Appendix B

Review of the *Information Privacy Act 2009:* Privacy Provisions

Background

Objectives of the review: To identify key issues and challenges raised by implementation of the legislation and seek the views of interested persons, agencies or organisations about these issues.

Part 1 – Considering the Australian Privacy Principles (APPS) in Queensland

There are differences between the APPs and Queensland's IPPs including:

- a privacy principle addressing direct marketing;
- a requirement for all entities subject to the Act to have a privacy policy; and
- the need to distinguish 'sensitive information' and provide it with a different level of protection to other personal information.

Any alignment of the IPPs with, or adoption of, the APPs would mean a single set of principles would apply to all agencies subject to the IP Act and may result in less compliance burdens for organisations. The principles would continue to deal with the collection, storage, use and disclosure of information held by Government.

1.0 What would be the advantages and disadvantages of aligning the IPPs with the APPs, or adopting the APPS in Queensland?

There would be advantages of a single set of Information Privacy Principles as it would be simpler to communicate both internally and with our customers. A change to the legislation would require training and communication but longer term, it could be less of a burden to local government.

Part 2 – Sharing Information

At times it is necessary for government agencies to work together in the interests of the community. To enable information to be shared appropriately, the IP Act sets out where personal information may be shared and also recognises that compliance with the privacy principles is not appropriate in all circumstances.

Exceptions include*:*

- individual has agreed to disclosure; disclosure is necessary to lessen a threat to life, health, or safety; disclosure is authorised or required by law; or disclosure is necessary for law enforcement reasons;
- The privacy principles do not apply to certain documents (for example, certain documents relating to covert activity);
- The privacy principles do not apply to certain entities for example parents and citizens associations, or the Legislative Assembly;
- The Information Commissioner may give an approval that waives or modifies an agency's obligation to comply with the privacy principles; and
- Law enforcement agencies are not subject to some of the IPPs in some circumstances

Appendix B

Despite the above exceptions, concerns are sometimes raised that the IP Act unreasonably prevents the sharing of information, particularly across Government. Individuals (including public servants) are concerned that their personal information is adequately protected by Government. However, privacy laws should not prevent appropriate information sharing.

2.0 Does the IP Act inappropriately restrict the sharing of information? If so, in what ways? Do the exceptions need to be modified?

There are options for information sharing internally under the IP Act. Often there can be misunderstanding of the Information Privacy Principles which can result in delays to decisions. The exceptions need to be clear in any changes that are made.

Part 3 – Definitions of 'personal information'

The definition of personal information is central to the effective operation of the IP Act. It is therefore important to ensure that the definition captures that information which deserves protection. Currently personal information is defined as: *'…information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.'*

The ALRC is recommending it be changed to: *'... information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual.'*

The Commonwealth Privacy Amendment Act definition *means information or an opinion about an identified individual, or an individual who is reasonably identifiable (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.*

Modernising the definition in accordance with the Commonwealth *Privacy Amendment Act* would not significantly change the scope of personal information in Queensland.

3.0 Should the definition of personal information in the IP Act be amended to bring it into line with the definition in the Commonwealth Privacy Amendment Act 2012?

Yes. Council would support the amendment of the definition to make it consistent with the Commonwealth Privacy Amendment Act 2012.

Part 4 – Definition of 'agency' – Government Owned Corporations

There is an inconsistency between the RTI Act (which applies to GOCs) and the IP Act (which does not). There may be benefits in extending the definition of agency in the IP Act to cover GOCs. Queensland GOCs would then be subject to only one state regulatory regime. It may also be easier for those interacting with GOCs to have their rights provided for under state legislation. On the other hand, it may be more appropriate for GOCs to remain covered under the Commonwealth legislation. The NPPs to which GOCs are currently subject may provide a higher level of privacy protection to individuals than the IPPs in the IP Act. As GOCs often hold a substantial amount of personal information and operate in a commercial environment, it may be beneficial that they remain subject to the NPPs.

Appendix B

Providing for State and Territory entities which are incorporated companies, societies or associations in the Commonwealth legislation may also avoid inconsistencies and gaps in coverage, particularly as there is no privacy legislation in some states.

4.0 Should government owned corporations in Queensland be subject to the Queensland's IP Act, or should they continue to be bound by the Commonwealth Privacy Act?

Although Council would not be directly affected by the changes, we can see merit in GOCs being covered by one set of legislation, instead of coming under both state and commonwealth legislation.

Part 5 - Transfer of personal information outside Australia

The privacy principles contained in the IP Act only apply to Queensland State and local government agencies. If there is no privacy protection in the jurisdiction which receives the information, the personal information of Queenslanders will no longer be protected. It is therefore important that the personal information of Queenslanders is only transferred outside of Australia in appropriate circumstances. In Queensland section 33 of the IP Act restricts the circumstances under which personal information can be transferred outside Australia by Queensland Government agencies.

Technology issues

Government officers use a range of technology and is increasingly likely to use technological developments to increase efficiency. The use of such technology may result in the transfer of personal information outside Australia, in situations where the conditions in section 33 are not met. The OIC Commissioner recently stated its view that if personal information is merely routed through another country and immediately directed back to Australia it has not been transferred overseas. However, there may still be cases where information is stored on overseas servers.

