Department of Justice and Attorney-General

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

Discussion paper

August 2013

Contents

Minister's Foreword

The *Information Privacy Act 2009* (the IP Act) commenced on 1 July 2009, after an independent committee chaired by Dr David Solomon, AM, conducted a wide-ranging review of Queensland's *Freedom of Information Act 1992*. The IP Act complements the *Right to Information Act 2009*, which commenced on the same day.

We are committed to crafting a new integrity system for the state as we move towards making the government the most open and accountable in the nation. We want to make government processes clear, straightforward and accountable. Our Open Government Policy Forum is part of this process as is this review of the *Information Privacy Act*.

The IP Act protects the personal information of individuals in the public sector environment. It does this through its privacy principles, which set out how government agencies collect, store, use and disclose that information.

Government agencies deal with a vast amount of personal information. Queenslanders provide this information for many purposes – for example, whenever they apply for a licence, write to a Minister, use a government service or phone a department with a query. Understandably, they want the information to be managed responsibly. However, the right to privacy is not absolute, and the IP Act aims to balance the right to privacy with other interests – for example, the need for agencies to lawfully co-operate with law enforcement agencies. There is always room to debate whether the IP Act has achieved the correct balance.

As information and communication technology continues to evolve and expand, this may present particular challenges for governments holding personal information. Technology may assist government to better deliver its services, but may raise broader privacy concerns.

The IP Act has been in effect for over four years. As with the RTI Act, however, a number of operational and policy questions have emerged through this time. The review of its provisions allows Queenslanders to participate in this process and provide input about the changes they think need to be made.

I welcome their views and encourage them to contribute to this review.

Jarrod Bleijie MP
Attorney-General and Minister for Justice

Introduction

Background

The *Right to Information Act 2009* (Qld) (**RTI Act**) and the *Information Privacy Act 2009* (Qld) (**IP Act**) commenced on 1 July 2009. The RTI Act and IP Act provide for a review of the Acts. Under the Acts the objects of the review include:

- deciding whether the primary objects of the Acts remain valid;
- deciding whether the Acts are meeting their primary object;
- deciding whether the provisions of the Acts are appropriate for meeting their primary objects; and
- investigating any specific issues recommended by the Minister or the Information Commissioner.

Terms of reference

The review's terms of reference were endorsed by the Premier and are attached (Appendix 1).

Purpose of this discussion paper

The purpose of this discussion paper is 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. It covers the provisions of the IP Act which regulate the collection, storage, use and disclosure of personal information by government. A separate discussion paper covers the RTI Act and Chapter 3 of the IP Act - those parts of the legislation dealing with access to information and amendment of personal information.

How to have your say

All comments or submissions must be made in writing. In providing comments on a submission please refer to the relevant question number and provide reasons and supporting details or data for your response.

Please provide any comments or submissions by **15 November 2013**.

- **by email**: FeedbackRTIandprivacy@justice.qld.gov.au
- **by post:** RTI and Privacy Review
  Department of Justice and Attorney-General
  GPO Box 149
  Brisbane QLD 4001

Privacy statement

Any personal information in your comment or submission will be collected by the Department of Justice and Attorney-General (DJAG) for the purpose of undertaking the review under section 183 of the RTI Act and section 192 of the IP Act. DJAG may contact you for further consultation on the issues you raise, and your submission and/or comments may be provided to others with an interest in the review, for example, the Parliamentary Legal Affairs and Community Safety Committee.

Submissions provided to the DJAG in relation to this Discussion Paper will be treated as public documents. This means that in all but exceptional cases, they may be published on the DJAG website, together with the name and suburb of each person making a submission. If you would like your submission, or any part of it, to be treated as confidential, please indicate this clearly. Please note however that all submissions may be subject to disclosure under the *Right to Information Act 2009,* and access applications for submissions, including those marked confidential, will be determined in accordance with that Act.

Next steps

A report on the review is to be tabled in Parliament by the Attorney-General as soon as practicable after the review is finished.[1]

The issues in this paper and the discussion of possible actions or alternatives do not represent Queensland Government policy.

1 Section 183(3) of the RTI Act and section 192(3) of the IP Act.

RTI and IP Legislation – History

A number of parliamentary committees have considered the protection of privacy interests in Queensland. The former Legal, Constitutional and Administrative Review Committee recommended in 1998 that either legislative or administrative measures be introduced to ensure greater protections of individuals' privacy.[2] The committee recommended that the protection of personal information held by Queensland Government agencies be addressed as a matter of priority.

