derived. Case law also already shows that controllers and processors will attempt to lay the blame for alleged

breaches of privacy with the other party(ies). This happens when a distinction is created and different responsibilities apply (ie: fewer responsibilities for processors).

For example, in Azienda Ospedaliera di rilievo nazionale “A. Cardarelli” 160 - 17.9.2020, the hospital (the controller) organized a competition on its website, whereby personal data was inappropriately published. The controller argued it had no responsibility, as the inappropriate publication was due to the malpractice of its third party supplier (the processor). There appeared to be website security flaws that enabled the publication. The Italian data protection authority held the controller did not provide the processor with the necessary instructions, nor did it supervise or review the security of the data processed by the processor. For these reasons, the responsibility of the security incident could not be attributed solely to the processor as the controller argued. The controller failed to adopt adequate technical and organisational measures to ensure the confidentiality and integrity of the personal data processed through the processor's platform.

In circumstances where processors purportedly operate beyond the scope designated by the controller, consideration needs to be given to where responsibility lies. The Australian Privacy Act has adopted the APEC concept of accountability, particularly in relation to cross-border data flows and ensuring notification occurs with respect to eligible data breaches. Notification risks err on the side of over-notification, rather than under-notification, by enabling any party involved in the eligible data breach to make the notification (thus erring on the side of over-notification if parties have not determined in advance who will be doing the notifying). An accountability approach ensures there are no gaps from a privacy protection perspective for the consumer and citizen.

As such, in circumstances where processors inappropriately handle personal information (and possibly go bankrupt (consider, for example, the matter involving Facebook and Cambridge Analytica), the Privacy Act should make clear whether the controller becomes accountable for those actions. In contrast, under Article 28(10) of the GDPR, “processors going beyond the controller’s instructions” are deemed to be controllers when they act outside the controller’s instructions. The accountability does not rest with the initial controller. This was recently seen in a Greek DPA decision, 47/2022.

Ultimately, in Privcore’s view, consumer and citizen privacy needs to be protected from inappropriate handling of personal information, with appropriate recourse, regardless of any distinction. Currently, the Australian privacy law operates without a controller-processor distinction in an effective manner.

Should the distinction be introduced, complexity and cost of regulation and doing business are likely to increase, with costs inevitably passed onto consumers and citizens. For every transaction involving personal information, regulated entities would need to determine whether they are acting as a controller or a processor (or joint controller). The regulator would need to assess whether those distinctions are appropriate in the factual circumstances of complaints, thus also increasing regulatory burden.

As such, the benefit to consumers and citizens of introducing the distinction needs to be determined, the costs to stakeholders, as well as ensuring no gaps for recourse for interferences with privacy should such a distinction be introduced. The distinction should not be adopted where there is no commensurate increase in privacy protection for consumers and citizens, just added complexity and burden (and potentially less privacy protection for consumers and citizens).

Conclusion

As costs and benefits are assessed and drafting strategies explored, Privcore would be pleased to contribute to any further reform discussions.

Privcore's submission may be made publicly available.

Yours sincerely

Annelies Moens

Annelies Moens

Managing Director

About Privcore

Privcore's team with over 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 by design, privacy health checks, algorithimic impact assessments, data breach prevention and recovery, builds privacy programs, provides advice, policies, privacy officer services 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.