5.0 Should section 33 be revised to ensure it accommodates the realities of working with personal information in the online environment?

With increasing developments in technology, Council is seeing more requirements for transfer of personal information overseas. It would be helpful if the legislation makes the requirements for overseas transfer absolutely clear. Council notes that there may be new technology developments over the coming years and it might be helpful for the legislation to be broad enough to capture the principles whilst allowing flexibility to cover emerging technological developments.

Part 6 – Cloud computing

Cloud computing usually involves storing or processing information outside Queensland. If it occurs through a 'private cloud' model, it is unlikely that section 33 will be relevant. However cloud computing services are more commonly hosted by service providers external to Government and located overseas, which requires information to be transferred outside Australia.

Appendix B

The requirements of section 33 will be met in some cases but not all. An OIC Information Sheet states: *A cloud services contract which robustly deals with the collection, storage, use and disclosure of information will go a long way towards satisfying the IP Act's overseas transfer rules*

Part 7 – Personal information published on agency websites

An OIC guideline makes clear that when agencies place personal information online, this is considered to be a 'transfer' for the purposes of section 33 of the IP Act. Agencies must therefore ensure that personal information is put online only in accordance with section 33 of the IP Act. Making it available to on a webpage makes it potentially available to anyone in the world. There could be instances where agencies may inadvertently contravene section 33 of the IP Act by publishing, for example, photos of individuals in a group or crowd where they are recognisable, and the requirements of section 33 of the IP Act have not been met.

An alternative approach to transferring personal information

An alternative to the current section 33 is the concept of 'accountability'. This would mean rather than preventing information being transferred, the IP Act could be amended so agencies would continue to be liable for breaches of the privacy principles when an individual's personal information is transferred outside Australia. Individuals could make a privacy complaint to the OIC if a breach occurred. The ALRC stated the policy position behind the concept of accountability was warranted by the high level of community concern attaching to cross-border transfers of personal information and the nature of the risks associated with such transfers. It however suggested exceptions (so that an entity would ***not*** remain accountable) when:

- the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to the privacy principles;
- the individual consents to the transfer, after being advised that the consequence of providing consent is that the agency will no longer be accountable for the individual's personal information once transferred; or the agency is required or authorised to transfer the personal information by or under law.
- Deciding whether other jurisdictions 'effectively uphold substantially similar privacy protections' to Queensland may however be challenging.

6.0 Does section 33 present problems for agencies in placing personal information online?

Section 33 does present challenges whenever information is placed online. Council would support more consistency of legislation across states.

7.0 Should an 'accountability' approach be considered for Queensland?

Council has developed a Cloud Service Policy and Guideline which outlines the strategy for the effective purchase, management and use of cloud services across Council and sets out responsibilities and a consistent approach. Council would support an accountability approach.

Appendix B

Part 8 – Privacy Complaints – a standard approach

The IP Act does not specify how a privacy complaint must be handled within an agency, meaning that there may be a lack of standardisation across the sector. In particular, the IP Act does not specify:

- requirements for lodgement of a privacy complaint to an agency (e.g. written, directed to a particular officer, outlines particular points to be addressed etc);
- timeframes for management of the complaint by an agency (including provision for extended timeframes where complaint is complex etc); or
- particular actions that must be undertaken (e.g. acknowledgement of complaint, investigation of circumstances raised by applicant, formal response to complaint).

This contrasts with very detailed processes specified for applications for access to and amendment of personal information held by an agency. While legislative processes need to remain flexible enough to accommodate differences between agencies, there may be benefits to standardisation.

8.0 Should the IP Act provide more detail about how complaints should be dealt with?

Council currently handles privacy complaints through its standard complaints process. There is currently very little detail in the legislation about what approach is expected. More guidance would be welcome but it is important to provide sufficient flexibility to accommodate a large variety of types of organisations covered by the legislation. In some cases, the privacy issue can form part of a more complex complaint.

Part 9 – Privacy complaints – timeframe for resolving

Section 166(3) of the IP Act provides that an individual must not make a complaint to the Information Commissioner unless they have made a complaint to an agency, the complaint has not been resolved to the individual's satisfaction and at least 45 business days has elapsed since the complaint was initially made to the agency.

Individuals may therefore complain to the Information Commissioner 45 days after their first complaint to the agency. However, agencies may not have finished dealing with the complaint at that point. Some agencies report it is difficult for them to resolve privacy complaints within the 45 day timeframe given other requirements. A privacy complaint may be part of another grievance (for example, a workplace dispute) which has different administrative timeframes or which is otherwise complex to resolve.

Alternatively, even if an applicant receives a response to their privacy complaint quickly, they must still wait until 45 business days have elapsed before bringing the complaint to the Information Commissioner.

9.0 Should the IP Act provide more flexibility about the timeframe for complaints to the OIC to be lodged?

If a complaint is resolved in less than 45 days and the complainant is not satisfied, they should be able to refer the matter to OIC, without waiting until 45 days from when their complaint had been submitted. Council has handled a very small number of complaints. In our experience 45 days has been sufficient time to investigate and respond.