In 2001, the then Government issued an administrative Information Standard (IS) 42 setting out agencies' privacy obligations, but indicated a commitment to introduce privacy legislation. IS 42 essentially adopted the 11 Information Privacy Principles (IPPs) from the Commonwealth *Privacy Act 1988* (the Commonwealth Privacy Act) and imposed a policy requirement on State Government agencies to protect personal information in accordance with those principles. IS42A was created as a separate standard based on the National Privacy Principles (NPPs) in the Commonwealth Privacy Act for Queensland Health and its relevant portfolio bodies.

Those Information Standards remained in force until the enactment of the *Information Privacy Act 2009* following recommendations of the 2008 Independent Review Panel, chaired by Dr David Solomon, that Queensland introduce privacy legislation and appoint a privacy commissioner.[3]

The IP Act, which commenced on 1 July 2009 is the first legislation in Queensland to specifically provide protection for the personal information of individuals held by State Government agencies.

The IP Act has been amended several times since commencement to clarify ambiguities and reflect changes in other legislation. Most significant was a broadening of the definition of 'law enforcement agency' in 2011 to bring it into line with the definition in the Commonwealth *Privacy Act 1988*. This change allowed agencies to provide personal information to additional agencies for law enforcement purposes.

National Privacy Reforms

In 2008, in its final report following an inquiry into the Commonwealth *Privacy Act 1988*, the Australian Law Reform Commission (ALRC) recommended adopting uniform privacy principles across the states and territories as part of an intergovernmental agreement. The ALRC also recommended the current exceptions, which exclude small business and employee records from coverage of the Commonwealth Privacy Act be abolished, and that a data breach notification scheme be introduced. The Commonwealth Government announced then that its response to the report would occur in two stages.

2 Legal Constitutional and Administrative Review Committee, Queensland Parliament, Privacy in Queensland, (1998), 22.

3 FOI Independent Review Panel, *The Right to Information: Reviewing Queensland's Freedom of Information Act* (2008), 47. While the Independent Review Panel focussed on reviewing the Freedom of Information Act 1992 (Qld) , its terms of reference included considering specific issues relating to access to personal information and the interaction between Queensland's freedom of information regime and the protection of privacy interests (p9).

On 23 May 2012, the Honourable Nicola Roxon MP, the then Commonwealth Attorney-General, introduced the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (the Privacy Amendment Bill) to Parliament. The Bill was passed on 29 November 2012, and will commence in March 2014. It will implement more than half the recommendations in the 2008 ALRC report. Its key features include:

- new Australian Privacy Principles (APPs) to apply to both the private and Commonwealth public sectors;
- a new privacy principle for direct marketing and stronger protections for consumers when companies disclose personal information overseas;
- the extension of privacy protections to unsolicited information;
- stronger and clearer rules around data quality and data protection;
- a new requirement for organisations and companies to develop detailed privacy policies which are clear and easily accessible to consumers;
- stricter rules about sending personal information outside Australia; and
- a higher standard of protection for 'sensitive information' including health related information, DNA and biometric data.

The *Privacy Amendment (Privacy Alerts) Act 2013* will further amend the Commonwealth *Privacy Act 1988*, with effect from March 2014, to introduce mandatory data breach notification provisions for the Commonwealth government agencies and private organisations which are subject to the *Privacy Act 1988*. The provisions will require those agencies and organisations to provide notice to affected persons and the Office of the Australian Information Commissioner when certain types of personal information are accessed, obtained, used, disclosed, copied, or modified by unauthorised persons. There is no data breach notification in the IP Act.

Cause of action for serious invasion of privacy

In September 2011, following the News of the World phone hacking scandal, the then Commonwealth Minister for Privacy and Freedom of Information, the Honourable Brendan O'Connor MP, released an Issues Paper which invited comment on whether Australia should legislate a statutory cause of action for privacy and, if so, what form it might take.

On 12 June 2013, the Commonwealth Attorney-General, Mark Dreyfus QC, asked the ALRC to conduct an inquiry into the protection of privacy in the digital era. This inquiry is to also address remedies for serious invasions of privacy. .

