Queensland's new Information Privacy Act a mixed bag

Graham Greenleaf & Nigel Waters, 8 July 2009

For publication in Privacy Laws & Business International Issue 100, August 2009

Queensland is now the sixth Australian State or Territory to have enacted a data protection Act covering its public sector (including local government), joining the ACT (1988), NSW (1998), Victoria (2000), Northern Territory (2002), and Tasmania (2004). Western Australia had a 2007-vintage Bill which has now lapsed, while South Australia has only administrative guidelines and an inactive oversight and advisory Committee. Queensland is a jurisdiction with a population and economy similar in size to a small Scandinavian country.

The *Information Privacy Act 2009* combines principles that hark back to the 1980s with an enforcement mechanism that is thoroughly up-to-date. It adds another layer of complexity to Australia's patchwork of privacy laws.

The scope of the Act is broad, covering most parts of Queensland's public sector including local government (s18), and Ministers but only in relation to the agencies they administer (s20). Complete exemptions are few (Schedule 2), the most significant being the Parliament, judicial aspects of adjudicative bodies, and government-owned corporations (as they are covered as private sector bodies by the Federal law).

Neo-classicism in Information Privacy Principles

The Act gives statutory effect to the two sets of administrative principles which Queensland agencies have been supposed to follow since 2001 (Information Standards 42 and, for the Health Department, 42A), although there has been no supervisory authority or reports on implementation.

The eleven Information Privacy Principles (IPPs) in the Schedule 3 of the Act are based squarely on the eleven similarly named principles applying to the Federal public sector in the *Privacy Act 1988* (Cth). However, they have numerous differences in wording, some with 'plain English' motivations but others being differences of substance. These principles also have many differences from the Uniform Privacy Principles (UPPs) proposed by the Australian Law Reform Commission in its review of the private sector and federal agency provisions (see Greenleaf and Waters, *Privacy Laws & Business* Issue 97), and so will need to be replaced if the ALRC has its way.

To add a little more complexity, the IPPs do not apply to the health department. Instead, the 'National Privacy Principles' (NPPs) in the *Privacy Act 1988* (Cth), which apply to private sector health providers in Queensland also apply to the Health Department (s31). The 1988-vintage IPPs do cover everything you would expect of OECD-influenced sets of principles. Missing are any post-1980s principles such as deletion/de-identification or data breach notification principles.

The Queensland IPPs inherit many deficiencies from their Federal cousins, including:

- Although collection is limited to data 'directly related' to an agency's lawful purposes, the finality principle is weakened in relation to disclosures because the collecting agency can merely declare in a notice to a data subject that it is its

'usual practice' to disclose the data to some other entity (not necessarily an agency) (IPP 1), and that notice is then in itself sufficient justification for the disclosure to the entity (IPP 11), provided the entity is only collecting the data for a legitimate purpose. By this means, agencies can 'bootstrap' disclosures that they could not otherwise justify.

- Requirements to give notice, to ensure data quality at time of collection, and to avoid intrusiveness, only apply if data is collected from the person concerned (IPPs 1 and 3), and not when collection is from a third party or (perhaps) by observation.

- Uses and disclosures need to be logged when made for investigative purposes (IPP 10(2) and IPP 11(2)), but not for any other purposes.

Innovations in the Queensland IPPs include:

- A broad exemption for both uses and disclosures for research or the generation of statistics, in the public interest, where publications are de-identified and obtaining consent is not practicable (IPPs 10 and 11).

- 'Disclose' is defined to mean where entity B did not know certain personal information and was not in a position to find out, and entity A either gives entity B the information or makes it possible for it to find out, and A ceases to control B in relation to who will know the information in future (s23). This definition has various implications, such as (a) information is not 'disclosed' if the recipient already knows the information (a dangerous rule, unless the source of the information is included as part of the information); and (b) there can be disclosure of information even if the discloser is not in possession of the information but discloses, for example, an access code on a third party's system.

- 'Use' of personal information is explicitly defined to include taking it into account in the making of a decision, and intra-entity transfers to a part of an entity with a different function (s23). Although 'use' and 'disclose' are key terms, such explicit definitions are unusual in Asia-Pacific data protection laws.

- An agency can disclose personal information to another entity for marketing purposes, but must ensure that entity complies with rules very similar to those governing direct marketing in the NPPs (IPP 11(4)).

In common with a trend in other Australian jurisdictions, the Act transfers access and correction rights and processes in relation to an individual's own personal information from the freedom of information legislation to the privacy law (Chapter 3).