Appendix B

Part 10 – Powers of the Privacy Commissioner

The Information Commissioner has a number of investigative powers which are necessary to perform external review functions under the IP Act and the RTI Act.

However, the same kinds of powers have not been given to the Information Commissioner (or Privacy Commissioner). The Information Commissioner must be 'satisfied on reasonable grounds' of the prerequisites to issue a compliance notice but it is difficult to see how a compliance notice could be issued without powers to investigate.
It could be argued that the Information Commissioner requires the same powers to investigate ongoing breaches of privacy as to investigate issues raised in reviewing access decisions.

10.0 Are additional powers for the Information Commission to investigate matters potentially subject to a compliance notice necessary?

It would seem appropriate that OIC have necessary powers to investigate privacy matters.

Part 11 – Person acting as an agent for a child

Section 196 allows a child's parent to do anything the child could do if the child were an adult, for access and amendment applications *or other matters under the Act*. This
means that a parent may be able to provide consent on behalf of a child for other matters involving the child's personal information. For example, they could consent on the child's behalf to disclosure of the child's information. In some circumstances this may not be appropriate, for example in the case of a 16 year old child who may be able to make this decision themselves.

11.0 Should a parent's ability to do things on behalf of a child be limited to Chapter 3 access and amendment applications?

No comment. Other agencies better placed to comment.

Part 12 – Generally available publication

The IP Act provides that a 'document' that is a 'generally available publication' is a document to which the privacy principles do not apply. The term 'generally available publication' is defined at Schedule 5 as: *'…a publication that is, or is to be made, generally available to the public, however it is published.'* The definition does not provide clear guidance about what constitutes a generally available publication. In particular, it not clear that generally available publications include publications which are available for a fee.

The ALRC recommended that the Commonwealth definition (which definition is more specific) be amended to make clear that the definition includes documents that are available for purchase. The definition in the Commonwealth *Privacy Amendment Act* states:
generally available publication *means a magazine, book, article, newspaper or other publication that is, or will be, generally available to members of the public:*
(a) whether or not it is published in print, electronically or in any other form; and
(b) whether or not it is available on the payment of a fee.

Appendix B

12.0 Should the definition of 'generally available publication' be clarified? Is the Commonwealth provision a useful model?

Yes. The Commonwealth provision is a helpful model.

Part 13 – IPPs specific to documents

The IPPs in schedule 3 of the IP Act refer to 'documents'. For example:

- IPP 1 which , requires the collection of personal information be lawful and fair, and relates to the collection of personal information 'for inclusion in a document or generally available publication'; and
- IPP 11 which …. relates to disclosure of personal information, and applies to an agency 'having control of a document containing personal information'.
- This means that the privacy principles only apply where the personal information is in documentary form. Most personal information which becomes the subject of a complaint will be contained in a document. However, this limitation means:
- the obligation to comply with the privacy principles only relates to personal information contained in documents;
- a complaint about breach of the privacy principles can only be made where the personal information the subject of the complaint is contained in a document; and
- where a collection or a disclosure of personal information occurs verbally and is never reduced to writing or otherwise recorded then there is no breach of the IPPs.

In contrast, the NPPs do not have the same limitation.

13.0 Should the reference to 'documents' in the IPPs be removed; and if so how would this be regulated?

Yes, Council holds personal information in many different forms, such as databases, files and other systems. The term 'document' could cause misunderstanding about what is covered.

Part 14 – IPP4 – element of reasonableness

IPP 4 provides that an agency having control of a document containing personal information *must ensure* that the information is protected against loss and misuse etc. The strict requirement in IPP4 means that there is no element of reasonableness or a requirement to take reasonable steps as is the case in the other IPPs. In effect, an agency would be responsible for a breach of IPP 4 where, for example, an employee simply steals personal information, even where all possible measures have been taken to keep the information secure.

14.0 Should IPP 4 be amended to provide, in line with other IPPs, that an agency must take reasonable steps to ensure information is protected against loss and misuse?

Council agrees that IPP4 should be amended so the agency must take reasonable steps to ensure information is protected as there would be situations beyond Council's control.

Appendix B

Part 15 – IPP2 and 3 – 'Collect' information? Or 'ask for' information?

IPPs 2 and 3 deal with the collection of personal information. However IPP(2)(2) and IPP3(2) state that the sections apply 'only if the agency asks … for the personal information. This contrasts with equivalent principles in other jurisdictions and in NPP 1, all of which use the phrase 'collects personal information'.

This raises the issue of whether the word 'ask' requires that collection of personal information involves an active request by the agency to the individual in order for IPPS 2 and 3 to apply. If correct, where personal information is collected without an agency having actively 'asked' for it (such as the use of CCTV recordings in government buildings) the principles do not apply and no collection notice is required. Similar arguments would apply where automated tools track and record internet usage and forms are accessed, completed and submitted on an agency website.

15.0 Should the words 'ask for' be replaced with 'collect' for the purposes of IPPs 2 and 3?

Yes. Collect covers the different ways agencies might obtain personal information. There are situations where information is collected by Council without specifically asking for the information, so clarification would be helpful.