Issues for consideration

Confusion and complexity in privacy across Australia

Privacy principles set out how personal information is to be collected, stored, used and disclosed. However, the content of the principles, and who they apply to, varies between federal, state and territory jurisdictions. This leads to significant confusion and complexity about how privacy law operates for governments and the private and community sector. In addition, it may create an unjustified compliance burden, particularly where organisations operate in more than one jurisdiction, and are required to comply with multiple layers of privacy regulation. Consumers who have complaints about privacy are often confused or unsure about who the appropriate privacy regulator is.

In Queensland, there are two sets of privacy principles under the IP Act. The National Privacy Principles (NPPs) in Schedule 4 of the IP Act apply to Queensland Health, and the Information Privacy Principles (IPPS) in Schedule 3 of the IP Act apply to all other Queensland agencies.[4] However, the Commonwealth Privacy Act affects some businesses and not-for-profit organisations in Queensland, because the National Privacy Principles in Schedule 3 of the Commonwealth Privacy Act apply to organisations 'with an annual turnover of more than $3 million, and all health service providers regardless of turnover.[5]

Considering the Australian Privacy Principles (APPs) in Queensland

There are differences between the APPs (as contained in the Privacy Amendment Act) 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.

The data breach notification requirements in the *Privacy Amendment (Privacy Alerts) Act 2013 (Cth)* will provide another point of difference when they commence.

The commencement of these provisions may raise questions as to whether the Queensland IPPs should be aligned to reflect the APPs or alternatively whether Queensland should adopt the APPs, and, if so, how they would apply to State Government agencies. The latter consideration would necessitate an assessment based on the *Queensland Government principles for Commonwealth-State/Territory intergovernmental activities* which guide Queensland's involvement in Commonwealth-State intergovernmental activities (see link at: www.premiers.qld.gov.au/publications/categories/guides/intergovernmental-activities.aspx)

4 All States and Territories except Western Australia and South Australia have privacy legislation.

5 The Commonwealth NPPs are similar, but not identical, to the NPPs in the IP Act.

Any alignment of the IPPs with, or adoption of, the APPs would mean that a single set of principles would apply to all agencies subject to the IP Act. The principles would continue to deal with the collection, storage, use and disclosure of information held by Government. Many of the concepts within them would remain the same as in the IPPs and the NPPs. If the same set of principles applied under both Commonwealth and Queensland privacy legislation, there may be less compliance burden for organisations.

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

Sharing Information

The ALRC noted that 'inconsistent, fragmented and multi-layered privacy laws' had prevented or impeded information sharing, acting as a barrier to information sharing between federal, state and territory government agencies, stating:

> *Information-sharing opportunities, which are in the public interest and recognise privacy as a right to be protected, should be encouraged. Rather than preventing appropriate information sharing, privacy laws and regulators should encourage agencies and organisations to design information-sharing schemes that are compliant with privacy requirements.*[6]

The Queensland IP Act operates in a similar manner to other privacy legislation across Australia. It:

- governs how Queensland Government agencies collect, store, use and disclose personal information;
- allows an individual to make a complaint about an agency's breach of the privacy principles;
- regulates the transfer of personal information outside Australia; and
- regulates how contractors to government handle personal information.

However, at times it is necessary for two or more agencies of government to work together in the interests of the community. Although members of the public expect the Government to respect their personal information, there are times when they also expect, or prefer, that their information is shared between agencies rather than have to repeat the information to a number of agencies.

In practice sharing of information across agencies does occur. For example clients of the Department of Communities, Child Safety and Disability Services who complete a Request for Assistance form consent to their relevant personal information being shared with a range of providers. This allows the department's staff to give information to non-government disability service providers, health service providers, and Commonwealth, Queensland and State Government departments and agencies so they can assist in meeting client needs.

To enable information to be shared appropriately, the IP Act sets out circumstances where personal information may be shared and also recognises that compliance with the privacy principles is not appropriate in all circumstances.

6 Australian Law Reform Commission, For your Information, Australian Privacy Law and Practice, Report no 108, Paragraph 13.11.

There are therefore a number of exceptions, including the following:

- IPP 11 allows information to be disclosed (from one agency to another) in circumstances which include where: the individual has expressly or impliedly agreed to the 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);[7]
- The privacy principles do not apply to certain entities for example parents and citizens associations, or the Legislative Assembly;[8]
- The Information Commissioner may give an approval that waives or modifies an agency's obligation to comply with the privacy principles;[9] and
- Law enforcement agencies are not subject to some of the IPPs in some circumstances - for example the Crime and Misconduct Commission is not subject to some IPPs for the performance of its activities related to law enforcement and its intelligence functions.[10]

Despite these exceptions, concerns are sometimes raised that the IP Act unreasonably prevents the sharing of information, particularly across Government. In some of these cases, other legislative confidentiality provisions, and not the IP Act, prohibit the sharing of information.

