

Privacy and local government: The Privacy and Responsible Information Sharing Bill 2024

By Austen Mell

Whilst local governments have to date been an exempt entity under the *Federal Privacy Act 1988* (Cth) (**Federal Privacy Act**), local governments are set to become a designated public entity in new legislation being introduced into WA Parliament that seeks to protect the privacy of personal information kept by local governments and regulate how such information is handled.

Overview of Privacy and Responsible Information Sharing Bill

On 16 May 2024, the WA Attorney General John Quigley introduced the 'Privacy and Responsible Information Sharing Bill 2024' into WA Parliament. The Bill lists its objects as being –

1. to promote responsible and transparent practices for handling personal information by IPP entities;
2. to balance the public interest in protecting the privacy of personal information handled by IPP entities with the public interest in the free flow of information;
3. to provide a means for individuals to complain about alleged interferences with their privacy;
4. to promote responsible information security practices by IPP entities;
5. to promote the responsible handling of information held by public entities as a public resource that supports government policy, programs and services;
6. to facilitate the responsible collection, use and disclosure for permitted purposes of information held by public entities;
7. to remove barriers that unnecessarily impede the responsible sharing of information held by public entities;
8. to provide protections in connection with the sharing of information, including by —
 - specifying the purposes for which, and the circumstances in which, information sharing is permitted or required; and
 - ensuring that information shared under the proposed Act is protected from unauthorised use or disclosure.

Not dissimilar to the Federal Privacy Act, the Bill details 'Information Privacy Principles' which apply to the abovementioned 'IPP Entities' with respect to personal information kept by those entities. This time, local governments are expressly designated as a 'public entity' within the definition of 'IPP Entity', and will therefore be required to comply with the Information Privacy Principles as an IPP entity (clause 20).

Information Privacy Principles

The 'Information Privacy Principles' are contained in Schedule 1 of the Bill and regulate broadly how an IPP entity may collect personal information, use and disclose personal information, and keep and maintain personal information regarding its correctness and security.

These are broadly aligned with the current Information Privacy Principles set out in the Federal Privacy Act. A notable distinction is the addition of a new principle which regulates how IPP entities may employ automated decision-making processes involving the use of personal information. This might be regarded as a response to calamities resulting from the use of automated decision-making at the Federal level in recent times,^[1] or a more global response to a growing adoption of processes by corporate entities making use of artificial intelligence.

The Bill allows for IPP entities to depart from compliance with the IPPs through adopting a privacy code of practice (clause 29), but these must be as stringent as the IPPs (clause 32(2)(b)), and must be approved by the Governor on recommendation of the Information Commissioner (clause 32).

'Personal information' is defined, broadly, to include information or an opinion that relates to an individual, living or dead, whose identity is apparent or can reasonably be ascertained from the information or opinion (clause 4, subclause (a) of the definition of **personal information**). The definition includes a list of the kinds of information referred to, which range from common identifiers such as contact information and a date of birth or address, to more complex identifiers such as 'technical or behavioural information in relation to an individual's activities, preferences or identity'.

A predictable exception to the application of the Information Privacy Principles under the proposed Act is 'publicly available information', which includes information contained in a document generally available to members of the public or published or available for inspection by members of the public (clause 22).^[2]

Interferences with Privacy

The Bill also sets out when an IPP entity is said to interfere with the privacy of an individual. This includes –

- doing an act or engaging in practice that contrary to, or inconsistent, with an Information Privacy Principle or a substituted approved privacy code of practice;
- failing to comply with prescribed actions in relation to a 'notifiable information breach' under the proposed Act;
- failing to comply with a direction from the Information Commissioner where the Information Commissioner reasonably suspects that a notifiable information breach has occurred;
- failing to respond to requests to remove personal information in certain circumstances (clause 15).

The Bill sets out that a 'notifiable information breach' occurs when personal information is accessed or disclosed without authorisation, or lost in circumstances where unauthorised access or disclosure is likely to occur, and in either situation serious harm is likely to occur to the person to whom the information relates (clause 57).

A person may make a privacy complaint to the Information Commissioner where there is alleged or suspected interferences with privacy (clause 82), and the Information Commissioner on its own motion may conduct investigations into the act or practice of an IPP entity that may be an interference with the privacy of an individual (clause 106).

In dealing with privacy complaints, and where it cannot be resolved informally between parties, the Information Commissioner must initiate a conciliation process between the individual subject of the complaint and the IPP entity (clause 95). As part of an agreement reached following conciliation, the Information Commissioner is empowered to make orders requiring action or compensation for loss or damage suffered by the actions or practice of the IPP Entity (clause 98).

Summary, application and next steps

This article has addressed just some of the privacy reforms which the Bill will bring about once it becomes law. Ultimately, the Bill is set to establish innovative and modern privacy legislation which responds to modern concerns about how public organisations collect and handle personal information. In a move not taken at the Federal level, local governments are now counted among these organisations. Not only is the proposed Act set to apply to local governments, it will also extend to service providers contracted by local governments (clause 130).

The Bill has undergone its first and second reading in Parliament, however as of the date of this article there is no further indication of the date it will become law as an Act of Parliament. Nonetheless, local governments should look to how personal information is currently handled within the organisation and be ready to respond to the proposed new law through internal and external policies and procedures.

The information contained in this article should not be relied upon without obtaining further detailed legal advice in the circumstances of each case. For any comments or questions on this article please contact Austen Mell by email to amell@mcleods.com.au.

Liability limited by a scheme approved under Professional Standards Legislation.

[1] See eg, Noel Cressie, 'Robodebt not only broke the laws of the land – it also broke laws of mathematics' (17 March 2023) *theconversation.com* <<https://theconversation.com/robodebt-not-only-broke-the-laws-of-the-land-it-also-broke-laws-of-mathematics-201299>>.

[2] Section 5.94 of the *Local Government Act 1995* provides a list of information which a local government must have publicly available for inspection.