Response to RTI/IP Act review: RTI Branch DCCSDS
16/02/2017

1. Are the objects of the RTI Act being met? Is the push model working? Are there ways in which the objects could be better met?

The primary object of the *Right to Information Act* (**RTI Act**) is still relevant; however, if all aspects of access and amendment are to be included in the one act then the objects need to include references to personal information access and amendment.

The objects of an Act are important given their role in statutory interpretation. The current objects could be strengthened to acknowledge the fundamental concept that the framework is intended to strike a balance between competing interests without weakening the push model philosophy. The concept of essential public interests warranting protection could be incorporated, as could the concepts of competing interests and protecting the private or business affairs of members of the community.

It is difficult to discern how effective the RTI Act has been in furthering the 'push model' philosophy. The public sector landscape has changed significantly since 2008 when the now repealed *Freedom of Information Act 1992* (**FOI Act**) was reviewed which led to the introduction of the RTI Act and the *Information Privacy Act 2009* (**IP Act**).

The basic elements of the push model in the RTI Act are:

- publication schemes
- disclosure log
- pro-disclosure bias
- section 20.

However, push model elements can now be found in a range of other initiatives across government, including open data.

2. Is the privacy object of the IP Act being met? Is personal information in the public sector environment dealt with fairly? Are there ways that this object could be better met?

The privacy object of the IP Act is being met. The objects could be expanded to clarify the scope of the application of the Act. Currently, section 3 of the IP Act provides:

> *(1) The primary object of this Act is 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.*
>
> *(2) The Act must be applied and interpreted to further the primary object.*

The objects could be amended to include a requirement that there needs to be an *expectation of privacy* for the protections of the Act to apply. For example, the objects

should make it clear that the Act intends that the privacy protections apply to information about the *private aspects* of the person's life rather than their commercial/professional/work life.

The notion of 'privacy' relates to the principles of human dignity, human uniqueness, the importance of solitude, and has historically been described as 'the right to be left alone.'[1] 'Privacy' covers several overlapping notions, including secrecy, confidentiality, solitude of the home, informational self-determination, freedom from surveillance, and the protection of an individual's intimate relationships.[2]

The different aspects of 'privacy' has been said to fall under six general headings:

(1) the right to be let alone - the right to privacy
(2) limited access to the self – the ability to shield oneself from unwanted access by others
(3) secrecy – the concealment of certain matters from others
(4) control over personal information – the ability to be able to control information about oneself
(5) personhood – the protection of one's personality, individuality, and dignity, and
(6) intimacy – control over, or limited access to, one's intimate relationships or aspects of life.[3]

Australia's legislative approach to privacy has centred on the fourth category – the control of information about oneself – i.e. 'information privacy'. Laws to protect the privacy of personal information appear to be in response to the increasing ability for governments and organisations to collect and store detailed caches of personal information.

As outlined above, the department supports the view that the IP Act could have a narrower application to protect only private, intimate aspects of the person's life rather than their professional/work life. In other words, it could be concerned only with protecting information about the person, the dissemination of which that person ought to be entitled to control.[4]

This is consistent with Article 17 of *the International Covenant on Civil and Political Rights* (**ICCPR**) which provides:

> *17. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.*

The approach is also consistent with the *European Convention for the Protection of Human Rights and Fundamental Freedoms*, which states at article 8:

---

1 Victorian Commissioner for Privacy and Data Protection, 'What is privacy?', accessed 23 January 2017, referring to Hon Michael Kirby AC CMG, 'Privacy: An elusive and changing concept,' *Griffith Journal of Law and Human Dignity*' (2013) 2653 and other research.

2 Victorian Commissioner for Privacy and Data Protection, 'What is privacy?', accessed 23 January 2017.

3 Victorian Commissioner for Privacy and Data Protection, *Privacy Background Paper*, p 2, citing Daniel Solove, 'Conceptualising Privacy', *Californian .Law Review*, 90 (2002) 90 1087.

4 As was discussed by the Information Commissioner in the context of the now repealed *Freedom of Information Act 1992* (Qld) protection of information concerning a person's 'personal affairs' in *Stewart and Department of Transport* (1993) 1 QAR 227.

Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[5]

The definition of 'personal information' could be amended (see discussion at question 25) and the objects provision of the IP Act should be amended to ensure that people's expectations of privacy are limited to the personal aspects of their life.

An objects provision sets out what the underlying purpose of the legislation is and is sometimes used to resolve ambiguity within the legislation itself. It may seek to provide a general understanding of an Act's purpose but it can also set out general aims of the Act to help the reader understand the more detailed provisions of the Act.[6]

Section 3(1)(a) of the IP Act is expressed too broadly regarding the kind of 'personal information' the Act should seek to protect.

The *Privacy Act 1988* (Cth) contains a set of objects in section 2A, the first of which provides that '*the objects of this Act are: (a) to promote the protection of the privacy of individuals*'.

Further, the *Privacy Act 1988* contains a number of preambles[7]*:*

> WHEREAS Australia is a party to the International Covenant on Civil and Political Rights, the English text of which is set out in Schedule 2 to the *Australian Human Rights Commission Act 1986*:
>
> AND WHEREAS, by that Covenant, Australia has undertaken to adopt such legislative measures as may be necessary to give effect to the right of persons not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence: [my underlining]
>
> AND WHEREAS Australia is a member of the Organisation for Economic Co-operation and Development:
>
> AND WHEREAS the Council of that Organisation has recommended that member countries take into account in their domestic legislation the principles concerning the

---

5 See also the European Union Parliament's *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive), Article 1.

6 Australian Law Reform Commission (ALRC), For Your Information: Australian Privacy Law and Practice (ALRC Report 108), Chapter 5: The Privacy Act: Name, Structure and Objects, 2008, citing D Pearce and R Geddes, *Statutory Interpretation in Australia*, 6th ed, 2006, p 154; Office of Parliamentary Counsel, *Working with the Office of Parliamentary Counsel: A Guide for Clients,* 3rd ed, 2008, para 125.

7 As set out in the *International Covenant on Civil and Political Rights* (ICCPR), Article 17.

protection of privacy and individual liberties set forth in Guidelines annexed to the recommendation:

AND WHEREAS Australia has informed that Organisation that it will participate in the recommendation concerning those Guidelines: …..

Despite the broad definition of 'personal information', individuals' privacy expectations are to be considered against the objects and the preamble of the *Privacy Act 1988,* ensuring that it is the private aspects of a person's life that is sought to be protected under the *Privacy Act 1988*.

Inclusion of an objects clause in the *Privacy Act 1988* was an outcome of the Australian Law Reform Commission's (**ALRC**) 2008 Report, *For Your Information: Australian Privacy Law and Practice*, Chapter 5 of which considered whether the Act should contain an objects clause. The ALRC believed that the *Privacy Act 1988* should contain an objects clause stating that the Act was intended to recognise individuals' right to privacy and to protect that right – this being one of various fundamental human rights in the ICCPR and other instruments.

An amended objects provision in section 3 of the IP Act (or a preamble) might state, for example:

(1) The primary object of this Act is—

(a) to give effect to the right of persons not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence, except as necessary in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others, and

(b) to provide for the fair collection and handling in the public sector environment of personal information. [my underlining]

(2) The Act must be applied and interpreted to further the primary object.

3. Should the way the RTI Act and Chapter 3 of the IP Act applies to GOCs, statutory bodies with commercial interests and similar entities be changed? If so, in what way? Is there justification for treating some GOCs differently to others?

No comment.

4. Should the RTI Act and Chapter 3 of the IP Act apply to the documents of contracted service providers where they are performing functions on behalf of government?

Increasingly, services which would have been provided by government agencies are being provided by non-government organisations by way of contract. This agency in particular relies upon non-government providers to deliver disability and community services and more recently, primary and secondary child protection services.

The issue is whether or not government believes it is important for the community to be able to access information about these services as if they were delivered by government. Consideration needs to be given to balancing these community expectations and the impact this would have on the sector or the contracted service provider (**CSP**).

Arguably, agencies may already be under obligation to consider, in applications to the agency, documents held by CSPs that fall within the terms of the application, given the definition of 'document of an agency' in section 12 of the RTI Act includes both 'in the possession' of and 'under the control of' the agency. Depending on the terms contained

within the contract, it may be that documents are under the control of agencies if they relate to a function being performed under the contract and there is a right to ask the CSP for access or specify how the documents related to the performance contract are dealt with at the end of the contract, for example, whether the contract requires all documents to be given to the agency at the completion of the contract.

It is far from clear what obligations and rights exist in relation to CSPs and applications made to agencies. Inconsistent contractual terms and disputes as to which documents held by a CSP rightfully fall within the terms of any particular application create uncertainty.

Some other jurisdictions have a range of mechanisms to bring information held by CSPs into the ambit of the access/amendment provisions.

Section 6C of the *Freedom of Information Act 1982* (Cth) requires agencies to take contractual measures to ensure it receives documents of CSPs (and subcontractors) which relate to the performance of the contract where an application has been received by the agency for access to the document/s. This appears to put in legislation the rights and obligations inferred from the concepts of possession and control that may apply under the RTI and IP Acts in Queensland.

In New Zealand, organisations are 'deemed' to be subject to the *Official Information Act 1982* (NZ) which seems to extend the reach of access and amendment provisions to non-government organisations.

It seems that there are four main options for dealing with CSPs:

1. Bring into the ambit of the RTI Act by changing the definition of 'agency' so that CSPs would be responsible for processing requests for documents directly made to them;
2. Deem particular organisations to be subject to the RTI Act (similar to New Zealand approach) and have those CSPs responsible for processing requests for their documents;
3. Provide an explicit power in the RTI Act for agencies to call documents in from CSPs when they are responsive to the terms of a request (similar to Commonwealth approach);
4. Retain the status quo but clarify the definitions around 'document of an agency' to ensure that agency obligations are clear to the community (whether or not those obligations are to include documents of CSPs) and rely on the terms of the contract for compliance.

Some members of the community will already have a right to access and amend their own personal information held by CSPs. Those CSPs working across borders will already be subject to obligations in multiple jurisdictions and should be consulted on any measures that would change those obligations. Many CSPs will have turnovers of greater than $3M and thus will be subject to the *Privacy Act 1988* (Cth) which contains access provisions for personal information held by those service providers. Further, many CSPs will be bound to comply with the Information Privacy Principles (**IPPs**) in the IP Act, including IPPs 6 and 7 which give rise to rights to access and amendment (noting that there is no processing framework or review rights to support those obligations). Some of this agency's CSPs are in fact already captured by the access and amendment provisions of the RTI/IP Acts because they are local councils or Hospital and Health Services.

So for personal information of a person, there may be pathways for access and amendment however there is a lack of consistency and most likely awareness that those pathways exist.

For non-personal information, or for applications made for personal information of others, there is no pathway for access other than applying to the contracting agency.

This is a complex area with multiple stakeholders and multiple jurisdictions involved. Any change to the obligations and rights needs careful consideration and extensive consultation before changes of any substance are made. It is suggested that one outcome of this review could be the recognition of this complexity and a referral of this issue for further investigation and a report back in say, 12 months, on the best way of balancing community expectations with the resource implications involved.

5. Should GOCs in Queensland be subject to the Queensland's IP Act, or should they continue to be bound by the Commonwealth Privacy Act?

No comment.

6. Does the IP Act deal adequately with obligations for contracted service providers? Should privacy obligations in the IP Act be extended to sub-contractors?

6.1 Obligations of contracted service providers

Section 35 of the IP Act requires agencies entering into service arrangements to take reasonable steps to bind CSPs to privacy principles if provision of services under the arrangement involves the exchange or handling of personal information in any way.

If the agency has taken reasonable steps to bind the CSP to the privacy principles, the CSP is a 'bound CSP'.

Section 36 provides that a bound CSP must comply with parts 1 or 2 and 3 of the IP Act in relation to the discharge of its obligations under the arrangement and its compliance can be enforced under the IP Act. The bound CSP will be a 'relevant entity' for the purposes of an individual making a privacy complaint under Chapter 5 of the IP Act if the CSP breaches the individual's privacy.

The standard government contracts include model privacy provisions and make Queensland the governing jurisdiction for agreement (e.g. *Queensland Government Service Agreement - Standard Terms for Social Services*[8] at clauses 7 and 23). Thus, the CSP would be required to submit to Queensland courts and tribunals for resolving privacy complaints.

If an agency has not taken the steps required of it to bind the CSP to the privacy principles under the IP Act, and there is a breach of a privacy principle, section 37 states that the obligations under the privacy principles will instead apply to the agency.

If section 37 applies, it would appear that the agency then becomes the 'relevant entity' in place of the CSP for the purposes of making a privacy complaint under Chapter 5 of the IP Act. Where the agency does attempt to 'take the steps required of it' under section 35 but the CSP is still not bound (e.g. because of refusal), it would appear that anyone who suffers a privacy breach as a result of the actions of the CSP has no recourse under the IP Act.

---

8 http://www.hpw.qld.gov.au/SiteCollectionDocuments/UpdateServiceAgreementStandardTerms.pdf

6.2 Making a privacy complaint where a CSP breaches privacy principles

Chapter 5 of the IP Act allows an individual to make a privacy complaint against a 'relevant entity'. A privacy complaint is a complaint about an act or practice of a relevant entity in relation to the individual's personal information that they believe breaches one or more obligations under the IP Act to comply with the privacy principles.[9]

The *'relevant entity*' is currently defined as:

- an *agency* in relation to the documents of the agency, or
- a *bound CSP* in relation to documents held by the bound CSP for the purposes of performing its obligations under a service arrangement[10]

Consideration should be given to expanding the definition of relevant entity, to capture situations where an individual may otherwise have no recourse. Irrespective of which definition is adopted, if the 'relevant entity' is the government agency, the agency should have a 'complaints management system'. If the relevant entity is the CSP, the terms of the agreement with the CSP should be drafted include a requirement for the CSP to have a complaint handling or complaints management system.

An individual whose personal information is, or has been, held by a relevant entity may make a privacy complaint. While section 165 states that the privacy complaint is made to Information Commissioner (**IC**), section 166(3) provides that the individual must first have complained to the relevant entity under its complaints management system (that is, the agency or the bound CSP). This process is discussed further at question 28 of this response.

An IC Guideline recommends that the service arrangement between the agency and the CSP specify who will be responsible for handling privacy complaints and how privacy complaints will be managed.[11]

The standard government contracts include provisions which require the CSP to notify the agency immediately upon becoming aware of any privacy breaches (e.g. *Queensland Government Service Agreement - Standard Terms for Social Services*[12] at clause 18.4). That contract also requires the CSP to '*fully cooperate with Us to enable Us to respond to applications for access to, or amendment of a document containing an individual's Personal Information and to privacy complaints*' (clause 18.1(h)). It includes an indemnity provision (clause 20.3) and stipulates that the governing law is the law of Queensland (clause 23).

---

9 *Information Privacy Act 2009* (Qld) section 164(1).

10 Or by the agency in relation to documents held by the agency: *Information Privacy Act 2009* (Qld) section 164(2).

11 Queensland Office of the Information Commissioner 'Part Two: General Guidance on privacy considerations when entering into a service arrangement', *Guidelines for Government*, 28 November 2014.

12 http://www.hpw.qld.gov.au/SiteCollectionDocuments/UpdateServiceAgreementStandardTerms.pdf

If the CSP does not or cannot or will not deal with the privacy breach within the 45 business day timeframe specified in section 166, then the IC will take over the handling of the privacy complaint. All the relevant provisions covering how the IC deals with the complaint will then be triggered. That will include the capacity for the IC to refer the matter to the Queensland Civil and Administrative Tribunal (**QCAT**) in specified circumstances (see Chapter 5, Part 4). Once the privacy complaint is under QCAT's jurisdiction, QCAT may dispose of it by any of the orders listed in section 178, including ordering compensation of up to $100,000 be paid to the complainant. Presumably such an order can be made against the bound CSP, but the Act is silent on this point.

An issue arises for complainants where the bound CSP is no longer a legal entity or is unable to pay compensation.

The *Privacy Act 1988* (Cth), section 53B, provides that if the Commonwealth Privacy Commissioner makes a determination in relation to a complaint that the CSP pay compensation but the CSP dies or ceases to exist, or becomes bankrupt or insolvent, the obligation is transferred to the contracting agency.