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?*

Definition of 'personal information'

The definition of personal information is central to the effective operation of the IP Act because obligations of agencies arise in relation to 'personal information'. It is therefore important to ensure that the definition captures that information which deserves protection.

Personal information is defined in section 12 of the IP Act 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.'*

7 Schedule 1 to the IP Act.

8 Schedule 2, part 1 of the IP Act.

9 Section 157 of the IP Act.

10 Section 29 of the IP Act.

This definition mirrors the definition in the Commonwealth *Privacy Act*. Although no operational difficulties with the current definition have been reported in Queensland, the ALRC recommended changes to that definition in the Commonwealth *Privacy Act* to remove unnecessary elements and bring it in line with other jurisdictions and international instruments.[11]

The ALRC recommended two changes to the definition of personal information. The first is to remove the reference to a database from the definition, noting that while this may have been necessary when the Commonwealth *Privacy Act* was first enacted in 1988, it is clear in 2013 that information in a database is caught by the definition.[12]

The second change relates to the use of the word 'identity'. To fall within the definition of personal information, the information must be about an individual whose identity is apparent or can reasonably be ascertained. A distinction has been drawn, in the ALRC's report, between an individual's 'identity', and an individual being 'identified'.

The concept of 'identity' is complex, and individuals may have a number of different identities which are defined by many factors. On the other hand, identification is the act of being identified, of linking specific information with a particular person.

The ALRC considered, and the Commonwealth Government has accepted, that the privacy principles should apply to information about an individual who is 'identified or reasonably identifiable' rather than information about an individual whose 'identity' is apparent, or reasonably ascertainable. This places a focus on the individual, rather than an identity. A similar change in the definition in Queensland's Act would also bring it into line with international instruments and other international jurisdictions.

The definition of personal information recommended by the ALRC is as follows:

> *information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual*

Section 36 of the Commonwealth *Privacy Amendment Act* repeals the current definition and substitutes the following:

> ***personal information*** *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?*

11 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) 309.

12 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108, (2008), 307.

Definition of 'agency' – Government Owned Corporations

Government owned corporations (GOCs) and their subsidiaries are included in the definition of an 'agency' for the purposes of the RTI Act and Chapter 3 of the IP Act - the information access provisions.[13] However, they are not captured by other parts of the IP Act.[14]

Queensland GOCs are subject to the NPPs in the Commonwealth Privacy Act which apply to private sector organisations.[15] This is because State or Territory organisations that are incorporated companies, societies or associations are deemed to be organisations for the purposes of the Commonwealth Privacy Act and are subject to that Act.

The Commonwealth Privacy Act allows a State or Territory to request that a particular organisation be excluded from the coverage of the Act. To date, no State or Territory organisations have been excluded from the Commonwealth Privacy Act.

Stakeholders have not raised operational issues about how GOCs are covered by the Privacy Act. However, 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 rather than being subject to the Queensland RTI Act and the Commonwealth Privacy Act. It may also be easier for those interacting with GOCs to have their rights provided for under state legislation. This would require the Queensland Minister to ask the Commonwealth Minister to exclude GOCs from coverage of the Commonwealth Privacy Act.

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. 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?*

Transfer of personal information outside Australia

The privacy principles contained in the IP Act only apply to Queensland State and local government agencies. Once personal information is transferred from the control of these agencies, the protections provided by the IP Act are lost. If there is no privacy protection in the jurisdiction which receives the information, the personal information of Queenslanders will no longer be protected.

13 See section 14 of the RTI Act and section 18 of the IP Act.

14 Section 18 of the IP Act.

15 Defined in section 6C to include individuals, body corporates, partnerships, other unincorporated associations and trusts.

It is therefore important that the personal information of Queenslanders is only transferred outside of Australia in appropriate circumstances. However this needs to be balanced against the ability of government to transfer information where there is a genuine need.

All Australian information privacy legislation has provisions dealing with the transfer of information out of Australia or (cross-border data flow' provisions). In Queensland section 33 of the IP Act restricts the circumstances under which personal information can be transferred outside Australia by Queensland Government agencies.

