



Committee Secretary
Finance and Public Administration References Committee
Department of the Senate
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Committee Secretary

Submission to the Inquiry into the digital delivery of government services

I welcome the opportunity to comment on the matter of digital delivery of government services as part of the Inquiry by the Finance and Public Administration References Committee.

By way of overall comment, I am broadly supportive of the increased focus on the digital delivery of government services, which aims to make it easier and faster for the public to access the information and services they need. However, the personal information entrusted to government to deliver these services must be respected, protected and handled in a way that is commensurate with broader community expectations about privacy.

The automated nature of digital service delivery has the potential to create new privacy concerns or amplify existing privacy issues. As with all government initiatives, agencies delivering digital services should consider whether the use of personal information strikes an appropriate balance between achieving the objectives of the project and any impact on privacy. Agencies should also ensure transparency in relation to their information-handling practices, so that individuals know how their personal information will be managed.

I strongly encourage agencies to ensure that privacy is a key consideration in early stages of their project, and throughout its lifecycle, by taking a 'privacy-by-design' approach. Having good privacy practices, together with effective communication and community engagement strategies, can help to build public trust in digital service delivery, and ensure that the handling of personal information is consistent with the community's expectations.

I provide some further comments in this regard below.

Australian Government agency obligations under the Privacy Act

Australian Government agencies are bound by the *Privacy Act 1988* (the Privacy Act). The Privacy Act contains the Australian Privacy Principles (APPs), which are the cornerstone of the

privacy protection framework in the Privacy Act. The APPs set out the standards, rights and obligations that apply in relation to the collection, use, disclosure and storage of personal information. The APPs are technology neutral, applying equally to paper-based and digital environments. This is intended to preserve their relevance and applicability, in a context of continually changing and emerging technologies.

Importantly, the APPs require agencies to be open and transparent with the public about how they handle personal information. For example, agencies are required to have a clearly expressed, up-to-date and freely available privacy policy (APP 1), and to take reasonable steps to notify an individual of certain matters when collecting their personal information (APP 5). These measures facilitate accountability of entities' personal information handling practices, which in turn can build community confidence.

If specific information-handling practices are required or authorised by an Australian law, the APPs may not apply (or may apply with modifications).¹ However, the agency would still be required to comply with the privacy principles which relate to transparency and security of personal information.

Where an agency is not meeting its obligations under the APPs, I can receive individual complaints and/or investigate on my own initiative.²

Privacy by design and Privacy Impact Assessments

Adopting a 'privacy-by-design' approach is about finding ways to build privacy into systems and projects from the design stage onwards.³ This helps agencies at the outset to take steps that minimise risks to an individual's privacy, while also optimising the use of data.

Privacy impact assessments (PIA) are an important tool that can assist in facilitating 'privacy-by-design'. A PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. For example, undertaking a PIA can assist agencies to:

- describe how personal information flows in a project
- analyse the possible impacts on individuals' privacy
- identify and recommend options for avoiding, minimising or mitigating negative privacy impacts, and
- build privacy considerations into the design of a project.

I strongly encourage agencies to conduct a PIA for all projects that involve new or changed personal information handling practices.⁴ This includes projects that apply new technologies

¹ See APPs 2, 3, 5, 6, 9, 11 and 12

² The OAIC's *Privacy regulatory action policy* provides information on when and how I may exercise my function, available on the OAIC website at www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy.

³ Privacy by Design was first developed in the 1990s by the former Privacy and Information Commissioner of Ontario, Canada, Dr Ann Cavoukian. Since then it has been adopted by both private and public sector bodies internationally. For further information, see www.privacybydesign.ca.

⁴ For more information about PIAs, see the OAIC's Guide to undertaking privacy impact assessments and our Undertaking a Privacy Impact Assessment e-learning course available on the OAIC website at www.oaic.gov.au.

to existing personal information handling processes. Where appropriate, I would also encourage agencies to publish their PIA reports. Publication contributes to the transparency of the project's development and intent, and demonstrates to stakeholders and the community that the agency has undertaken a critical privacy analysis of the project.

Australian Public Service Privacy Governance Code

On 18 May 2017, I announced the development of the *Australian Public Service Privacy Governance Code* (the Code) that will apply to all Australian Government agencies that are subject to the Privacy Act. The Code is being developed by my Office, with the support of the Department of Prime Minister and Cabinet. The Code will come into effect on 1 July 2018 and will play a key role in building public trust and supporting strong privacy governance and capability in Australian Government agencies.⁵

The Code will set out the specific requirements and key practical steps that an agency must take as part of complying with APP 1.2 (which requires reasonable practices, procedures and systems in place to comply with the APPs).

Importantly, the Code will require all agencies to undertake a PIA for 'high privacy risk' projects or initiatives that involve personal information. My decision to include a specific requirement on PIAs highlights how vital they are for facilitating privacy compliance and best practice in the development of government programs and projects, particularly those involving the digital delivery of services.

If you wish to discuss any of these matters further, please contact Sarah Ghali, Director Regulation and Strategy, at [redacted] or [redacted].

Yours sincerely


Timothy Pilgrim PSM
Australian Information Commissioner
Australian Privacy Commissioner

15 September 2017

⁵ Further information on the Code can be found on the OAIC website at www.oaic.gov.au/engage-with-us/consultations/aps-privacy-governance-code.