Another way of dealing with this issue is found in the Victorian legislation which ensures that the contracting agency remains liable for any breach of IPPs. This is discussed further at question 28.

6.3 Subcontractors

The IP Act itself does not provide for subcontractors to be subject to the IP Act's provisions. Thus, an individual cannot make a privacy complaint under the IP Act against a subcontractor for a breach of the privacy principles. An OIC Guideline recommends agencies consider either prohibiting the use of a subcontractor or requiring any subcontractor to comply with the privacy principles.[13]

It has become increasingly common for CSPs to engage subcontractors. It is clearly envisaged that CSPs may use contractors: for example, clause 22.2 of the *Queensland Government Service Agreement - Standard Terms for Social Services*[14] requires a CSP to ensure that subcontractors comply with the Agreement as if they were a party and that the CSP remains liable under the Agreement. Further, the Deed of Privacy specifically refers to obtaining a deed of privacy from subcontractors:

7.1 *If requested by the Department, the Recipient must obtain from its sub-contractors a deed of privacy in a form acceptable to the Department.*

---

13 Queensland Office of the Information Commissioner) 'Part Two: General Guidance on privacy considerations when entering into a service arrangement', *Guidelines for Government*, 28 November 2014.

14 http://www.hpw.qld.gov.au/SiteCollectionDocuments/UpdateServiceAgreementStandardTerms.pdf

If subcontracting is to occur, then the IP Act could require the CSP to bind the subcontractor to comply with the privacy principles and the subcontractor to be liable for their own privacy breaches or alternatively, for the CSP to be liable for any privacy breaches by the subcontractor.

7. Has anything changed since 2013 to suggest there is no longer support for one single point of access under the RTI Act for both personal and non-personal information?

The proposal for one single point of access and amendment under one RTI Act is still supported by this agency. The framework for the access and amendment scheme should be through one single entry point with the information privacy management obligations remaining in a Privacy Act designed only to deal with information handling practices and complaints management.

The current system, with two acts and two entry points, is confusing and overly burdensome for both applicants and agencies. For example, the current approved application form sets out the following, requiring applicants to check the relevant box:

> *a. All of the documents I'm applying for contain my personal information OR I'm seeking access on someone else's behalf, and all the documents contain that person's personal information –* ***IP application, no application fee.***
>
> *b. Some of the documents I'm applying for do not contain my personal information OR I'm seeking access on someone else's behalf, and some of the documents do not contain that person's personal information –* ***RTI application, application fee payable.***
>
> *c. None of the documents I'm applying for contain my personal information OR I'm seeking access on someone else's behalf, and none of the documents contain that person's personal information –* ***RTI application, application fee payable.***

If applicants are not familiar with the definition of personal information as stated in the Act, or have difficulty understanding that, for example, information about other family members is not <u>their</u> personal information, applicants will often choose the incorrect check box.

When this occurs, the application must be dealt with under section 54 of the IP Act, i.e. the 'wrong Act' provisions. When an applicant cannot be contacted immediately, the agency must write to the applicant to give them an opportunity to re-scope their application so that it applies only to their own personal information or to pay the fee to change their application to RTI. This process appears confusing for applicants who have little knowledge of how the legislation works and adds another layer of unnecessary red tape.

A way to simplify this for applicants, while enabling them to maintain a high level of involvement and control in the process, is by a single entry point (i.e. the RTI Act). Applicants would still be able to specify, in the first instance, whether their application is limited to personal information; however the agency could decide ultimately whether the terms of their request are likely to include documents containing non-personal information, without further consultation with the applicant. This was the case in the now repealed FOI Act and worked well, with an application fee levied where it was likely that there was at least

one document within the terms of the request that did not contain the applicant's personal information.

Later in this paper there is discussion about strengthening the definition of personal information which should be noted in considering application fees and the structure of the proposed single entry point.

8. Noting the 2013 response, should the requirement to provide a schedule of documents be maintained?

The 'schedule of documents' does not need to be a separate requirement requiring formal waiver. However, it is important to note that an RTI schedule of documents is not a detailed list of every document responsive to the request; rather it is an outline of the general classes of documents and the estimated number of pages in each of those classes. The RTI schedule is useful information for applications and an important aid to revisiting the terms of an application so that applications are better targeted and costs are minimised.

For example, a typical schedule may be by the types of documents or by the subject matter of documents. Table 1 below is an example of the former with Table 2 an example of the latter.

Table 1

File description	**Number of pages (personal)**	**Number of pages (non-personal)**
Emails	6	35
Human Resources documents	60	10
Service delivery documents	200	60
Contract management documents	0	337
TOTALS	**266**	**442**

Table 2

File description	**Number of pages (personal)**	**Number of pages (non-personal)**
Medical records	45	0
Personnel file	60	10
Cabinet documents	0	200
Legal file	45	300
TOTALS	**150**	**510**

If the requirements for schedules is not clear in the legislation then it may be that providing greater clarity around that would be more useful than removing the requirement to provide schedules altogether.

9. Should the threshold for third party consultations be changed so that consultation is required where disclosure of documents would be 'of substantial concern' to a party?

Yes. The threshold for third party consultations would be better returned to the pre-2009 standard of *substantial concern*. The original test of 'substantial concern' worked well having struck an appropriate balance between the rights of third parties, rights of access applicants and the administrative demands of processing applications. Returning to this test is a simple and straightforward way to assure the community expectation as to when third parties will be consulted.

Section 37 of the RTI Act is a natural justice provision which requires that access can only be given to a document that contains information the disclosure of which may **reasonably be expected to be of concern** to a government, agency or person if steps that are reasonably practicable have been taken to obtain the views of the relevant third party.

This requirement to consult is important and provides a framework for seeking views of third parties who have a legitimate interest in the disclosure of the information which concerns them in some way. Consulting with third parties gives decision makers the opportunity to obtain important relevant information for consideration in the decision making process. It also provides third parties consulted with the opportunity to seek internal or external review of a decision to disclose documents contrary to their views. The threshold for consultation was lowered in 2009 from '***substantial concern***' to '***concern'***.

The Solomon Review recommended section 51 of the now repealed FOI Act be retained and did not appear to contemplate lowering the threshold to the current section 37 provision that "matter the disclosure of which may reasonably be expected to be of ***concern*** (…)". Indeed, it may have been a drafting error.

The lowering of the threshold has increased the number of third parties who have a legitimate expectation to be consulted about the disclosure of documents that concern them. This department has dealt with a number of applications which, on the lower threshold, required consultation with up to 40 third parties. Where there are multiple third party participants the prospect of dealing with the application may give rise to considering whether the refuse to deal provisions should be called upon - which is not an intended or desirable outcome. If an application with multiple third parties is processed it is likely to be onerous and unwieldly for decision makers and parties alike.

Additionally, this agency understands that failing to consult with a third party, even where the decision maker has considered but decided against consulting, may amount to jurisdictional error which would make any decision void and put into question the lawfulness of any disclosures made under that decision.

It is noted that some other jurisdictions have different consultation requirements for different classes of documents or types of third parties (see table below). It is suggested that this should be avoided in Queensland. Regardless of the type of document or third party, consultation should be about assessing relative interests of third parties and giving rise to review rights.

Commonwealth	Requires third party consultation where the documents comprise information falling into certain categories (e.g. personal information, business and financial, intergovernmental relations) and if it appears that a third *might reasonably wish to make a contention* for an exemption.
South Australia, Western Australia, Northern Territory	Once the documents comprise information falling into certain categories (commonly re privacy/personal information, business and financial matters, trade secrets, intergovernmental relations) the obligation to consult the third party to whom it relates is triggered.
Australian Capital Territory	A threshold of '*of concern*' to a person or another entity. If the information of a particular type (similar to the above categories for other jurisdictions) that indicates that it may be 'of concern'.
New South Wales	Once the information falls into a particular category then the requirement to consult is created if a *person may reasonably be expected to have concerns about the disclosure of the information*.
Tasmania	Threshold to consult the third party is different depending on the nature of the information to the third party. It must be '*of concern*' to the third party where the third party's personal information may be the subject of disclosure. However, there must be a reasonable expectation of '*substantial concern*' where the business affairs of a third party are in issue.

10. Although not raised in 2013, is the current right of review for a party who should have been but was not consulted about an application of any value?

Review rights should only relate to documents to which access has been refused. Once at external review, the obligation for consulting with third parties sits squarely with the Information Commissioner, the agency being *functus officio* at that point. In those cases, the obligation for the Information Commissioner to join parties to reviews could be strengthened to make it clear that the Information Commissioner must join as participants to a review relevant third parties who have a legitimate interest in the documents. Any impediment in the Acts to the IC sharing information with a third party to ensure that their views are properly considered should be removed.

Once a decision is made and documents released under an access decision then there is no recourse to review because reviewable decisions relate to refusal of access. There may be other legal avenues of action, for example, in tort or equity, for persons whose interests have been adversely affected by the disclosure of documents without consultation, but this agency has not encountered such circumstances.

The publication of documents on a disclosure log may be an issue where a third party, not afforded the opportunity to provide views on disclosure or review rights, takes issue with the agency publishing documents released to an applicant. If the agency is approached by a third party and after consideration of their information takes the view that already published documents contain information that should not have been published because it comprises their personal information or is defamatory for example, then the agency is not prevented from removing those documents and republishing with the offensive information removed.

11. Are the exempt information categories satisfactory and appropriate? Are further categories of exemption needed? Should there be fewer exemptions?

This department considers the range and number of current exemptions to be generally appropriate.

Preliminary comments are made in relation to the general discretion in the RTI Act which, in our experience, has been the source of some confusion and inconsistent application across government.

General discretion

The general discretion was primarily inserted into the RTI Act to make clearer in the new legislation the approach that had been long adopted by the Information Commissioner under the now repealed FOI Act. The general discretion in the FOI Act was found by construing section 28 of the FOI Act to allow access to documents even though they may technically be exempt documents (*Norman and Mulgrave Shire Council* (Queensland Information Commissioner 1993 L0021, 28 June 1994, 13).

Making the discretion explicit in the RTI does give greater certainty and also reinforces the ideology of push over pull model of information access; however, may be the source of some confusion as to its application.

Discussion of general discretion

Section 48(3) of the RTI Act provides that:

…despite an agency or Minister being able, under section 47(3)(a), to refuse access to all or part of a document, the agency or Minister may decide to give access.

The discretion in section 48(3) is properly limited by the operation of other law or principles which apply to the information the subject of the application. If the chief executive officer or Minister is not authorised to release the information then the RTI decision maker is not authorised to exercise the residual discretion in the RTI and IP Acts to release it.

Common limitations on release of documents for which the general discretion could not be lawfully exercised by a decision maker would include:

Legal advice or documents prepared for litigation (legal professional privilege)

- The privilege attaches to the client. In the case of legal advice provided to the state, the Attorney-General as the first law officer is the client and therefore the only officer with the power to waive privilege.

Cabinet documents and executive council (Cabinet confidentiality)

- Only Cabinet or Executive Council can waive confidentiality.

Documents which are the subject of judicial or quasi-judicial orders (contempt of court)

- Only the court, tribunal or commission of inquiry can vary the orders.

Documents the release of which would infringe the privileges of Parliament (Parliamentary privilege)

- Only Parliament can waive parliamentary privilege.

Documents where there are legal agreements which govern the confidentiality of the documents, for example, where the terms of a contract provide for confidentiality or where there would be found to be an equitable obligation of confidence owed to third parties or statutory prohibitions.

- In these cases the general law, contract law and equity determine the rules of disclosure so that the relevant parties can rely on the promises made and obligations arising from contract or fiduciary obligation for example.

Section 3A of the *Freedom of Information Act 1982* (Cth) is framed so as to make clear the limitations on the exercise of the residual discretion and could be considered as an approach for Queensland. Section 3A provides:

3A Information or documents otherwise accessible

Scope

(1) This section applies if a Minister, or an officer of an agency, has the power to publish, or give access to, information or a document (including an exempt document) apart from under this Act.

Publication and access powers not limited

(2) Parliament does not intend, by this Act, to limit that power, or to prevent or discourage the exercise of that power:

a. In the case of the power to publish the information or document-despite any restriction on the publication of the information or document under this Act; and

b. In the case of the power to give access to the information or document-whether or not access to the information or document-whether or not access to the information or document has been requested under section 15.

It may be prudent to make more certain the limitations of the residual discretion with respect to exempt information so that decision makers do not risk making unlawful disclosures, some of which carry with them criminal penalties, for example, the offence provisions in the *Child Protection Act 1999* (**CP Act**).

Exemptions

Schedule 3, section 12

The department recommends a minor amendment be made to the exemption at Schedule 3, section 12 to improve outcomes for applicants.

This agency is by far the most frequent user of this exemption given that, amongst other types of information, it makes exempt information which is prohibited from disclosure under sections 186-188 of the CP Act.

In 2014-15[15], this department applied Schedule 3, section 12 on a total of 150,990 pages. The next most frequent user of the exemptions were the Hospital and Health Services (collectively) which applied the exemption on a total of 1474 pages.

The main issues experienced by this department, which would be overcome by the amendment recommended, are as follows:

1. The requirement for families to lodge separate applications under the IP Act for each individual family member, rather than applying once under the RTI Act to access information relating to all family members;
2. The inability of parents of deceased children to access child protection related information about those children;

[15] This is the most recent annual report which is available.

3. The inability of people seeking information about relatives, particularly those who identify as Indigenous and seek to trace their history, to access information about family.

1. Individual IP applications

This issue has arisen out of the decision in *Hughes and the Department of Communities, Child Safety and Disability Services* (Queensland Information Commissioner, Unreported, 17 July 2012) (*Hughes*), in which the IC considered Schedule 3, section 12 in the context of section 187 of the CP Act. Section 187 of the CP Act provides that information collected in the course of administering the CP Act must not be disclosed, with limited exceptions. The most relevant exception for the purposes of processing applications under the RTI/IP Acts is that at section 187(4)(a) which provides that the information may be disclosed to a person to the extent that the information is about that person.

In *Hughes,* the IC found that the exception at section 187(4)(a) [2] of the CP Act:

> *…only applies where the information is **solely** about the applicant. Thus where information is simultaneously about the applicant and others, the CP Act exception will not apply.*

If the approach in *Hughes* is to be accepted, information which is either not about the applicant or which is simultaneously about the applicant and others, must be found to be exempt under Schedule 3, section 12 of the RTI Act, given that its effect is to limit the applicability of the exception to section 187 of the CP Act.

The nature of child protection documents generally is that they are rarely solely about one person. Frontline child protection work aims to be holistic and consider the needs of the family as a whole (not just one member of that family). Documents will contain information about, for example, both parents, multiple children, extended family members and friends supporting the family. Accordingly, in order for a parent to access all of the information about their family unit, they need to make separate applications for their own information and then on behalf of each of their children (because only information solely about the applicant can be disclosed). This is unnecessarily burdensome for the agency as well as applicants, and if there was a public interest test attached to Schedule 3, section 12, a parent could apply under the RTI Act and be granted access to all of the information about their family that was in the public interest to disclose, regardless of the approach taken in *Hughes*.

2. Deceased children

This issue arises because while the Act provides for parents to make applications for their children, this can only apply to living persons. Given that Schedule 3, section 12 effectively makes child protection information about others exempt, without providing discretion for the department to decide otherwise, parents of deceased children do not have a way of accessing information about their deceased child. The mechanism under which they could previously access this information was removed by the introduction of the RTI Act. This is not consistent with the objects of the Act in terms of accountability and transparency.

3. Family histories

In a similar vein, historical information about family members can also be covered by the confidentiality provisions of the CP Act. In particular, this may adversely affect people who identify as Indigenous and are seeking access to information to help trace family histories.

---

[2] *Hughes and the Department of Communities, Child Safety and Disability Services* (Queensland Information Commissioner, Unreported, 17 July 2012), 26.