Section 33 of the IP Act requires agencies to consider whether personal information will be transferred out of Australia. Agencies bound by the IP Act may only transfer personal information out of Australia where one of a number of exceptions applies.

Section 33 of the IP Act provides:

> *An agency may transfer an individual's personal information to an entity outside Australia only if—*
>
> *(a) the individual agrees to the transfer; or*
> *(b) the transfer is authorised or required under a law; or*
> *(c) the agency is satisfied on reasonable grounds that the transfer is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare; or*
> *(d) 2 or more of the following apply—*
>
> *(i) the agency reasonably believes that the recipient of the personal information is subject to a law, binding scheme or contract that effectively upholds principles for the fair handling of personal information that are substantially similar to the IPPs or, if the agency is the health department, the NPPs;*
> *(ii) the transfer is necessary for the performance of the agency's functions in relation to the individual;*
> *(iii) the transfer is for the benefit of the individual but it is not practicable to seek the agreement of the individual, and if it were practicable to seek the agreement of the individual, the individual would be likely to give the agreement;*
> *(iv) the agency has taken reasonable steps to ensure that the personal information it transfers will not be held, used or disclosed by the recipient of the information in a way that is inconsistent with the IPPs or, if the agency is the health department, the NPPs.*

Agencies are increasingly taking advantage of technologies which make dealing with many kinds of information faster and more cost effective. BlackBerry phones are commonly used, cloud computing solutions are increasingly adopted and the community expects to be able to interact with agencies via the internet. Government regularly engages with the community using Web 2.0 platforms, including social media.

Technology issues

Both State and local government officers use a range of technology (including smartphones and tablets) as part of their day to day business, and government is increasingly likely to use technological developments to increase its 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 - for example, if messages are relayed to overseas locations. The Office of the Information 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.[16]

In an earlier Privacy Discussion Paper[17], the ALRC asked whether the *Privacy Act* should define 'transfer' (for the purposes of transfer of personal information outside Australia) to exclude temporary transfer of data such as when information is emailed from one person located in Australia to another person located in Australia, but, because of internet routing, the email travels (without being viewed) outside Australia on the way to its recipient in Australia.

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?*

Cloud computing

An OIC Guideline[18] states:

> *The phrase 'cloud computing' is simply a shorthand term for moving functions from a computer and agency-owned server to an online environment, for example, employees accessing word processing programs through a webpage interface instead of from the Programs menu on their computer. Computing power, storage space, applications and programs may all be outsourced to 'the cloud', i.e. a remote provider whose services are accessed via the internet. Cloud computing is not a new concept; webmail services, such as Hotmail which has been in operation since 1997, is an example of cloud computing.*

Cloud computing usually involves storing or processing information outside Queensland. If it occurs through a 'private cloud' model, where cloud computing services are hosted on government-owned infrastructure and delivered over government-owned networks, 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

16 Office of the Information Commissioner, Transfer versus transit: Emails and section 33 (13 September 2012) www.oic.qld.gov.au http://www.oic.qld.gov.au/about-us/consultation/whats-new/2012-09-13-transfer-versus-transit-emails-and-section-33>

17 Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper No 72 (2007).

18 Office of the Information Commissioner, *Cloud Computing and the Privacy Principles*, Guidelines- Privacy Principles (2012) <http://www.oic.qld.gov.au/information-and-resources/guidelines/guidelines-privacy-principles/cloud-computing-and-privacy>.

outside Australia. 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*[19]

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.[20] Agencies must therefore ensure that personal information is put online only in accordance with section 33 of the IP Act.

Even though the information may not in fact be transferred until someone outside Australia accesses it, making it available to on a webpage makes it potentially available to anyone in the world.

Personal information is generally only published online by agencies after careful consideration, and in circumstances where section 33 would not be breached- for example, individuals have consented. However, 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'.[21] Applied in Queensland, this would mean that rather than preventing information being transferred, as is the case under section 33, the IP Act could be amended to provide that agencies subject to the IP Act 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. The ALRC 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

---

[19] Top 10 Privacy Myths – Busted! February 2013

20 Office of the Information Commissioner, Personal Information: Disclosure, the World Wide Web and section 33, Guidelines- Privacy Principles (2010) 4 < http://www.oic.qld.gov.au/information-and-resources/guidelines/guidelines-privacy-principles/personal-information-world-wide-web>

21 This was suggested by the ALRC in DP 72.

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

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?*

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.