A dodgy data export provision

Separate from the IPPs, there is a data export limitation principle (s33) which purports to limits transfers to 'an entity outside Australia' (not 'outside the State', unlike the equivalent controls in the Victorian and NSW laws). The conditions for a personal data export are based on NPP 9 in the Federal Act, but modified to apply to agencies, and also tightened so as to require a higher standard than the Federal provisions (which are not as restrictive as EU Directive Article 25).

Personal data cannot be so exported unless the individual agrees, unless the transfer is authorised or required under a law, or the agency reasonably believes that the transfer is necessary to prevent or lessen various types of 'serious threats', or unless the transfer meets at least two of four further conditions (any one of which was sufficient to meet the Federal provisions). The four conditions, in summary, are (i) reasonable belief in similar principles being enforceable at the export destination; (ii) necessary for performance of the agency's functions; (iii) for the benefit of the individual, and consent would have been likely if possible to obtain; or (iv) the agency has taken reasonable steps to ensure that recipient will act consistently with the IPPs.

The signal problem with this provision is that since it is located outside the IPPs, none of the Act's enforcement provisions apply to it. Both the requirements for a compliance notice (s158) and the privacy complaint provisions (s164) only apply to IPPs. The meaning of 'IPPs' is limited to what is in Schedule 3 (s25, s26 and Schedule 5 Dictionary). By the same token the commissioner cannot relax s33 any further by the waiver/modification procedure (s157), since it also only applies to an IPP. This is all either a result of negligence by the draftsperson (and the Parliament) or an indefensible policy choice of an unenforceable 'principle'. The latter seems unlikely, but the Explanatory Notes to the Bill shed no light.

Enforcement

A Privacy Commissioner is to be appointed as a deputy to the Information Commissioner, who can delegate powers to him (s139), and can direct him (s142). Both are referred to herein as 'the Commissioner'. The Information Commissioner's office is now being established as part of a conjoint review of Queensland's FOI law, following recommendations of the Solomon review of 2008. The Privacy Commissioner, although oddly described as a member of the Information Commissioner's staff (s141), is to be appointed after advertisement and after consultation with a Parliamentary Committee (s145) and can be re-appointed for up to a total of ten years (s146). The newly-established Queensland Civil and Administrative Tribunal (QCAT) commencing in December 2009, is to be the adjudicative body in relation to complaints.

The Act enables persons to make have a complaint about the handling of their personal information by an agency first to the agency for internal review (s166(2)), and then if the agency is unable to satisfy the complaint, to the Commissioner who must take all reasonable steps to mediate the complaint (s171). The terms of agreement of successful mediations can be certified by the Commissioner, and the terms then enforced by QCAT (ss172, 173).

The Act is, on paper, too rigid in its timing requirements and gives the Commissioner too much latitude to discontinue complaint investigations because of 'lack of cooperation' by complainants or other reasons (s168). Complainants cannot bypass the Commissioner and go directly to the Tribunal after internal review (in contrast to NSW), or to the Courts (s39). Much will depend on the Act being sympathetically administered.

If mediation is unsuccessful, then at the request of the complainant (only), unresolved complaints must be referred by the Commissioner to QCAT (s176). Following a hearing, QCAT will be able to make orders for a range of remedies for breaches of the privacy principles (s178), including requiring injunctions against continuing breaches, apologies, compensation of up to A$100,000, and reimbursement of expenses in

pursuing the complaint. This approach is most similar to that in the Victorian legislation.

Breaches of the IPPs can also result in the Commissioner issuing compliance notices to an agency, where a breach is 'serious or flagrant', or has occurred on five separate occasions in two years (s158). Agencies must take all reasonable steps to comply or they can be subject to a civil penalty (s160). They can seek a review by QCAT (s161).

The Commissioner has other broad powers including conducting reviews of any systemic privacy issues, reporting results to Parliament, 'conducting compliance audits' of any entities under the Act, commenting on any privacy issues relating to the public sector, and issuing guidelines on the application of the Act and 'privacy best practices generally' (s137). Much will depend on the size of the Commissioner's budget allocation to carry out these tasks, which is subject to government determination, but his/her priorities and exercise of powers are not otherwise subject to direction (s134).

The Commissioner also has a power of approving waivers or modifications of agencies' obligations to comply with the IPPs (s157). Such exemptions are called 'Public Interest Determinations' in the Federal Act, and as in that Act the Commissioner here must be satisfied that such a waiver or modification is in the public interest. In the Queensland Act there are no provisions for public hearings or submissions before such an approval is made, but it is treated as subordinate legislation (s157(2)) and is thus subject to Parliamentary disallowance.

Conclusions

Although this legislation is a mish-mash of good and bad provisions from various other Australian information privacy laws, and an equally inconsistent set of omissions and innovations, the overall result is probably no worse than other public sector laws in Australia. If it is effectively enforced it could be more useful than most of them, but as always that is the main question.