Background to this exemption

Prior to the enactment of the RTI Act in 2009, the now repealed FOI Act contained a similar exemption to that now contained in Schedule 3, section 12. The exemption at section 48 provided:

> ***48 Matter to which secrecy provisions of enactments apply***
>
> *(1) Matter is exempt matter if its disclosure is prohibited by an enactment mentioned in schedule 1 unless disclosure is required by a compelling reason in the public interest.*
>
> *(2) Matter is not exempt under subsection (1) if it relates to information concerning the personal affairs of the person by whom, or on whose behalf, an application for access to the document containing the matter is being made.*
>
> *[emphasis mine]*

The public interest consideration attached to the exemption did not carry over in the transition to the structure of the RTI Act. The Solomon report raised concern with having two types of public interest and recommended (at recommendation 45) that the exemption actually be repealed and only appear as a factor favouring non-disclosure so as to keep one standard of public interest test across the Act (as per recommendation 41). However, the exemption was retained but with the removal of the public interest discretion.

It is recognised that these types of information should be afforded a higher level of protection than that afforded by the public interest factors; however, the removal of the public interest discretion from the exemption has resulted in reduced access to particular types of information, a consequence which was both unintended and undesirable.

We appreciate the design principles that Solomon recommended (i.e. separating exemption from public interest and having one standard of public interest) but, having worked within the framework since 2009, prioritising form over substance in the legislation design has not resulted in the best outcomes for the community. It is recommended that a public interest test be reinstated to allow this agency and others the discretion to disclose information where there is a clear and compelling reason in the public interest (for example, in the case of families seeking access to deceased children's information).

A suggested drafting of this recommended amendment is as follows:

> ***12 Information disclosure of which prohibited by Act***
>
> *(1) Information is exempt information if its disclosure is prohibited by 1 of the following provisions—*
>
> *(…)*
>
> *(2) Information is not exempt information under subsection (1) in relation to an access application if it is personal information for the applicant.*
>
> *(3) Subject to subsection (2), information is exempt information if it is contained in a document mentioned in section 112(1) of the repealed Freedom of Information Act 1992.*
>
> ***Insert:***
>
> ***(4) Information is not exempt information under subsection (1) in relation to an access application, if there is a compelling reason in the public interest for disclosure.***

Such an amendment would not adversely affect those other entities which rely upon this exemption to maintain the confidentiality of other types of information (for example, audit

documents of the Queensland Audit Office) because the 'compelling' public interest test proposed still affords a higher level of protection to this kind of information and it would be at each agency's discretion to decide the circumstances in which the test might be satisfied.

12. Given the 2013 responses, should the public interest balancing test be simplified; and if so how? Should duplicated factors be removed or is there another way of simplifying the test?

See 14.

13. Should the public interest factors be reviewed so that (a) the language used in the thresholds is more consistent; (b) the thresholds are not set too high and (c) there are no two part thresholds? If so, please provide details.

See 14.

14. Are there new public interest factors which should be added to schedule 4? If so, what are they? Are there any factors which are no longer relevant, and which should be removed?

In response to all of the questions above about public interest:

The FOI Act framework contained:

- 'true exemptions', such as Parliamentary privilege, Cabinet confidentiality and prejudice to law enforcement activities;
- exempt unless disclosure was in the public interest.

The new Act retained most of the 'true exemptions' and converted the 'exemptions with public interest discretion' to public interest 'harm factors'. Essentially, these harm factors (those at Part 4 of Schedule 4) were the old exemptions minus the public interest balancing tests. In addition to these 'harm factors, the new Act included lists of public interest factors favouring disclosure and favouring non-disclosure (those at Parts 2 and 3 of Schedule 4). There was some discussion at the time about whether the 'public interest harm factors' were stronger than the lists in Parts 2 and 3 but it was made clear that this was not the intention.

The listed factors in Parts 2 and 3 of Schedule 4 are mostly derived from case law and as such have arisen from particular circumstances of a case and can be relevant in some cases and not relevant in others depending on the circumstances. Extracting public interest factors and listing them in a schedule risks the application of them out of context and in circumstances that may have been expressly excluded in the case in which they were originally developed. They lack the sophistication necessary to balance complex interests which are characteristic of many RTI applications. Although the lists were never intended to be exhaustive or applied in a mix and match way, this is almost inevitable without the grounding in the context of the cases from which they derive. They are frozen in time and so specific that they may cease to be useful.

It is recognised that the lists of public interest factors in Parts 2 and 3 of Schedule 4 were intended to assist decision makers, applicants and third parties and to improve the quality of decisions and reasons for decision; however, they do not promote excellence in decision making. Additionally, it was the intention as recommended by the Solomon report for the list to be non-exhaustive and this does not seem to be clear in the RTI Act (see for example, in section 49(2) where it says that the schedule 4 factors are those that Parliament considers

appropriate for deciding whether disclosure would, on balance, be contrary to public interest).

Including both the lists and the public interest harm factors causes confusion and unnecessary duplication. To promote clarity, reduce confusion and duplication and improve decision making, the public interest factors in Parts 2 and 3 of Schedule 4 could be removed from the Act entirely and be the subject of guidelines issued by the IC.

It should also be made clear in the Act that the public interest is a broad and dynamic concept and any factors listed in the Act are intended to be non-exhaustive.

The 'harm factors' in Part 4 of Schedule 4 are much more useful for decision makers because their form is familiar across jurisdictions and they essentially equate to the conditional exemptions in the repealed FOI Act and to the *Freedom of Information Act 1982* (Cth). The form and substance of these factors are commonly found internationally and allow for leveraging off other law for the purposes of making quality decisions. Their structure is clear with elements to be satisfied, information to be characterised and material facts identifiable so that making decisions on access to particular documents and writing reasons for those decisions becomes a much less random exercise as can be the case with the lists of factors.

It is recognised that there may be the need to include a small number of additional factors to the 'harm factors' to make up for the removal of the lists and we would welcome the opportunity to participate in scenario testing to fine tune their development.

15. Are there benefits in departmental disclosure logs having information about who has applied for information, and whether they have applied on behalf of another entity?

See 18.

16. Have the 2012 disclosure log changes resulted in departments publishing more useful information?

See 18.

17. Should the disclosure log requirements that apply to departments and Ministers be extended to agencies such as local councils and universities?

See 18.

18. Is the requirement for information to be published on a disclosure log 'as soon as practicable' after it is accessed a reasonable one?

In response to all of the questions above about disclosure logs:

Consideration should be given to returning to the pre-2013 position where publishing documents was not mandatory but rather more focused on those documents in which there was a wider community interest. Mandatory publication of documents based on an entirely different set of criteria is onerous for agencies and does not seem to have resulted in a benefit of more useful information being published; nor does it seem to have reduced numbers of applications made.

If the requirement to publish the terms of applications as they are received is retained, then the mandatory requirement to publish the actual documents is of little value because members of the community can contact the agency and seek access to the documents provided under previous applications by referring to the terms published on the disclosure log.

If the access and amendment provisions of the two Acts are consolidated into a single entry point, consideration should be given to which applications are required/able to be published on the disclosure log.

19. Do agency publication schemes still provide useful information? Or are there better ways for agencies to make information available?

No. Agencies already publish reasonably consistent information on their websites; for example, annual reports, strategic plans, key project papers and corporate structures. It appears to be of little benefit to have these types of documents on a separate Publication Scheme at a time when websites have become more easily navigable and consistent with user experience requirements. Further, a move towards grouping web content into franchises will make navigating to the content much easier for people seeking to engage with Queensland Government.

The Publication Scheme model might no longer be relevant given that there are measures in place to ensure agencies publish similar information on their websites. These data initiatives might better led by the data management sector so that one approach to all information is taken with minimal duplication. Open Data goes a significant way to fulfilling the push philosophy so consideration should be given to allowing Open Data to grow into that space and remove the publication scheme entirely from the RTI Act and Information Commissioner functions.

However, reinstating a register of the types of documents held by an agency in the form of something akin to the previous Statement of Affairs may be useful in assisting members of the community locate the correct contact for matters associated with those documents. It may be that a whole-of-government approach would be of more value to the community so that the register could be accessed through one portal rather than through individual government agencies. This would also make the register agile enough to cope with changes in machinery-of-government changes.

20. Should internal review remain optional? Should the OIC be able to require an agency to conduct an internal review after it receives an application for external review?

Yes, internal review should remain optional. It is a practical approach giving applicants the choice of dealing with the agency at internal review or going straight to external review. In most cases it is preferable that the applicant retains control over how they want to engage with review mechanisms. Although the proposal that the OIC could require an agency to conduct an internal review is not supported, there may however be merit in allowing agencies to request the OIC to remit a matter for internal review. This could be useful for instances where an agency locates further documents after its initial decision has been made which could be considered by the agency at internal review.

Please see overleaf a cross-jurisdictional analysis of review models which may be useful in considering this matter.

21. Should applicants have a right to appeal directly to QCAT? If so, should this be restricted to an appeal on a question of law, or should it extend to a full merits review?

A right of appeal directly to QCAT would not appear to have great benefit to applicants or agencies. The IC is the first level review and thus is the appropriate body to conduct merits review. Questions of law are quite appropriately directed to QCAT appeal panel

The table overleaf sets out the process for reviewing freedom of information/right to information decisions in other Australian jurisdictions. The points considered are:

- the types of reviews
- whether Internal review is optional or compulsory
- options for external review
- the external review process and whether the review is conducted on the merits
- whether there is a further review or appeal on a question of law.

Freedom of Information/Right to Information: Review of decisions

Jurisdiction	Types of review and internal review process	External review	Other review/appeal rights
New South Wales	Three options for review of certain decisions[16] made by under Part 5 of the *Government Information (Public Access) Act 2009* (GIPA Act): • internal review by agency (optional if access applicant), • external review by: o the Information Commissioner, or o the NSW Civil and/or Administrative Tribunal (NCAT) <u>Internal review</u> Internal review under Part 5, Division 2: • application by a person aggrieved by a s 80 reviewable decision • no Internal review if initial decision made by Minister or staffer[17]	<u>External review by Information Commissioner</u> Person aggrieved by reviewable decision of agency entitled to review by Information Commissioner under Part 5, Division 3: • access applicant does not have to have an IR before external review (but if not the access applicant, must have internal review first)[19] • review by Information Commissioner is on merits • on review, the Information Commissioner may make such recommendations to the agency about the decision as he/she thinks appropriate:[20] • recommendation to agency to reconsider the decision and make a new decision (and agency may then reconsider and make a new decision by way of internal review [21] • recommendation against agency's decision that there is an overriding public interest against disclosure of	Review by NCAT Appeal Panel – generally on a question of law.

16 Section 80 lists '*reviewable decisions*' for the purposes of Part 5 of the GIPA Act.

17 GIPA Act, s 82.

19 Or if IR cannot be sought – eg the decision is by a minister (or personal staff of minister) or principal officer of agency: GIPA, s 89.

20 GIPA Act, s 92.

21 GIPA Act, s 93.

Jurisdiction	Types of review and internal review process	External review	Other review/appeal rights
	• internal review is by way of making a new decision afresh.[18]	government information (but must consult Privacy Commissioner first if concerns a privacy related public interest consideration)[22] • recommendation to agency to change general procedure re dealing with access applications to conform to GIPA Act or further its objects.[23] • Information Commissioner can refer decision of agency to NCAT with consent of applicant.[24] External review by NSW Civil and Administrative Tribunal Person aggrieved by reviewable decision of agency entitled to review by NCAT under Part 5, Division 4: • administrative/merits review under *Administrative Decisions Review Act*[25] • do not have to first have the decision reviewed internally, or by Information Commissioner[26] (but if review by Information Commissioner, timeframe	

18 GIPA s 84.

22 GIPA Act, s 94. A '*public interest consideration*' is a public interest consideration referred in in Table to s 14, cl 3(a) or (b).

23 GIPA Act, s 95.

24 GIPA Act, s 99.

25 GIPA Act, s 100.

26 GIPA Act, s 100 (note).

Jurisdiction	Types of review and internal review process	External review	Other review/appeal rights
		to apply to NCAT is 20 days not 40 days)[27] • onus on agency to justify decision.[28]	
Victoria	Under Part VI of the *Freedom of Information Act 1982*: (FOI Act (Vic)) the review process is: • review by FOI Commissioner[29] (unless decision of agency's principal officer or a Minister) • no process for seeking internal review by agency[30] then • further review by Victorian Civil and Administrative Tribunal (VCAT) of specified FOI Commissioner decisions[31] Must usually go to FOI Commissioner first then to VCAT, except in certain cases (see next column).	Review by FOI Commissioner Under Part VI, Division 1 of the FOI Act (Vic), applicant may apply to the FOI Commissioner for review of a s 49A decision: • direct from agency (but if decision made by agency's principal officer or a Minister, must go to VCAT)[32] • FOI Commissioner cannot review certain other decisions including decisions regarding cabinet documents; documents affecting national security, defence or international relations • review on the merits (make fresh decision which takes effect as if agency's decision)[33]	External review by Victorian Civil and Administrative Tribunal Under Part VI, Division 3 of the FOI Act (Vic), an applicant or agency (and certain third parties) may apply to VCAT for review of : • most fresh decisions made by the FOI Commissioner under r s 49P and dismissals on s 49G grounds.. • decisions by agency's principal officer or a Minister of refusal or deferral of access[35]and other decisions that cannot go to FOI Commissioner

27 GIPA Act, s 101. Any review on foot by the IC must end when application to NCAT is made.

28 GIPA Act, s 106. However, some constraints on NCAT include decisions about disclosure of Cabinet and Executive Council information being limited to whether there were reasonable grounds for the claim and cannot review of merits.

29 FOI Act (Vic), Part VI, Division 1.

30 However, agency can reconsider on own initiative under s 49M of the FOI Act (Vic).

31 The FOI Commissioner has direct review of decisions by agency's principal officer or a Minister or of deemed refusal by agency.

32 FOI Act (Vic), s 49A

33 FOI Act (Vic), ss 49H, 49P.

35 FOI Act (Vic), s 50(9)(a), (f).

Jurisdiction	Types of review and internal review process	External review	Other review/appeal rights
		• can ask agency to reconsider or agency can reconsider on own initiative and make a new fresh decision[34] • FOI Commissioner can facilitate agreement under s 49N • FOI Commissioner can dismiss application on various s 49G grounds (eg more appropriate for VCAT review).	• various other decisions listed in s 50.[36] VCAT can: • confirm the decision • make a different decision.[37] VCAT decisions can only be appealed at the Supreme Court of Victoria on a question of law.[38]
Western Australia	Under the *Freedom of Information Act 1992* (FOI Act 1992), a person aggrieved by a decision made by an agency can apply for: • internal review by the agency of specified decisions (compulsory except in certain circumstances),[39] then, if still dissatisfied:	External review by FOI Commissioner After internal review, access applicant or agency can apply for external review (complaint) by the FOI Commissioner under Part 4, Division 3:[44] • review on the merits • confirm, vary or set aside agency's decision[45]	Part 4, Division 5 of the FOI Act 1992 provides for appeals to the Supreme Court on a question of law.

34 FOI Act (Vic), s 46L and s 46M.

36 See also, FOI Act (Vic), ss 53, 53AA. Can also seek review of refusal on Cabinet or national security grounds.

37 (eg ordering that some or all of the documents be provided to the applicant).

38 Victorian Government, Freedom of Information, Review by FOI Commissioner, 13 October 2016.

39 FOI Act 1992, Part 2, Division 5. Section 39 sets out the types of reviewable decisions.

4444 FOI Act 1992, s 65.

45 FOI Act 1992, s 76.

Jurisdiction	Types of review and internal review process	External review	Other review/appeal rights
	• external review by WA Information Commissioner of internal review decision[40] <u>Internal review</u> A person is generally required to go to internal review before seeking external review:[41] • review of application as if new (on merits)[42] • the internal review officer may confirm, vary or reverse the decision under review.[43]	• can refer a question of law to Supreme Court[46] • FOI Commissioner's decision is final unless an appeal is made to the Supreme Court on a question of law	
Tasmania	Under Part 4 of the *Right to Information Act 2009* (RTI Act), the types of review regarding applications for 'assessed disclosure are:'[47]: • internal review,	<u>External review by Ombudsman</u> Under ss 44-48 of the RTI Act, the Ombudsman undertakes external review on application by access applicant or certain third parties:	No express provision for review by the courts on error of law or otherwise. However, possible review on error of law under the *Judicial Review Act 2000* (Tas).[54]

40 FOI Act 1992, Part 4, Division 3.

41 FOI Act 1992, s 66(5). However, Commissioner may allow a complaint to be made even though internal review has not been applied for or has not been finalised if the complainant shows cause why internal review should not be undertaken or completed: s 66(6).