Section 141 of the IP Act establishes the Privacy Commissioner, who is a deputy to the Information Commissioner with particular responsibility for privacy functions.[22]

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

22 Section 141 of the IP Act.

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?*

Powers of the Privacy Commissioner

The Information Commissioner may give an agency a 'compliance notice' if satisfied that the agency has breached the privacy principles in a serious or flagrant way or has done so on five occasions within the last two years.[23] The notice can ask the agency to take certain action, with which the agency must take all reasonable steps to comply.

The Information Commissioner may require a person to provide documents or to attend and give evidence in relation to privacy complaints or compliance notices. Failure to comply results in an offence.[24]

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, for example the Information Commissioner is entitled to access to all documents;[25] may require agencies or Ministers to conduct searches;[26] may examine witnesses;[27] and may require information, documents and attendance.[28] However, the same kinds of powers have not been given to the Information Commissioner (or Privacy Commissioner) for the performance of privacy related functions e.g. the Information Commissioner may give an agency a compliance notice but there are no explicit powers which would enable the Information Commissioner to investigate a compliance issue.

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.

The Commonwealth *Privacy Amendment Act* provides greater powers to the Privacy Commissioner which improve the Commissioner's ability to resolve complaints conduct investigations and promote privacy compliance. It provides that:

23 Section 158 of the IP Act.

24 Section 197 of the IP Act.

25 Section 113 of the IP Act.

26 Section 115 of the IP Act.

27 Section 117 of the IP Act .

28 Section 116 of the IP Act.

The Commissioner has power to do all things necessary or convenient to be done for, or in connection with, the performance of the Commissioner's functions.

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

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?

Generally available publication

The IP Act at Schedule 1, section 7 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.

Both the Commonwealth and Victorian Privacy Acts include more specific definitions of generally available publications. The ALRC recommended that the Commonwealth definition 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.*

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

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?*

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?*

IPP 2 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 (for example, the Commonwealth, Victoria and NSW) and in NPP 1, all of which use the phrase 'collects personal information'.[29] 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?*

29 NPP 1.3 in schedule 3 of the *Privacy Act 1988* (Cth) and Privacy Principle 1.3 in Schedule 1 of *the Information Privacy Act 2000* (Vic).

APPENDIX 1 - Terms of Reference

REVIEW OF THE *RIGHT TO INFORMATION ACT 2009* AND *INFORMATION PRIVACY ACT 2009*

Background

The introduction of the *Right to Information Act 2009* (RTI Act) and the *Information Privacy Act 2009* (IP Act) followed an extensive overhaul of the State's freedom of information laws by a panel of experts chaired by Dr David Solomon.

The legislation includes provisions that require a review of the Acts. These reviews are to examine the practical application of the legislation and identify and resolve issues arising during implementation. While focussing on operational issues, the review will consider issues of efficiency and effectiveness, and whether there are opportunities to reduce the regulatory burden on agencies without compromising the objects of the Acts.

Purpose of the review

Section 183(1) of the RTI Act and section 192(1) of the IP Act provide for a review of the two Acts.

The purpose of the review is set out in section 183(2) of the RTI Act and section 192(2) of the IP Act respectively and is to:

(a) decide whether the primary objects of the Acts remain valid;

(b) decide whether the Acts are meeting their primary objects;

(c) decide whether the provisions of the Act are appropriate for meeting their primary objects; and

(d) investigate any specific issue recommended by the Minister or the information commissioner.

The Minister must table a report about the outcome of the review in Parliament.

Objects of the Acts

Section 3 of the RTI Act states its primary object as:

> *… to give a right of access to information in the government's possession or under the government's control unless, on balance, it is contrary to the public interest to give the access.*

Section 3 of the IP Act sets out the objects of that Act, to provide for:

(a) the fair collection and handling in the public sector environment of personal information; and

(b) a right of access to, and amendment of, personal information in the government's possession or under the government's control unless, on balance, it is contrary to the public interest to give the access or allow the information to be amended.

Conduct of the review

The review is being conducted by the Department of Justice and Attorney-General (DJAG), as agency with administrative responsibility for the legislation, with oversight by a steering committee of senior representatives from relevant departments.

As required by section 183(2)(d) of the RTI Act and section 192(2)(d) of the IP Act, the Information Commissioner will be consulted throughout the review.