42 FOI Act 1992, s 42.

43 FOI Act 1992, s 43.

46 FOI Act 1992, s 78.

47 Where a request is made under the RTI Act for documents that are not otherwise available under other avenues.

54 Advice from Tasmanian Ombudsman's Office is that, given there has not been any appeals under the RTI laws, they are unclear about the source of a right of appeal but judicial review options would appear to be relevant.

Jurisdiction	Types of review and internal review process	External review	Other review/appeal rights
	then (except in certain circumstances)[48] • external review by the Ombudsman <u>Internal review</u> Internal review by applicant for access and certain third parties under s 43: • no internal review where review is of a decision of a Minister or principal officer • reconsideration of initial decision and making of fresh decision.	• Ombudsman may make any decision on the application for review that could have been made by agency or Minister (merits review)[49] • Ombudsman may also direct that his or her decision be implemented by the agency within 15 days or less. Failure to implement is reportable to Parliament[50] • Ombudsman has other powers (eg directing internal review if this has not occurred, conciliation or settlement)[51] • Ombudsman may make application to the Supreme Court on a question of law.[52] Where a decision has been finalised, the Ombudsman may only reconsider it to correct an accidental mistake or omission.[53]	
South Australia	Under Parts 3 and 5 of the *Freedom of Information Act 1991* (FOI Act 1991) the types of review are‘:	<u>External review by Ombudsman SA</u> Part 5, Division 1 of the FOI Act 1991 deals with external review by the SA Ombudsman.[57]	<u>Appeals District Court</u> Part 5, Division 2 of the FOI Act 1991 covers external review by the District Court.

48 RTI Act, ss 44-45. Examples include deemed refusals.

49 RTI Act s 47(1)(k).

50 RTI Act s 47(7), (8).

51 RTI Act s 47(1).

52 RTI Act s 47(2).

53 RTI Act s 48(2).

57 The Police Ombudsman is the external review body for decisions by police or the Police Minister: FOI Act 1991, s 39(1).

Jurisdiction	Types of review and internal review process	External review	Other review/appeal rights
	• internal review (compulsory unless exceptions apply), then (except in certain circumstances) • external review by the Ombudsman, or • appeal to District Court. <u>Internal review</u> Internal review application by a person who is aggrieved by a determination made by an agency regarding access to documents (Part 3, Division 3): • no internal review where review is of a decision of a principal officeror at the direction of, the principal officer of the agency (usually the Chief Executive),[55]	An application for external review can be made by a person aggrieved by internal review decision or a decision that cannot be internally reviewed.[58] Can only seek external review if: • there has been an internal review of the determination, or the original determination has been made by, or at the direction of, the principal officer of the agency[59] • SA Ombudsman has the power to investigate any action of the agency during the review, by exercising the powers of a Royal Commission. • SA Ombudsman may attempt to reach a settlement[60] • SA Ombudsman may confirm, vary or reverse the determination.[61]	An agency aggrieved by Ombudsman's determination may, with Court's permission, appeal to the District Court on a question of law.[62] A person (other than an agency) aggrieved by: • an internal review; by an agency, or • a determination not subject to internal review, or • a determination by the SA Ombudsman on external review, may appeal to the District Court.[63] Not restricted to question of law.[64]

55 Or at the direction of a person or body to which the principal officer is responsible: FOI Act 1991, s 29(6).

58 FOI Act 1991, s 39(2).

59 Or at the direction of a person or body to which the principal officer is responsible: FOI Act 1991: s 39(3).

60 FOI Act 1991, s 39(5).

61 FOI Act 1991, s 39(11).

62 FOI Act 1991, s 40(1).

63 FOI Act 1991, s 40(2).

64 The FOI Act 1991, s 40(2) does not refer to a 'question of law'. This is confirmed by advice from legal officer of Ombudsman SA in telephone conversation on 19 October 2016.

Jurisdiction	Types of review and internal review process	External review	Other review/appeal rights
	• agency may confirm, vary or reverse the determination under review[56]	An external review can also be undertaken by the Administrative and Disciplinary Division of the District Court. Doing this means any current Ombudsman external review stops. However, the District Court can conduct an external review after the Ombudsman's external review.	
Australian Capital Territory	Part 7 of the *Freedom of Information Act 1989* (FOI Act 1989) governs reviews of decisions. The review types are:: • internal review (compulsory, except in certain circumstances), then • external review by ACT Civil and Administrative Tribunal (ACAT) Final right of appeal to ACT Supreme Court on error of law. Internal review Part 7 provides for internal review: • an applicant affected by a determination listed in s 59 is entitled to an internal review	External review by ACT Civil and Administrative Tribunal External review under Part 7 of the FOI Act 1989: • ACT Civil and Administrative Tribunal (ACAT)[66]: o review of internal review decision unless internal review not possible (eg Minister or principal officer, deemed refusal) then direct to ACAT o merits review o decision has same effect as if made by agency or Minister o cannot apply to ACAT if Ombudsman investigation/review is on foot. • Ombudsman can investigate decisions and delays by agency but does not	If ACAT has made a mistake of law in its decision there is a right to appeal to the ACT Supreme Court (source for this???)

56 FOI Act 1991, s 29(3).

66 FOI Act 1989, ss 60-63.

Jurisdiction	Types of review and internal review process	External review	Other review/appeal rights
	• must have internal review before external review unless internal review not possible (see below) • no internal review where review is of a decision of a Minister or principal officer • reconsideration of initial decision • review on the merits – reconsideration of initial decision • agency may confirm, vary or reverse the determination under review[65]	undertake a review on the merits like ACAT:[67] o cannot appeal to ACAT until Ombudsman's report on complaint is provided	
Northern Territory	Parts 3, 7 and 7A of *Information Act* (IA) govern reviews of decisions. The review types are:: • internal review (compulsory, except in certain circumstances), then • external review by the NT Information Commissioner, and	<u>External review by NT Information Commissioner</u> External review under Part 7 of the IA by the NT Information Commissioner (complaint): • by a person aggrieved by internal review decision • internal review application can also be referred to Information Commissioner by the agency[70] • cannot further review decision if Information Commissioner has referred	Under Part 8 of the IA, a person aggrieved by an appealable decision may appeal to the Supreme Court on a question of law only.

65 FOI Act 1989, s 29.

67 See FOI Act 1989, Part 6.

70 IA, s 103.

Jurisdiction	Types of review and internal review process	External review	Other review/appeal rights
	• referral to NT Civil and Administrative Tribunal in certain circumstances. <u>Internal review</u> Under Part 3, Division 4: • person aggrieved by agency decision may apply for internal review[68] • reconsideration of decision on merits • may confirm or vary or revoke decision and remake decision • can also send application to the Information Commissioner[69]	complaint back to agency for further review • many grounds in s 106 on which Information Commissioner can refuse to deal with complaint • can also refer complaints to other bodies (eg ombudsman)[71] • Information Commissioner must investigate the matter in manner considered appropriate. If substantiated, it must go to mediation under s 111[72] • if no resolution in mediation, the Information Commissioner investigates further and makes a decision • parties can ask for referral to NT Civil and Administrative Tribunal (NCAT) if matter not resolved at mediation or complainant can ask if Information Commissioner decides insufficient evidence to proceed[73] and the matter must be referred to NCAT. Part 7A covers review by NCAT: • NCAT must conduct a hearing of the complaint	

68 IA s 38.

69 IA, s 39A.

71 IA, s 108.

72 However, mediation can occur at any time during the Information Commissioner's investigation: IA, s 110.

73 IA, s 112A.

Jurisdiction	Types of review and internal review process	External review	Other review/appeal rights
		• NCAT can confirm or vary decision or revoke and make a new decision (ie merits review). • If the referral is because of dismissal for insufficient evidence, NCAT can confirm that decision. If decides sufficient evidence, NCAT can refer back to mediation or conduct a hearing[74]	
Commonwealth	The *Freedom of Information Act 1982* (Cth FOI Act) provides for • internal review (optional), and/or • external review by Information Commissioner, then • review by the Administrative Appeal Tribunal (AAT) of decision by the Information Commissioner. Can also appeal to Federal Court on a matter of law Internal review	Part VII of the Cth FOI Act covers external review by the Information Commissioner: • application by applicant or certain affected third parties • merits review • decision can be varied or set aside and a new decision substituted[76] • can refer a question of law to the Federal Court[77] The Information Commissioner can decline to undertake a review if satisfied 'that the interests of the administration of the [FOI] Act make it desirable' that the AAT consider the review application.[78] For example, the IC	Part VIIA of the Cth FOI Act enables review of certain decisions by the Information Commissioner (such as decision to to affirm, vary or set aside a decision.[79] AAT has power to review any decision that has been made by an agency or Minister and to decide any matter that could have been or could be decided by an agency or Minister.[80]

74 IA, s 115D.

76 Cth FOI Act, s 55K.

77 Cth FOI Act, s 55H.

78 Cth FOI Act, s 54W(b).

79 Cth FOI Act ss 55K and 57A(1)(a).

80 Cth FOI Act, s 58.

Jurisdiction	Types of review and internal review process	External review	Other review/appeal rights
	Under Part VI of the Cth FOI Act: • application by access applicant or affected third party • cannot seek Internal review if decision made by Minister or principal officer to a deemed refusal[75] • merits review – reconsideration of original decision	review is linked to ongoing proceedings before the AAT or a court. An agency or minister must comply with an IC review decision (s 55N). If an agency or minister fails to comply, the Information Commissioner or the review applicant may apply to the Federal Court for an order directing them to comply under s 55P(1).	The Federal Court may determine matters in two situations: • deciding questions of law referred by the Information Commissioner • on appeal on a question of law from the Information Commissioner's decision[81] The Federal Court may also direct an agency or minister to comply with the Information Commissioner's decision
Queensland	Three review options: • internal review by the agency (optional), or • external review by the Queensland Information Commissioner (QIC) of certain decisions made by an agency under the RTI Act or IP Act.	*Under s 85 RTI Act, 'a person affected by a reviewable decision'*[82] can apply for external review • do not need to first undergo internal review • certain decisions made by agencies under the RTI Act and IP Act to be independently reviewed by the QIC.	May be limited rights of appeal following an external review to QCAT. Only on a question of law and after OIC makes a formal decision which is adverse to applicant

75 Cth FOI Act, ss 54-54E.

81 Cth FOI Act, s 56.

82 Schedule 6 of the RTI Act provides an exhaustive list of *'reviewable decisions'*.

Jurisdiction	Types of review and internal review process	External review	Other review/appeal rights
		• reconsiders all aspects of the original decision including questions of law, questions of fact, discretion and policy	

22. Should the OIC have additional powers to obtain documents for the purposes of its performance monitoring, auditing and reporting functions?

Additional powers of this nature do not seem to be necessary as agencies cooperate with the Office of the Information Commissioner in relation to its performance of these functions.

23. Is the information provided in the Right to Information and Privacy Annual Report useful? Should some of the requirements be removed? Should other information be included? What information is it important to have available?

It is considered that the types of information provided should remain as it is now, with additional measures taken administratively to ensure consistency in the way agencies report statistics.

24. What would be the advantages and disadvantages of aligning the IPPs and/or the NPPs with the APPs, or adopting the APPs in Queensland?

Adopting the APPs by Queensland is not supported at this time as it would impose a significant compliance burden for arguably little benefit for Queenslanders and without achieving the main object, namely harmonisation of privacy laws Australia-wide. Consideration might be given to whether or not there is still benefit in retaining the NPPs, and that the obligations of Queensland health agencies should be amended to align with either the IPPs or the APPs.

However, there are some aspects of the federal privacy regime which might be worthy of incorporating into the Queensland privacy regime, and they are discussed below.

24.1 Should Queensland adopt the Australian Privacy Principles?

Prior to 2014, the Commonwealth Privacy regime contained two sets of privacy principles: Information Privacy Principles (IPPs) applying to the public sector, and National Privacy Principles (NPPs) applying to the private sector. In 2014, these were replaced by one set of privacy principles, the Australian Privacy Principles (APPs) that apply to both the Commonwealth public sector and particular private sector organisations. The IPPs in the Queensland IP Act were modelled on the IPPs in the Commonwealth Act.

A review of the new APPs finds that although their purpose covers similar territory to the Queensland IPPs, there are enough differences to take a very cautious approach to the question of whether or not adopting the APPs would best serve Queenslanders.

The IPPs were introduced in 2009 and closely resembled the previous administrative privacy scheme contained in the now repealed Information Standard 42 (IS 42). Since 2010, local governments have been covered by the IP Act. Queensland public entities and contracted service providers have also been bound by IPPs since the introduction of IS42 in early 2000 and the subsequent introduction of the IP Act in 2009.

The Queensland public sector (and other affected entities) has implemented its privacy regime in accordance with those IPPs and information handling practices have been adopted to comply with those principles. The implementation and compliance costs which

would come with introducing a completely different set of privacy principles, both in structure and content, would be significant for, arguably, little benefit for Queenslanders.

The main driver for considering adopting the APPs would be to move towards a national privacy scheme. This is an important goal as it would mean greater certainty for the community across borders as well as potentially removing the need for business to comply with various privacy obligations if they do business across borders or meet the threshold for coming under the Commonwealth privacy scheme.

However, before moving to adopt the APPs consideration should be given to the following:

- There is no national commitment to adopt the APPs so to move to the APPs without the likelihood of the other states adopting the same principles would not greatly assist the community in terms of red tape and cross jurisdictional issues.
- The APPs have been developed to deal with private as well as public sector environments. It may be that the privacy issues confronting these two environments are not sufficiently similar to warrant adopting common obligations. It is likely that the critical private sector privacy issues are not issues for the public sector because of the regulatory and integrity frameworks that apply to the public sector.
- The IP Act obligations have had the benefit of lessons learned from 2000 when IS 42 was introduced. The costs of implementing a new scheme aligned with the APPs would be significant at a time of fiscal restraint. If resources need to be reallocated to implement a different regulatory scheme then other work will need to be deferred.

However, a review of the IPPs is timely because there have been a small number of recurring issues identified since implementation and this review presents an opportunity to rectify these so that Queensland can have a mature privacy scheme that strikes the right balance between protecting the personal information held by government and the ability of government to facilitate the provision of services to the community. Making some minor amendments to the IP Act will assist in the development of a mature privacy regime for Queensland.

24.3 Comments relating to the APPs

APP 1—open and transparent management of personal information

Section 27 of the IP Act states that agencies 'must' comply with the privacy principles. The Commonwealth Act adopts an approach that allows for agencies to take a risk assessment approach to the implementation of the privacy principles. This recognises that circumstances might impact on an agency's ability to strictly comply with all the obligations in relation to all its information holdings. The approach taken in APP 1 seems to be a sensible way to deal with compliance which should be considered for incorporating into the IP Act by amending section 27.

The wording of APP1.2 is clear and may provide a model for section 27.

> ***APP 1***
>
> ***Compliance with the APPs etc.***
>
> *1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:*
>
> *(a) will ensure that the entity complies with the APPs and a registered APP code (if any) that binds the entity; and*
>
> *(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the APPs or such a code.*

In relation to the APP1 privacy policy objectives, these are adequately provided for in IPP5 of the IP Act.

APP 2—anonymity and pseudonymity

This provision would appear to be unnecessary. From this department's perspective, this is not a live issue for our clients or the community generally. Notifications about children in need of protection are frequently made anonymously. Feedback via the departmental portal is able to be made anonymously and complaints about service or the conduct of business of the department are currently able to be made anonymously where the identity of the complainant is not critical to managing the complaint.

Placing a general right of anonymity for any transaction or communication with an agency may impose unnecessary constraint upon how the agency conducts its business, arguably leading to privacy complaints arising from a refusal to allow anonymity or pseudonymity in particular circumstances.

APP 3—collection of solicited personal information

IPP 1 adequately deals with the collection of personal information.

APP 3 prescribes conduct in relation to collecting 'sensitive personal information', a sub-set of personal information which is afforded a higher level of protection. The APP Guidelines note that having a class of sensitive personal information recognises that inappropriate handling of this type of information can have particular ramifications for the individual concerned or those associated with the individual.

However, the current framework of the IP Act appears to work well to protect the type of information defined as 'sensitive' in the Commonwealth Act. Under the IP Act, the sensitivity of the information is a prime consideration in determining the level of protection required for the type of information. Applying a two tier approach would not add any greater protection *per se*. Agencies are used to working within that framework and it would appear to be unnecessary to overly complicate the obligations by having separate obligations in relation to

prescribed types of information. A move to a model that prescribes particular classes of personal information that require different information handling practices would be onerous to administer and arguably add no value or greater protection for the community.

APP 4—dealing with unsolicited personal information

APP 4 would place onerous obligations on agencies dealing with personal information that has not been solicited by the agency. Essentially, APP 4 requires agencies to assess each item of personal information that is sent to it and determine whether or not it could have been collected under APP 3 and if not, then the agency must destroy or de-identify the information, unless it is in a Commonwealth record. If the agency could have collected the information under APP 3 then APPs 5 – 13 apply to that information.

The Queensland IP Act currently does not place additional obligations on agencies in respect of unsolicited information and it is this department's view that the status quo should be maintained in this regard. It is acknowledged that having to manage a range of information that has been provided to the agency does pose challenges but usually the department's record keeping obligations and its retention and disposal schedule should deal adequately with much of the unsolicited information.

APP 5—notification of the collection of personal information

Elsewhere in this submission there are recommendations about the wording of IPP 2 which deals with the core ideas in APP 5. However, IPP 2 is clearer than APP 5 and adequately deals with the issues of collection notice obligations. To change the IPP 2 obligations, even marginally, would result in significant implementation costs across government because every collection notice at every point of collection would need to be reworded, including all forms, counter signs, telephone notices and web notices.

APP 6—use or disclosure of personal information

APP 6 equates to IPPs 10 and 11 – Use and Disclosure. Comments on and suggested amendments to IPPs 10 and 11 are found later in this submission.

Apart from those issues, we believe the structure of the IPPs 10 and 11 are clearer than APP 6 and that it is simpler to deal with use and disclosure issues as separate principles.

APP 7—direct marketing

The direct marketing APP applies only to organisations – not APP entities that are a part of the public sector. IPP 11(4) provides similar protection in relation to the public sector (and bound contracted service providers (CSPs)) which would appear to be adequate in the circumstances.

APP 8—cross-border disclosure of personal information

Section 33 of the IP Act deals with the overseas transfer of personal information. This is an increasingly important aspect of privacy regulation, particularly in the context of globalisation

and IT trends which increasingly cross national and international borders. An appropriate balance needs to be struck between adequate privacy protection for the community, facilitation of services and fulfilling the functions of government.

Comments in relation to section 33 appear below, but in short the APP 8 obligations in relation to the overseas transfer of personal information appear to be complex and onerous. The preferred approach is to maintain section 33 as a stand-alone obligation in the Act with the amendments suggested by the department.

APP 9—adoption, use or disclosure of government related identifiers

APP 9 relates only to non-government organisations and regulates their handling of government related identifiers (GRIs) such as the CRV social security number and the Medicare number. There is no equivalent IPP in the IP Act.

The department is not aware of agencies or CSPs adopting GRIs as their own identifiers, but if it is assessed that this is an issue, it would be open to the review to make special provision for GRIs in the IP Act so that it is clear that those numbers are not to be adopted as identifiers by the receiving agency.

APP 10—quality of personal information

IPPs 3 and 8 deal with the collection and use of personal information and agencies' obligations in relation to ensuring that information is 'up to date and complete'. There would appear to be no real benefit in changing the current IPPs in relation to this APP.

APP 11—security of personal information

IPP 4 deals with similar obligations to those contained in APP 11. The comments on and suggested amendment to IPP 4 are found later in this submission. In short, it is suggested that the wording of APP 11(1) be considered to replace the similar obligation in IPP 4 because it is less ambiguous making it easier for agencies to apply and for the community to understand.

APP 4(2) however, is not provided for in the IPPs and it is recommended that it not be considered for inclusion. APP 4(2) places an obligation on agencies to destroy or de-identify personal information no longer needed by the agency if the information is not contained in a (Commonwealth) record. The comments above in relation to APP 4 apply equally to this APP in that such an obligation would require systems to be put in place to assess all personal information for whether it was a record or not and, if not, whether the information is still needed by the agency. If not needed then the information would need to be subject to a destruction schedule or de-identification process. This would be an onerous administrative process and arguably one that would be difficult to comply with, with any great precision. The department's record keeping obligations and the retention and disposal schedules already deal adequately with this process.

APP 12—access to personal information

APP 12 provides for an access scheme which appears to be a quasi RTI scheme. IPP 6 contains a similar provision but it is recommended that access and amendment provisions be removed from the IP Act and placed in the RTI Act, so that there is one statutory access mechanism. This would eliminate current confusion for applicants in having two access and amendment rights in two separate statutes.

IPP 6 should then be amended to make it clear that obligation under IPP6 may be met by way of an application under an administrative access scheme or a statutory access mechanism (eg RTI Act). This qualification is necessary to ensure that people who simply 'ask' for access to their personal information and don't use the established access mechanisms cannot then make a privacy complaint if they are not given access and are advised to use a statutory or other approved process. It would also clarify the obligations of contracted service providers who are contractually bound to comply with the relevant parts of the IP Act but are not subject to the RTI Act.

APP 13—correction of personal information

APP 13 deals with amendment and correction of personal information – its equivalent is IPP 7 and it is recommended that access and amendment provisions be moved to the RTI Act. If the one Act approach is adopted then it would be necessary to amend IPP7 to make it clear that it is sufficient to meet the requirements of IPP 7 if a person has a right to apply to amend their own personal information under an administrative process or a statutory mechanism (e.g. RTI Act). As outlined above, this qualification is necessary to ensure that people who simply 'ask' to amend their personal information cannot then make a privacy complaint information if it is not amended and they are advised to use a statutory or other process. It would also clarify the obligations of contracted service providers who are contractually bound to comply with the relevant parts of the IP Act but are not subject to the RTI Act.

25. Should the definition of 'personal information' in the IP Act be the same as the definition in the Commonwealth Act?

Given that information must be '*personal information'* to trigger the protections under the IP Act and to be able to seek redress if personal information is misused, it is important for there to be precision about the meaning of 'personal information' and it is worth considering amending the IP Act definition to achieve more certainty.

It has been the department's experience that the broad definition of personal information captures information which either does not have a 'personal' aspect (e.g. professional, business or commercial information, and routine work related information) or information in relation to which there cannot reasonably be an expectation of privacy. Placing special obligations on departments for handling information that is not of a 'personal character' appears to be unintended. The current broad definition does give rise to privacy complaints with little or no merit, but which still require substantial resources to respond to and defend.

Having now had 7 years' experience in working with the current definition of 'personal information' we have come to the view that the definition could be amended along the following lines:

> *This Act applies to information (personal information) of a personal character, recorded in any form, whether true or not, about an individual whose identity is apparent or can reasonably be ascertained.*

Including the phrase 'of a personal character' distinguishes information which has the necessary quality of privacy from information of a non-personal character, e.g. that a person is a chair of a committee, CEO of a non-government organisation, public servant, office bearer of community organisation, member of board, proprietor of business.

Currently in the Queensland IP Act, 'personal information' can include any identifying information, including information that would not usually be considered to be information relating to the private/personal aspects of a person's life, for example, routine work information, capturing an employee's name in work systems, official work matters, commercial information, professional information etc.

The now repealed FOI Act made a distinction between 'personal information' (which was very broad and encompassed identity information) and 'personal affairs information', which referred to 'affairs of or relating to the private aspects of a person's life'[83]. There is information that clearly falls within the ambit of 'personal affairs information' and that which clearly does not. In between, there is a grey area.

For the 'grey area', the guiding principle is that 'personal affairs information' covers information concerning the affairs of a person the dissemination of which that person ought to be entitled to control.[84] This notion aligns with the principles underpinning the development of privacy, namely openness (a person should be able to find out what information is held about them) and control (as far as possible, a person should be able to control the way information about them is used or disseminated).

It may be useful for the development of Queensland's privacy regime in this area to consider the distinction drawn in the FOI space by the IC in the decision of *Stewart and the Department of Transport* (1993) 1 QAR 227 between personal affairs and business affairs and the consideration given to business, professional, commercial and affairs.

25.2 Minor recommended changes to definition of 'personal information'

If the proposed new definition of personal information is not accepted, the following matters should be considered as part of the review of the current definition of 'personal information':

- The terminology *'including information or an opinion forming part of a database'* is arguably outdated. It seems unnecessary that just one type of storage method is specifically referred to. The italicised words could be removed from the definition. The

---

83 *Stewart and Department of Transport*(1993) 1 QAR 227, paras

84 *Stewart and Department of Transport* (1993) 1 QAR 227, paras 75, 76.

essential thing is that the information is 'recorded' not the particular form in which it is recorded.

- It must be personal information that has been *recorded*, i.e. documented by the agency as distinct from a thought or idea or opinion in a person's mind which has never been captured in any material form. It appears that the reference in the definition to information whether 'recorded in a material form or not' may have been an attempt to clarify the *method* of recording information i.e. whether held in a database or electronically, as opposed to hard copy records. In that regard, it is noted that the IPPs refer to information in 'documents' suggesting the need for actual 'recording' in some material form (whether hard copy or electronic). This can be addressed in the definition by including the words 'recorded in any form'.
- It is important that the personal information protected is only to the extent that a person's identity can be ascertained from readily available other information without needing to undertake many other steps or inquiries to establish a link to the person's identity. However, the phrase *'from the information'* has created some uncertainty. There was opinion obtained soon after the introduction of the IP Act that on plain reading, the material used to ascertain identity was limited to the actual information – with no recourse to any extraneous material. Such an approach would weaken the protections. The better approach to privacy protection, particularly in the digital and Open Data environment, is to make it certain that information is personal information if the identity of an individual can *reasonably be ascertained*, not just from the information itself, but from a range of information that may be available to a person or the community. As noted above, there is case law to the effect that you can refer to other information, but the plain reading of those words seems to suggest otherwise.

25.3 'About an individual whose identity is apparent or reasonably ascertained'

The OIC's Guidelines state that for information to be 'personal information' two criteria must satisfied:

- it must be *about* an individual – in the circumstances in which the information appears, there is sufficient connection/link between the fact or opinion and the individual to reveal something about the individual. Clear examples are medical records, financial records, salary information. In other cases, the link will not be so obvious. However, information stating that rates for a specified property have not been paid is about that land but also shows that its owner has not paid them (the land owner land is able to be readily searched for after paying a small fee, thus the person's identity is readily ascertainable),[85] and
- the individual's identity must be reasonably ascertainable from the information or opinion – it will be 'apparent' if identity can be found without needing to refer to other information. It will be 'reasonably ascertainable' if the information can be cross-referenced with other information to identity the person but how far this cross-referencing can go depends on the circumstances (e.g. is other information readily

[85] Queensland Office of the Information Commissioner (OIC) *Guidelines to Information Privacy Act 2009 – Section 12 Personal information*, 4 March 2016.

available? How many steps are required to identify the person? How certain with the identification be?).[86]

'About an individual'

The OIC approach is consistent with the Administrative Appeals Tribunal (AAT) decision in *Telstra Corporation Limited and Privacy Commissioner*[87] where Deputy President Forgie said that the threshold question is whether the information is 'about an individual', and only then do you consider whether their identity is apparent or can reasonably be ascertained.

However, in considering that threshold question, she stated that there had to be 'more than a tenuous link to the individual'; it was not enough that the information would not have existed but for the individual in question. She gave the following examples:

- Information in service records for a car that the Deputy President had purchased was information about the car, or about the repairs that had been carried out on the car, but was not information about the Deputy President, even though the records may have referred to the registration number of the car and even her name.
- In an accident involving a motorist and a pedestrian, any hospital records about the treatment of the pedestrian for injuries sustained in the accident would not be information "about" the motorist, even though the identity of the motorist could potentially be traced by linking the hospital admission records to the ambulance records and then to the accident report.

The decision was taken on appeal to the Full Court of the Federal Court[88], but the only issue raised in the appeal was whether the words 'about an individual' in NPP6.1 (as it was at the relevant time) had any substantive effect. No issue was raised on the appeal about its application to the facts, and the appeal was dismissed.

The decision in *McKay and Department of Justice and Attorney-General* is also relevant in this context. It concerned a report of an investigation of a complaint about staff and it was held that this was information *about* those staff not *about* the complainant.[89] This appears to be consistent with the Deputy President's approach in *Telstra Corporation Limited and Privacy Commissioner.*

'Reasonably ascertainable'

The extent of the actions that need to be taken for identity to be 'reasonably ascertainable' was considered by Deputy President Forgie in *Telstra Corporation Limited and Privacy*

---

86 Queensland Office of the Information Commissioner, *Guidelines to Information Privacy Act 2009 – Section 12 Personal information*, 4 March 2016; Queensland Office of the Information Commissioner, *Guidelines: Routine personal work information of public sector employees*, 4 February 2014.

87 *Telstra Corporation Limited and Privacy Commissioner* [2015] AATA 991 (18 December 2015)

88 *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 (19 January 2017) http://www.austlii.edu.au/cgi-bin/sinodisp/au/cases/cth/FCAFC/2017/4.html?stem=0&synonyms=0&query=privacy%20commissioner%20telstra

89 *Re McKay and Department of Justice and Attorney-General*, (Queensland Information Commissioner, 25 May 2010) para 81.

Commissioner. At paragraph 72, Deputy President Forgie quoted Deputy President Coghlan in *WL v La Trobe University*[90] (*WL*):

> As to whether WL's identity could "... *reasonably be ascertained, from information or opinion*" Deputy President thought that the use of some extraneous material or information might be contemplated.

In paragraph 74, Deputy President Forgie went on to quote Deputy President Coghlan's conclusion:

> "*Even allowing for the use of external information, the legislation requires an element of reasonableness about whether a person's identity can be ascertained from the information and this will depend upon all the circumstances in each particular case. Here, the alleged process of ascertainment would require inquiries from different databases, cross-matching and then cross-matching with an external database and even then the making of any possible connections would not identify with certainty. Even on the most favourable view to the applicant, this is beyond what is reasonable.*"[91]

It is recommended that some guidance be provided for practitioners and the public by the IC, about what will fall within the scope of information '*about an individual whose identity is apparent or can reasonably be ascertained*'.

25.4 Application of the Act to deceased persons

There is some dispute as to whether the information handling obligations on departments apply equally to information of living and deceased people. This department provides equal protection under the IP Act of information of living and deceased people.

The IC is of the view is that the obligations under the IP Act do not apply to the personal information of deceased persons because 'personal information' refers to an 'individual'. However, it is not clear on what basis that view is formed.

The term 'individual' is not defined in the IP Act. Thus, it is necessary to refer to the *Acts Interpretation Act 1954* (Qld) (AIA). Under Schedule 1 of the AIA:

> ***individual*** means a natural person

and

> ***person*** includes an individual and a corporation.

The term, 'natural person' is not further defined in the AIA Act.

Section 32D(1) of the AIA provides that, in an Act, a reference to a person generally includes a reference to a corporation as well as an individual.

---

[90] *Telstra Corporation Limited and Privacy Commissioner* [2015] AATA 991 (18 December 2015) footnote 57
[91] *Telstra Corporation Limited and Privacy Commissioner* [2015] AATA 991 (18 December 2015) footnote 62

Thus, it would seem that the context of the AIA definition of 'individual' is by way of juxtaposing a human being from an artificial being, such as a corporate entity. It is unclear whether the human being must be a *living* human being but it would seem that the crucial point is to distinguish an individual as a human being rather than an artificial corporate being.

In the Federal context, the Australian Law Reform Commission noted that in the Office of the Privacy Commissioner's review of the private sector provisions of the Commonwealth *Privacy Act* (the OPC Review), it was said that:

> *The term 'natural person' is not defined under the Privacy Act or the Acts Interpretation Act 1901; however it appears the term is usually used to distinguish human beings from artificial persons or corporations. Whether the term 'natural persons' includes a deceased human being does not appear to have been subject to judicial consideration in Australia or the United Kingdom. The Office considers the term 'natural person' to mean a living human being as this is the plain English meaning of the term.*[92]

Turning to a consideration of the 'plain English meaning' (as referred to by the Commonwealth OPC) of the term *natural person*, a number of dictionary definitions define 'natural person' in the context of an individual as distinct from a body corporate or other artificial legal entity. For example, the *Oxford Dictionary online* provides:

> a *natural person* is 'a person having legal status as an individual as distinct from a body corporate, representative etc.[93]

Osborn's Concise Law Dictionary provides the following definition:

> *Natural persons.* Human beings, as distinguished from artificial persons or corporations recognised by the law eg. Companies.[94]

Arguably, those general definitions do not differentiate between living and dead human beings or individuals – the main point is that these human beings/individuals are not artificial beings.

The Commonwealth Office of the Privacy Commissioner (OPC) has taken '*the term 'natural person' to mean a living human being as this is the plain English meaning of the term*'.

Similarly, the Queensland Office of the Information Commissioner's *Privacy Principles Guidelines*, it is stated that:

> *'Individual' is not defined in the IP Act, but it is defined in the Acts Interpretation Act 1954 (Qld) as a natural person. This means that only living people can have personal information.*

---

92 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (ALRC Final Report 108), 2008, Chapter 8, citing Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 281

93 *Oxford Dictionary online (English).*

94 R Bird, *Osborn's Concise Law Dictionary,* 7th ed., 1983.

It is not clear why that distinction is made between the living and the dead. It may be that the Commonwealth OPC and Queensland Information Commissioner could be adding an extra 'layer' to the concept of 'human being'/'individual' when the focus of the definition is to draw the distinction with corporations and similar artificial bodies.

In Chapter 8 of the *Your Right to Know* Report, the ALRC considered whether the *Privacy Act 1988* (Cth) should be amended to provide protection for the personal information of deceased individuals. The ALRC said that while a deceased individual may 'feel no shame or humiliation', there are sound public policy reasons to regulate the use and disclosure of the personal information of deceased individuals; access by third parties; data quality; and data security.[95]

At paras 8.43-8.44, the ALRC said:

> *8.43. …. On balance, in the ALRC's view, the Privacy Act should be amended to include provisions on the handling of personal information of deceased individuals where that information is held by organisations. This would have a number of benefits. It would introduce a level of consistency in the way this information is handled across the private sector. Currently, personal information held by organisations may be subject to state or territory legislative requirements, a duty of confidentiality or simply dealt with as a matter of organisational policy. It would also allow the Privacy Commissioner to become involved where there is a dispute about the handling of such information*.
>
> *8.44 The ALRC notes the view that the right to privacy attaches to the individual and should not survive the death of the individual, but is of the view that there are legitimate public policy reasons for extending some protection to the personal information of deceased individuals. These include: the fact that individuals may hesitate to share personal information while they are alive if they believe that the information may be handled inappropriately after they die; the need for living individuals to access the personal information of deceased individuals in some circumstances; and the distress caused to living individuals where the personal information of deceased individuals is handled inappropriately…..*

The question then becomes one of whether or not it is desirable to afford deceased people the same protections as living persons. As a human services department which holds a great deal of personal information of deceased people it would be preferable from the community's perspective to have that information subject to at least a minimum requirement in relation to information handling practices. Currently this department does not distinguish between living or deceased persons' information for the purpose of the IPP obligations in practice. It is accepted that a deceased person is not able to have a 'privacy interest' and is not entitled to make a privacy complaint pleading a 'breach of privacy'. However, the IP Act is not a statute which is rights based, except in relation to lodging complaints. It sets standards for agencies for personal information handling practices. If it is not clear that the IP Act applies to deceased persons, then perhaps an amendment could be made to clarify this matter.

---

[95] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (ALRC Final Report 108), 2008, Chapter 8, para [4.2].

However, personal information of persons (whether living or deceased) which is held by government should not be subject to strict prohibitions on disclosure such as those found in IPP11 where that information is needed for the purposes of establishing family linkages for the purpose of cultural identity or where it is otherwise in the public interest (e.g. to parents of deceased children). This could be included as an additional exception in IPP11.

26. Does the IP Act inappropriately restrict the sharing of information? If so, in what ways? Do the exceptions need to be modified? Would adopting a 'use' model within government be beneficial? Are other exceptions required where information is disclosed?

26.1 Sharing personal information between government agencies – the 'use' model

Under the IP Act, 'use' and 'disclosure' of personal information are separate concepts and are defined in section 23. The crucial distinction appears to be the relinquishment of effective control over the personal information.

While a sharing of information within different parts or unit of one government agency will be a 'use', section 23(5) provides that 'use' of the personal information does not include the action of disclosing the personal information to another entity. Thus, if one government agency shares information with another government agency, it is a 'disclosure' rather than a 'use'.

The Information Privacy Principles (IPPs) deal with the 'use' of personal information in IPPs 8- 10 and 'disclosure' of such information in IPP 11.

There has been considerable discussion about whether the IPPs unduly restrict information sharing between Queensland departments/agencies in other than situations such as exchanging information for protection of safety or health etc.

The Department strongly supports the adoption of a 'use' model within government to facilitate the proper sharing of information within government. In law, the State of Queensland is the legal entity so it would align with that concept. Government departments are established under Administrative Arrangements Orders the composition and names of which change relatively frequently under machinery-of-government changes (MOGs). These movements and realignments of government functions present challenges for information handling practices. Adopting a 'use' model rather than a 'disclosure' model would facilitate business across departments, give greater certainty in times of change and reduce red tape by removing artificial barriers to doing business and delivering services to Queenslanders.

Under a 'use' model, a department that obtains information for a particular purpose would be able to give that information to another department if it was to be used for the particular purpose for which it was collected or another purpose that was directly related to the purpose for which it was obtained. This approach maintains a 'purpose-related' focus, still restricting uses to the original purpose and safeguarding information from use for totally unrelated purposes and for purposes which the individual would not expect, which would uphold the intention of these particular protections. It also means that the community would

benefit by not being required to provide the same information to different agencies in connection with the provision of the same or related services. It may require some conditions so that the secondary purpose doesn't become a primary purpose in the other department, but these are drafting issues to be considered by the parliamentary counsel.

At a minimum, the use model should be applied to Queensland government departments (including bodies such as the Office of the Public Guardian). Consideration should be given to whether it should extend to independent bodies such as Queensland Family and Child Commission, Ombudsman, Queensland Audit Office and the Office of the Information Commissioner.

The 'use' model is not adopted by any other jurisdiction but from an agency's perspective it would facilitate service delivery whilst maintaining the other important protections in the IP Act which ensure that personal information is handled appropriately.

27. Does section 33 create concerns for agencies seeking to transfer personal information, particularly through their use of technology? Are the exceptions in section 33 adequate? Should section 33 refer to the disclosure, rather than the transfer, of information outside Australia?

In the current global climate, business and agencies are increasingly taking advantage of new technologies that require personal information to be transferred overseas. The use of technologies such as cloud computing and web tools allows agencies to deal with personal information faster in turn improving their business performance and cost efficiency. In some cases, the use of these technologies may also improve privacy protections. However, there are compliance and privacy risks for agencies, particularly if the use of such technologies may result in the transfer of personal information outside of Australia in circumstances where the requirements of section 33 are not able to be met.

Section 33 of the IP Act restricts the circumstances in which agencies may transfer personal information outside of Australia. It is arguable that, when compared with privacy legislation in other Australian jurisdictions (where such transfer legislation exists), the Queensland provisions in section 33 are much more restrictive.

As part of the Commonwealth's *Privacy Amendment (Enhancing Privacy Protection) Act 2012* amendments, changes have been made in relation to cross border data flows with the new APP 8. The amendment moves the focus from 'transfer' to 'disclosure' of personal information to overseas recipients. 'Disclosure' appears to be much better suited to accommodate the demands of operating in a global digital environment than 'transfer'. In relation to online data flows this would seem to suggest for example, that the mere routing of personal information through servers outside of Australia, where there is no access to the information by a third party, will not be a 'disclosure' under APP 8. Similarly, if encrypted information is stored on a cloud platform hosted overseas and not accessed by the host, there is no 'disclosure'. These Commonwealth changes to 'disclosure' would facilitate business across international borders.

It is recommended that Queensland consider adopting the concept of 'disclosure' similar to APP 8 in section 33 and omit 'transfer'. Use of 'disclosure' would be less restrictive, as a disclosure could occur when an overseas recipient accesses the personal information, whether or not the personal information that is accessed is stored on a server in Australia or elsewhere, for example, in the cloud. It also recognises the reality that in the digital age, access is not determined by physical proximity.

Further, it is recommended that the current exceptions in section 33 be amended and the subparagraphs be listed as separate alternatives. In addition, it is recommended that changes to section 33(d)(i) be made to incorporate APP 8 subclause 8.2 (a) (i) and (ii) such that an agency may disclose personal information to an overseas recipient if:

(a) the entity reasonably believes that:

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the privacy principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme.

The above proposal would need to ensure that a person whose privacy is breached would not have to resort to international legal action for remedy – there should be a way of ensuring that such breaches be actioned under Queensland law.

28. Should the IP Act provide more flexibility about the timeframe for complaints to the OIC to be lodged? How should this be approached?

There should be more clarity about the complaints process generally, including timeframes, in the IP Act. Given the privacy complaint jurisdiction allows for the award by QCAT of up to $100,000 in compensation for a privacy breach, the complaints processes should be robust and transparent. The agencies and the community would benefit from having the complaints process better prescribed. To that end, the Act should provide detail about the complaints handling process including the threshold requirements for applications, complaint handling processes for agencies and the IC, and the scope of QCAT referrals.

The current provisions in the IP Act do not adequately detail the process for agencies and the IC in dealing with privacy complaints. This creates uncertainty and inconsistency for agency complaint outcomes. This is in stark contrast to the detailed processes specified for applications for access and amendment of personal information held by an agency. There is certainly merit in processes remaining flexible enough to accommodate differences between agencies. However, a standard approach would alleviate uncertainty and inconsistency for complainants and agencies alike.

The privacy complaint handling guidelines issued by the IC are high level and provide very little guidance for agencies or complainants in managing privacy complaints and about how the IC will manage privacy complaints. By contrast the IC publishes comprehensive external

review guidelines under the RTI and IP Acts for both parties in relation to access and amendment applications.

Additionally, while there is provision for mediation in the IP Act, there is no detail regarding how the IC is to conduct the mediation process. This creates uncertainty and confusion for agencies on how the IC will deal with a privacy complaint. From this department's experience the process adopted by the IC is closer to informal resolution on the papers rather than a mediation model.

28.1 Privacy complaints to an agency

The IP Act does not clearly outline that privacy complaints must be first made to an agency nor does it specify validity requirements, timeframes or guidance on how to deal with complaints.

Reliance on agencies to develop an appropriate privacy complaints handling practice is not sufficient to ensure certainty and consistency, and there could be some legislative guidance and standardisation across the sector, as is the case in most other comparable jurisdictions.

Consideration could be given to including specific provisions in the IP Act that address how agencies should deal with privacy complaints made to an agency.

Validity requirements

The Act could include validity requirements for a privacy complaint:

(a) be in writing

(b) be addressed to the relevant entity

(c) state an address of the complainant to which notices may be given

(d) be made to the relevant entity within 6 months from the time the complainant first became aware of the act or practice the subject of the complaint

(e) give full particulars of the act or practice complained of, including:

(i) when the act or practice occurred; and

(ii) the date on which the complainant became aware of the act or practice; and

(iii) which information privacy principles the complainant believes the relevant entity has failed to comply with

Dealing with complaints

The complaints experience for complainants and agencies could be improved by providing statutory guidance on how an agency is to deal with complaints including particular actions that must be undertaken. The IP Act does not provide for what constitutes a 'response'. Advice has suggested that the requirement for a response could be fulfilled by mere acknowledgment of a complaint.

The IP Act could be amended to stipulate:

- That the relevant entity must:

(a) acknowledge the complaint (i.e. the relevant entity must with a specified period of time after the complaint is made give the complainant a written notice that acknowledges the complaint), confirming in writing with the complainant the exact terms of the complaint (in order to focus the matters in dispute for both parties);
(b) investigate the complaint, with a reasonable time in which to adequately do so; and
(c) provide a formal response to the complainant, i.e. after investigating the complaint, the relevant entity must, within a specified period (i.e. 45 business days, or longer as agreed with the complainant or the IC; see discussion below) set out the outcome and state that if the complainant is not satisfied with the outcome, they may make a complaint to the OIC or appropriate Tribunal under the applicable provision.

Timeframes for management of privacy complaints

The IP Act currently allows a minimum period of 45 business days for an agency to respond to a privacy complaint (section 166(3)(b)). If within that 45 business day period the agency has provided a response, but the complainant is not satisfied with the response or the agency has not provided a response to the complainant, the complaint may take their privacy complaint to the IC.

An agency's alibility to adequately investigate and respond to a privacy complaint within 45 business days will be different in every case and depend upon a number of factors:

Although the IC may decline to deal with the complaint because the agency has not had an adequate opportunity to deal with the complaint this makes it an additional unnecessary burden on agencies to then have to simultaneously deal with the IC in relation to a complaint that is still being investigated.

It is recommended that an agency be given scope to negotiate a reasonable time for the management of and dealing with privacy complaints.

28.2 Privacy Complaints to the IC

The current provisions about how the IC is to deal with a privacy complaint are uncertain and need clarification. The processes need to be robust and transparent, particularly given the privacy complaint jurisdiction allows for the award by QCAT of up to $100,000 in compensation for a privacy breach.

Validity requirements

The Act could require that a privacy complaint to the IC can only be made after a privacy complaint has been made to the relevant entity in accordance with its complaints management process and either –

- the relevant entity has provided a response but the complainant does not consider it to be an adequate response; or
- the period of 45 business days (or such longer period as may be approved by the IC) has expired.

The Act could also provide that a privacy complaint to the IC:

- *be in writing*
- *state an address of the complainant to which notices may be given*
- *be made to the IC within 20 business days (or such longer period as the IC may allow) from:*
    - *the date of the response to the complainant from the relevant entity, or*
    - *if no response has been received, the expiration of 45 business days (or such longer period as has been agreed between the complainant and the relevant entity) from the date the complainant complained to the relevant entity.*
- *give full particulars of the act or practice complained of, including:*
    - *when the act or practice occurred; and*
    - *the date on which the complainant became aware of the act or practice; and*
    - *which information privacy principles the complainant believes the relevant entity has failed to comply with, and*
    - *any response to the complaint provided by relevant entity.*

Dealing with complaints

The Act could require the IC to make preliminary enquiries with the relevant entity before accepting a complaint, unless it has determined not to accept the complaint.

It should also provide:

- that the IC process be confidential and without prejudice
- protections against actions for defamation or breach of confidence apply to participants to encourage open and frank discussions.

Section 168(1) could be amended to include the words in italics: 'may decline to deal *or decline to continue dealing* with a privacy complaint', because sometimes this information will only become known after the privacy complaint has been accepted and there is currently no power for the IC to decline to continue dealing with it.

Section 168 provides for when the IC may decline to deal with a privacy complaint. The grounds should be expanded to include:

- the power to dismiss stale complaints as is the case in other state/Commonwealth privacy legislation (i.e. Victoria)
- the power to decline to deal with a complaint if they have not first complained to the respondent (s168(1)(b)
- where the complainant has complained to the relevant entity as required, and the relevant entity has dealt or is dealing adequately with the complaint or has not yet had an adequate opportunity to deal with the complaint.

Mediation or another model?

This agency would support a review of the mediation of privacy complaints process under the IP Act. There needs to be greater certainty and accountability in the mediation process so that the confidentiality and protections issues are clear.

Currently the mediation complaints management processes as applied are inconsistent and difficult for both complainants and agencies to engage in an informative way outside of QCAT. This is highlighted by the experience of this agency which has been that the process adopted is one of shuttle negotiations rather than true mediation.

As part of a review, consideration should be given whether there are other forms of alternative dispute resolution (**ADR**) other than mediation better suited to privacy complaint management.

The IP Act provides for mediation of complaints in section 171 but only to specify that the IC must consider whether in the circumstances resolution of the complaint could be achieved through mediation (but no examples or factors to consider are provided) and if it is reasonably likely that resolution of the privacy complaint could be achieved through mediation the IC should take all reasonable steps to cause the complaint to be mediated.

There is no further statutory guidance on how the mediation process should occur or which complaints would be suitable for mediation. It does not state whether the Commissioner is to conduct the mediation or that the role be performed by an independent person. No formal requirements are set down for the mediation process.

The IC does not have an investigative or determination role in privacy complaints; only the provision of a mediation service to the parties. The guidelines on privacy complaints published by the IC provide little guidance and information for either complainants or agencies as to how complaints will be managed or the mediation process. This is in contrast to the external review guidelines under the RTI Act that provide detailed information for both parties.

Issues sometimes arise where this mediation process is not formalised: for example, there is no consistent 'preliminary enquiry' process undertaken as occurs in a RTI external review.

An alternative mechanism to mediation, and which might fit better with current practice, is conciliation. Conciliation is similar to mediation, in that it is negotiation and agreement making within a structured process, run by an impartial and unbiased third party professional, the conciliator. Conciliation however, has an element of advice that is not in the mediation process. The conciliator explains the law and processes, explore what may have occurred, points out strengths and weaknesses in each party's case, suggests options for settlement and assists the parties to understand each other's points of view. There is also the mechanism of a conciliation conference. The Act should provide more detail about the process once a matter is referred to the OIC, including whether mediation, conciliation or some other form of ADR is appropriate.

Other jurisdictions

Other jurisdictions such as the Commonwealth and Victoria contain specific provisions that deal with the conciliation process. The *Anti-Discrimination Act 1991* (**AD Act**) also provides for conciliation of complaints which forms part of the Anti-Discrimination Commissioner of Queensland (ADCQ) complaint handling model. It may be useful to look further at other

models and other forms of ADR to develop a better privacy complaints handling model, including the Ombudsman or the QCAT compulsory conference model.

Under the Victorian Act, the Commissioner must 'make all reasonable endeavours' to conciliate the complaint. There is a conciliation process via the Commissioner's staff. If agreement is reached, the Commissioner records the agreement for registration in VCAT. If no agreement is reached, either party can require referral to VCAT for hearing.

Under the Commonwealth Act, the Commissioner has a range of powers, including conducting preliminary inquiries, conciliation of complaints if the Commissioner considers conciliation may be successful. The Office of the Australian Information Commissioner (**OAIC**) has a Guide stating the factors to assist in determining if conciliation is likely to be successful. The Act does not provide any detail about how to conciliate but the same Guide provides some assistance. The Commissioner has power under the Act to direct attendance at a conciliation conference (refusal is an offence). If agreement is achieved at conciliation, a formal agreement is prepared. Otherwise, the Commissioner makes a section 52 determination to resolve the complaint.

In New South Wales, the Commissioner must endeavour to resolve the complaint by conciliation. There is a conciliation process (in section 49 of the NSW Act) which appears to have some compulsion element but procedures are determined by the Commissioner. In practice, it seems that attempts are made to achieve informal resolution providing sufficient time and flexibility to do so. If parties have no willingness to conciliate, the Commissioner may just proceed to deal with the matter under more general powers. If agreement is reached, the Commissioner makes a written report with recommendations.

In the Northern Territory, the Commissioner has quite broad powers of investigation, as part of which he or she can refer the complaint to mediation. The complaint must be referred to mediation if the investigation is complete and there is sufficient prima facie evidence to substantiate the complaint. Regardless of either, mediation is a prerequisite to the NT Civil and Administrative Tribunal (NTCAT) hearing. The Act (section 111) specifically sets out process for mediation (by the Commissioner or an agreed/appointed person). If mediation succeeds, the parties can apply for orders to give effect to the agreement. If not successful, either party can seek referral to NTCAT for hearing.

The AD Act provides for conciliation of discrimination complaints (Chapter 7, Part 1). The Commissioner may set a date for a conciliation conference which may form part of the Commissioner's general investigation process. The AD Act sets out a compulsory and formal conciliation process where the Commissioner considers the complaint may be resolved by conciliation. If resolution is achieved, the agreement is documented and filed with QCAT where it becomes an enforceable order. If no agreement is reached, the complainant can ask for referral to QCAT. If the Commissioner takes over 6 months to resolve complaint, either party can seek referral to QCAT.

Currently the Privacy complaints resolution function in Queensland is split between three bodies, namely:

- the agency investigates the initial complaint under the agency's usual complaints handling processes
- the Commissioner can conduct a mediation to resolve the complaint informally
- QCAT can ultimately arbitrate the complaint.

Having a complaints process that includes the opportunity for informal resolution before arbitration is supported. How those processes are organised and who undertakes the responsibilities may warrant further consideration. For example, both the informal resolution and arbitration functions could arguably be performed by QCAT.

QCAT has the processes that accommodate informal resolution followed by arbitration through the compulsory conference and hearing model. This would have the benefit of a one stop shop for complaints resolution. QCAT has established procedures and the infrastructure to deal with complaints.

This type of approach would remove the need to have the IC involved in the complaints process and free it to support agencies and the community in privacy advisory matters, without the risk of actual or perceived conflicts of interest arising. As it currently is structured, the IC is limited in its ability to provide formal privacy advice to government and complainants because it also may be the body who will be required to investigate. The IC has investigated only one agency formally and published a report on its investigation. This would not have been possible had the IC given that agency particular advice or if the agency was following the guidelines issued by the IC on the particular practice.

There is little data on current complaints resolution in the privacy sphere so before any changes are contemplated the data on timeliness and effectiveness of informal resolution and arbitration by QCAT would be worth reviewing.

28.3 Referring a privacy complaint to QCAT

The IP Act should provide more detail about the process for referring a complaint to QCAT, including:

- what is the timeframe for lodging the complaint e.g. 20 business days after confirmation from IC that the matter is not capable of resolution
- the scope of the complaint that can be lodged with QCAT (e.g. can it be broader that the complaint raised with the agency or the matters referred to the IC?)
- whether the complaint must be lodged by the IC or whether it can be lodged with QCAT directly by either or both of the parties
- the requirements for service, including time and method for service on the other party.

Section 112A of the Northern Territory *Information Act* may be of assistance in determining the process. That section provides:

> *112A (1) The complainant may apply to the Commissioner to refer a complaint to the Tribunal if:*

(a) the Commissioner decides under section 110(3) there is sufficient prima facie evidence to substantiate the matter complained of and that matter is not resolved by mediation or other agreement; or

(b) the Commissioner dismisses the complaint under section 110(5).

(2) The respondent may apply to the Commissioner to refer a complaint to the Tribunal if the Commissioner decides under section 110(3) there is sufficient prima facie evidence to substantiate the matter complained of and that matter is not resolved by mediation or other agreement.

(3) For subsections (1)(a) and (2), the application must be made within 28 days after the applicant has been given both of the following:

(a) notification under section 110(6) of the Commissioner's decision under section 110(3) that there is sufficient prima facie evidence to substantiate the matter complained of;

(b) a mediator's certificate under section 111(4) in relation to the matter complained of.

(4) For subsection (1)(b), the application must be made within 28 days after the complainant has been given notification under section 110(6) of the Commissioner's decision to dismiss the complaint.

(5) If the Commissioner receives an application under this section, the Commissioner must:

(a) refer the complaint to the Tribunal; and

(b) inform the Tribunal whether or not there has been an attempt to resolve the matter complained of by mediation.

29. Should there be a time limit on when privacy complaints can be referred to QCAT?

Yes – see discussion above.

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

Part 6 of Chapter 4 of the IP Act deals with compliance notices. Consideration should be given to whether the mechanism of compliance notices is appropriate for dealing with government compliance with the IP Act.

The IP Act gives the IC power to issue compliance notices to government agencies and to prosecute agencies if they fail to take all reasonable steps to comply with the notice (100 penalty points). The definition of agency includes department, Minister, local government and public authority. As far as this department is aware, no compliance notices have been issued since the commencement of the IP Act in 2009.

There is a question as to whether or not the IC should have the power to issue compliance notices against departments and Ministers. This power to sanction and to prosecute exceeds the powers of the IC in relation to RTI and the Ombudsman in relation to investigating administrative actions.

Specifically, the circumstance in which the IC may give a compliance notice is where the commissioner is satisfied that the agency:

- has done an act or engaged in a practice in contravention of the agency's obligation to comply with the privacy principles; and the act or practice:
  - is a serious or flagrant contravention of the obligation; or
  - is of a kind that has been done or engaged in by the agency on at least 5 separate occasions within the last 2 years.
- A compliance notice may require an agency to take stated action within a stated period for the purpose of ensuring compliance with the obligation.

An agency may apply to QCAT for a review of the IC's decision to give a compliance notice.

It might be more appropriate for the IC to assist government to comply with the requirements of the Act by making recommendations to agencies about compliance rather than to exercise powers of sanction. The compliance notice model is one that is most useful when government is performing regulatory functions, particularly in respect of the private sector. The IP Act does not apply to the private sector other than by the mechanism of being a bound contracted service provider. Compliance notices cannot be issued to contracted service providers.

Government agencies are required to abide by the law and if an agency was inclined to ignore an IC recommendation then the IC can use his or her power to report to Parliament. This model of working with government to achieve compliance is one which has worked well for the Ombudsman over the years. The types of investigations undertaken by the Ombudsman into administrative actions and processes are not dissimilar to the personal information handling practices that concern the IC.

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

The privacy principles in the IP Act will not apply to a document that is a 'generally available publication' (see section 16 and schedule 1, section 7).

A '*generally available publication*' is defined in the Dictionary of the IP Act as *a publication that is, or is to be made, generally available to the public, however it is published*.

Unlike other Australian jurisdictions, the IP Act also defines '*publication*' as *including a book, magazine or newspaper*. It is an inclusive definition. However, it appears to suggest (e.g. on statutory interpretation principles) that electronic formats (e.g. posts, blogs, emails) are not 'publications'. This conflicts with the above definition of 'generally available publication' (which

incorporates the words 'however it is published') and fails to recognise the digital environment in which we operate.

In the agency/organisational context, if there is a social media website that enables members of the public to engage with the agency without needing a password or any other restriction, any personal information posted on the site by the individual, inadvertently or otherwise, is part of a generally available publication and the IP Act protections would not apply.

Arguably, if a person posting/uploading information places controls on who may access that information on their Facebook page or social media site, the Facebook page or social media site is not a 'generally available publication' for the reasons outlined below.

Various court and tribunal decisions in the employment/unfair dismissal context have taken the view that Facebook posts are not 'private' communications, and that users of Facebook are (or should be) aware that the contents of their posts etc. can be communicated to persons beyond the 'friends' permitted by a user's privacy settings to access the comments.[96] Facebook posts have a permanence and potential audience that casual conversations at a work water cooler or after hours social drinks do not.[97]

It would appear that information on social media is 'published… by the individual' and section 28 IP Act would apply (excluding the operation of IPPs 8-11 in relation to information that is related to or connected with that information). However, this is a different issue to whether comments on social media such as Facebook are a 'generally available publication'. In the latter case, the IP Act does not apply at all to that information.

Certainly there are many social media pages which would fall within this definition, e.g. the Department's Facebook page which invites comments from the public and has no privacy settings or access restrictions.

However, personal Facebook or other social media pages, while accessible to a number of people, even people other than those permitted by the person publishing the comments, do not seem to have the nature of a 'generally available publication' in the sense of anyone being able to immediately/readily/easily access the data without overcoming some restriction or hurdle. It is similar to online journals requiring a subscription to be able to access.

Therefore, it is arguable that most social media sites where individuals can (and do, at some level) restrict access would not constitute 'generally available publications' and the IP Act privacy principles would not be excluded on that basis.

However, consideration should be given to whether information that is published on these sites should be afforded privacy protections. Arguably, there should be no strong expectation of privacy

---

96 See, for example, *Senior v Police* [2013] NZFLR 356 (High Court) at [6]; *Linfox Australia Pty Ltd v Stutsel* [2012] FWAFB 7097, [25], [26].

97 *Hook v Stream Group (NZ) Pty Limited* [2013] NZEmpC 188, [31].

in relation to such information. Consideration could be given to an approach that provides that information which is published by way of social media or internet generally does acquire privacy protections.

In response to whether the Commonwealth definition would be a more useful model, it does go further to make clear that a generally available publication would include publication for which a fee would be charged, such as public registers. However, it would still seem to exclude internet publication on social media sites because the class of document in the genus is book, article or newspaper.

Consideration might be given to amending the list of documents to which the privacy principles do not apply, in Schedule 1, Section 7 of the IP Act to include *(e) published on social media or otherwise on the internet.*

32. 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?

The Department supports the amendment of IPP4 to insert a requirement to 'take all reasonable steps'. Amendment of IPP4 to align with all IPPs would allow consistency across the IPPs and so be in the best interests for clear and consistent law.

In section 4.6 table:

IPP 4 –

- replace 'must ensure that' with 'take reasonable steps to'
- IPP 4(2) – should be clarified – the level of security should be commensurate to the sensitivity of the information.

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

The department strongly supports maintaining the words **'asked for'** for the purposes of IPP2 and 3.

The general meaning of the term 'ask for' is to solicit or request. The term 'collect' means to gather, hold or accumulate information, whether it is asked for or not and so it could include solicited and unsolicited information.

The obligations in IPPs 2 and 3 to information that is collected by an agency should not be widened to 'collection'. If the IP Act was amended in that way, agencies would incur collection obligations in relation to unsolicited personal information which was not asked for and is not relevant or necessary for following up the complaint/query.

For example, where people send a letter to the Director-General in order to lodge a complaint or raise a query, providing irrelevant background information about themselves, people they know and others they perceive to be involved. This collection, while unsolicited,

would make the IPPs applicable and so could require the department to issue a collection notice to the letter writer as well as those people mentioned by the letter writer.

The concern is that the outcome flowing from this example would be unmanageable. A person has volunteered the information and even if completely irrelevant to an enquiry, then the agency must issue a collection notice. A reasonable person would not expect to receive a collection notice where an agency has not sought information from them and they have provided information freely, nor would a reasonable third party expect to receive notice that their information has been collected by the government where they have been mentioned in an unsolicited letter.

Widening of the application of IPPs 2 and 3 to collection would subsequently also increase the administrative burden for agencies in needing to determine collection scenarios and in needing to respond to an increased number of collection notices under IPP2 as a result of receipt of a large amount of unsolicited information.

34. Are there other ways in which the RTI Act or the IP Act should be amended?

Suggested amendments:

- Move the access and amendment rights currently in the IP Act to the RTI Act to reduce red tape and assist applicants submitting applications by having a single entry point.
- Confine the IP Act to personal information handling obligations and complaints handling.
- Expand the objects of the RTI Act to better reflect how the push model balances competing essential public interests that are protected in the Act, such as privacy, privileged information and third party commercial information.
- Section 21(3)(b) (Meaning of public authority): there appears to be an error *"an office or member of a body"*
- IPP 11(1)(a) should be redrafted to remove the limitations and to create greater certainty for agencies and the community by omitting '*under IPP2 or under a policy or other arrangements in operation before the commencement of the schedule*'.

Data breach notifications

Is the suggested amendment to the *Privacy Act 1988* (Cth) – mandatory notification of breaches and definition of eligible data breach a further requirement than what the Queensland regime has now – albeit informally – and what issues might arise from putting it into legislation?

This paper firstly provides a summary of whether a legislative mandatory notification scheme such as that being introduced into the *Privacy Act 1988* (Cth) by the Serious Data Breach Notification Bill 2016 would be preferable to the existing voluntary notification requirements covered by the Office of the Information Commissioner's (**OIC**) guideline.

The remainder of the paper discusses:

- the OIC's guideline
- the main features of the Commonwealth Serious Data Breach Notification Bill 2016 and observations on the Bill
- submissions to the earlier 2015 Privacy Amendment (Notification of Serious Breaches) Bill 2015 by the OIC and the Australian Office of the Information Commissioner (**OAIC**).

Overview: Advantages and disadvantages of a mandatory legislative notification scheme

There is some uncertainty whether mandatory legislative requirements for notification of data breaches, similar to the Commonwealth's Serious Data Breach Notification Bill 2016, for Queensland government is preferable to the existing voluntary notification requirements covered by the Queensland Office of the Information Commissioner's (OIC) *Privacy breach management and notification guideline* (and similar guidelines issued by the OAIC).

Some of the considerations are:

- The *Information Privacy Act 2009* (**IP Act**) does not specifically require Queensland Government agencies to notify affected individuals or the Information Commissioner (**IC**) of a privacy breach.
- In its submission to the Serious Data Breach Notification Consultation Bill, the OIC expressed in principle support for a mandatory legislative scheme because it strengthens existing regulatory framework and brings Australia into line with other countries such as the UK, USA and the EU.[98]
- Under the current voluntary or self-regulatory model under the OIC and OAIC guidelines, entities that tell their customers about a serious data breach may suffer damage to reputation and/or financial and other impacts in contrast to agencies that choose not to tell. A statutory mandatory notification scheme puts all agencies on the same footing.[99]

---

98 Queensland Office of the Information Commissioner *Submission to the Serious Data Breach Notification Consultation Bill*, March 2016

99 Office of the Australian Information Commissioner, Submission to the Attorney-General's Department on the *Discussion paper – Mandatory data breach notification* (Discussion Paper), 3 March 2016.

- It has been envisaged that the Australian Commissioner will issue guidelines to complement the new 2016 Bill so there remains room for similar guidelines to be made by the OIC for any Queensland legislation.
- Mandating notification by statute provides an important transparency measure for government agencies with which the community entrusts their personal information.[100]
- Mandating notification by statute may provide citizens with the assurance that the government regards the protection of personal information as sufficiently important to enshrine in legislation.[101]
- Changes to the enforcement provisions in the *Privacy Act 1988* under the 2016 Bill gives legislative authority for the Australian Privacy Commissioner to:
  - direct an agency or business to notify individuals about a serious data breach, and
  - investigate breaches and to require remedial action.[102]
- The Commonwealth 2016 Bill has a statutory threshold to trigger the notification requirements but the OIC guidelines do not directly establish a threshold. Under the Bill, notification is required where there has been an 'eligible data breach' which occurs where the access, disclosure or loss is likely to result in serious harm to any individual to whom the information relates. A list of factors assists in making a decision about likelihood of serious harm. These factors appear to reflect those set out in the OIC guidelines and the Australian OIC guidelines regarding factors to consider to decide if notification is appropriate.

  The explanatory memorandum for the 2016 Bill states '*It is not intended that every data breach be subject to a notification requirement. It would not be appropriate for minor breaches to be notified because of the administrative burden that may place on entities, the risk of 'notification fatigue' on … individuals, and the lack of utility where notification does not facilitate harm mitigation.'*

  On the other hand, a lower statutory threshold might mean that entities will be less likely to notify – even after having regard to the listed statutory factors. The OIC guidelines appear to adopt a more flexible approach, adopting a holistic assessment of all the circumstances.

  However, the concern that the statutory threshold is set too high could be rectified by redrafting the notification triggers. The provisions could state that once there has been a breach, the entity must have regard to a number of (non-exhaustive) statutory factors to determine whether notification is appropriate in all the circumstances.

---

100 Queensland Office of the Information Commissioner *Submission to the Serious Data Breach Notification Consultation Bill*, March 2016; Office of the Australian Information Commissioner, Submission to the Attorney-General's Department on the *Discussion paper – Mandatory data breach notification* (Discussion Paper), 3 March 2016.

101 Queensland Office of the Information Commissioner *Submission to the Serious Data Breach Notification Consultation Bill*, March 2016.

102 Office of the Australian Information Commissioner, Submission to the Attorney-General's Department on the *Discussion paper – Mandatory data breach notification* (Discussion Paper), 3 March 2016.

The above approach overcomes beginning with the question of whether the breach is *likely to result in serious harm* (having regard to the statutory factors) which might unconsciously cause entities to adopt a stricter approach.

- There is some concern that the new laws may open the way to class actions against entities that suffer eligible data breaches on the basis that notification can look like admission of liability. However, even in the USA, which has the greatest incidence of class action litigation, only a small percentage of notified data security breaches lead to class actions.[103]

Current Queensland Notification Scheme

Under the IP Act, Information Privacy Principle (**IPP**) 4 requires agencies to ensure that they apply appropriate protections to the personal information they control.[104]

> *(1) An agency having control of a document containing personal information must ensure that—*
>
> *(a) the document is protected against—*
>
> *(i) loss; and*
>
> *(ii) unauthorised access, use, modification or disclosure; and*
>
> *(iii) any other misuse; and*
>
> *(b) if it is necessary for the document to be given to a person in connection with the provision of a service to the agency, the agency takes all reasonable steps to prevent unauthorised use or disclosure of the personal information by the person.*
>
> *(2) Protection under subsection (1) must include the security safeguards adequate to provide the level of protection that can reasonably be expected to be provided.*[105]

The OIC considers that a 'security safeguard' contemplated under IPP 4(2) is to notify any individuals if their personal information becomes the subject of the breach. Indeed, one of the objects of the IP Act is to provide for the fair handling of personal information. [106]

The IP Act does not specifically require Queensland Government agencies to notify affected individuals or the IC of a privacy breach. However, the information security incident

---

103 Charles Davies and Nick Valentine, 'Australia's Data Breach Bill – third time lucky?', King & Wood Mallesons Insights, 19 October 2016

104 Queensland Office of the Information Commissioner (OIC), 'Protection and Security of Information', *Guidelines for Government,* 19 July 2013.

105 The Queensland Information Commissioner considers that agencies should refer to relevant legislation, whole of government standards, regulations and policies that relate to information security, such as Information Standard 18 – Information Security (IS18)Queensland Office of the Information Commissioner, 'Protection and Security of Information', *Guidelines for Government,* 19 July 2013.

106 Queensland OIC, 'Protection and Security of Information', *Guidelines for Government,* 19 July 2013.

reporting requirements under Information Standard 18 does contain obligations for agencies to report incidents to the Queensland Government Chief Information Officer.[107]

Despite the lack of mandatory obligations in the IP Act, the OIC encourages agencies to have data breach notification as part of its business practices. It also encourages communications with the Privacy Commissioner when data breaches occur for guidance about how to manage the breach, including whether or not to notify the affected individual.[108]

In general, if a data breach creates a risk of harm to an individual, the affected individuals should be notified. However, there are times where notification can be counter-productive.[109]

The Privacy Commissioner also has a *Privacy breach management and notification guideline* to assist agencies.

Queensland OIC's Guideline

The Queensland OIC's *Privacy breach management and notification guideline* seeks to assist agencies in managing a privacy breach, including about whether notification if appropriate.

The guideline states that there are four main steps in responding to a privacy breach, the first three of which should be carried out concurrently if possible. The following provides a summary of the requisite actions:[110]

1. *Contain the breach*

   The agency should take necessary possible steps to contain the breach and minimise damage – retrieve the personal information including any copies (which may involve legal action if a third party will not return it), close down the system which has been breached, suspend the activity causing the breach, change passwords or codes.

   It will usually be necessary to internally report the breach to senior management and the privacy contact officer should be told of all breaches.[111]

2. *Evaluate the associated risks*

   Further steps may be required so the situation must be assessed in terms of the personal information involved in the breach and the consequent risks. The factors to consider include:

---

107 Queensland OIC, *Submission to the Serious Data Breach Notification Consultation Bill*, January 2016, p 3.

108 Queensland OIC, *Submission to the Serious Data Breach Notification Consultation Bill*, January 2016, p 3.

109 Queensland OIC, 'Once more into the breach' *OIC News*, 8 April 2015.

110 Queensland OIC, *Privacy breach management and notification guideline*, 10 March 2015.

111 In other cases, telling other units such as legal services, ethical standards, media relations might be appropriate.

- nature of the personal information – does it involve tax file or Medicare numbers, health information, credit or debit card numbers the unauthorised disclosure of which may be worse than disclosing a name on a newsletter subscription list?
- who is affected by the breach and do any individuals affected have personal circumstances that may accentuate the risk of harm?
- what caused the breach? Was it an inadvertent oversight or a targeted attack? Has the personal information been recovered and/or the breach contained?
- what may be the harm to the individuals concerned?[112]

3. *Consider notifying affected individuals*

While there is no obligation to do so under the IP Act, failing to notify could worsen the damage (e.g. if credit card needs to be cancelled) or adversely affect the agency's reputation.

Factors to consider when deciding whether to notify the individual affected by the data breach:

- The potential for reasonably foreseeable harm to result from the breach for the persons whose information is involved ('data subjects') or otherwise affected, having regarding to the nature of the information, in particular its sensitivity, the amount of information, the extent of the unauthorised access, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, especially in mass media or online, and any relationship between the recipient(s) and the data subjects.
- The extent to which the data subjects may already be aware of the breach of their information privacy and be able themselves to minimise the harm.
- The potential for notification itself to cause reasonably foreseeable harm to the data subjects (or any other person).
- Whether, considering the points above, notification is reasonably likely to alleviate more harm than it would cause. [113]

An example where notification many not be warranted is given in the guideline. An agency officer takes home a memory stick containing personal information (names, email addresses and the correspondence) of 100 members of the public who are involved in community consultation being conducted by the agency. However, the data is protected by encryption and is not able to be accessed without the relevant decryption key.

4. *Prevent a repeat*

---

[112] Could there be identity theft, threats to safety, financial loss, workplace bullying, damage to reputation, humiliation etc. The impact/effect may depend on who is the recipient of the information and/or risk of further disclosure.

[113] Queensland OIC, 'Protection and Security of Information', *Guidelines for Government*.

Commonwealth Serious Data Breach Notification Bill 2016 (Cth)

The Serious Data Breach Notification Bill 2016 (Cth) is currently awaiting royal assent, having passed the House of Representatives on 7 February 2017 and the Senate on 13 February 2017.

The 2016 Bill implements a Government commitment in response to the Parliamentary Joint Committee on Intelligence and Security's February 2015 Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015.

In its 2008 review of privacy, the Australian Law Reform Commission (**ALRC**) recommended the introduction of a mandatory data breach notification scheme. This prompted the Australian Privacy Commissioner to set up a voluntary data breach notification scheme and publish guidance material about data breach notification practices. However, the Commissioner has had continued concern that data breaches are underreported.[114]

The Commissioner has said that he suspects that many Australian entities do not voluntarily report all serious data breaches or recognise which incidents they should report: '*Data breaches regularly come to my attention through the media and allegations from third parties*'.[115]

The 2016 Bill draws on the ALRC's recommendation and practical experience gained from the commissioner's voluntary scheme and guidance.[116] It also takes into account submissions received in response to consultation on the Commonwealth Government's *Exposure draft Privacy Amendment (Notification of Serious Data Breaches) Bill 2015.*

Framework of the Serious Data Breach Notification Bill 2016 (Cth)

The Bill inserts a proposed new Part IIIC into the *Privacy Act 1988* to establish a scheme for notification of eligible data breaches.

The *Explanatory Memorandum* for the Bill notes that:

> It is not intended that every data breach be subject to a notification requirement. It would not be appropriate for minor breaches to be notified because of the administrative burden that may place on entities, the risk of 'notification fatigue' on the part of individuals, and the lack of utility where notification does not facilitate harm mitigation.117

---

114 Hon M Keenan MP, Minister for Justice and Minister Assisting the Prime Minister for Counter-Terrorism, Second Reading Speech, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth), *House of Representatives, Hansard*, 19 October 2016, p 2430.

115 Office of the Australian Information Commissioner, Submission to the Attorney-General's Department on the *Discussion paper – Mandatory data breach notification* (Discussion Paper), 3 March 2016.

116 In 2013, the then Labour government introduced a bill to strengthen the voluntary data breach notification framework implementing the ALRC recommendation in this regard. However, while it passed the House of Representatives, it lapsed on prorogation of Parliament before it could pass the Senate.

117 Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth), *Explanatory Memorandum*, para 11.

When introducing the Bill into the House, the Minister, the Hon M Keenan MP, said:

> The rationale for mandatory data breach notification is that, if an individual is at likely risk of serious harm because of a data breach involving their personal information, receiving notification of the breach can allow that person to take action to protect themselves from that harm. For example, an affected individual might change an online password or cancel a credit card after receiving notification that their personal information has been compromised in a data breach.[118]

What entities are covered by the Bill?

An agency or organisation regulated by the Privacy Act[119] must provide notice to the Australian Information Commissioner (the Commissioner) and affected individuals if:

> (a) it has reasonable grounds to believe that an eligible data breach has happened; or
>
> (b) it is directed to do so by the Commissioner.

Where an entity discloses information to an overseas recipient and APP 8 applies under the proposed section 26WC, the entity retains responsibility for any serious data breach involving the personal information as if the breaches happened to the entity.

What is an 'eligible data breach'?

- An '*eligible data breach*' arises where (see section 26WE):
  - (a) in relation to personal information[120] about one or more individuals (the affected individuals), or where such information is lost in circumstances that are likely to give rise to unauthorised access or unauthorised disclosure
  - (b) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and
  - (c) a reasonable person would conclude the **access, disclosure or loss is likely to result in serious harm to any of the individuals** to whom the information relates (my bolding).

The *Explanatory Memorandum* to the 2016 Bill observes that *serious harm*, in this context, could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach.[121]

---

118 Hon M Keenan MP, Minister for Justice and Minister Assisting the Prime Minister for Counter-Terrorism, Second Reading Speech, Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth), *House of Representatives, Hansard*, 19 October 2016, p 2430.

119 The Bill contains general rules for the majority of entities regulated by the Privacy Act as well as analogous rules for credit reporting bodies and credit providers that are subject to specific regulation under Part IIIA. The provisions also apply to recipients of tax file number information.

120 The requirements apply also to credit reporting information, credit eligibility information or tax file number information held by the relevant entity.

121 Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth), *Explanatory Memorandum*, para 9.

Further, the reasonable person would also need to be satisfied that the risk of serious harm occurring is *likely*, that is, more probable than not.

Factors to consider in deciding likely or not likely to result in serious harm

To determine whether a reasonable person would conclude that an access to, or a disclosure of information would be likely or not likely to result in serious harm, agencies must have regard to a list of 'relevant matters' in section 26WG:

- the kind/s and the sensitivity of the information
- whether the information is protected by one or more security measures and the likelihood that any of those security measures could be overcome (e.g. use of an encryption key)
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information
- if a security technology or methodology
  - was used in relation to the information
  - was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information

  the likelihood that the persons, or the kinds of persons, who
  - have obtained, or who could obtain, the information
  - have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates

  have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology[122]
- the nature of the harm, and
- any other relevant matters.

Exception to when eligible data breach – remedial action

An unauthorised access or disclosure will not be an 'eligible data breach' where, as a result of remedial action taken by the entity *before* it results in serious harm to any individual, a reasonable person would conclude that the unauthorised access or disclosure is unlikely to result in serious harm to any of the individuals (section 26WF).[123]

Assessment

- Where an entity has reasonable grounds to suspect that there may have been an eligible data breach but is not aware there are reasonable grounds to believe the breach has occurred, the entity must undertake a reasonable and expeditious (i.e. completed within 30 days of becoming aware) assessment of whether there are reasonable grounds to believe the circumstances amount to an eligible data breach (see section 26WH).

---

122 The note to this section states that if the security technology or methodology is encryption, an encryption key is an example of 'information required to circumvent…'

123 Similar exceptions apply where there is a loss of information. Under section 26WD an exemption applies to e-Health information if the breach is required to be notified under the mandatary notification requirements of the *My Health Records Act 2012*.

The inclusion of section 26WH which had not appeared previously allows an entity, which may have reasonable grounds to suspect a breach but not enough to be certain, to undertake an assessment before needing to notify. Some submitters had expressed concern about the burden of deciding if a breach had to be notified and this provision gives entities time to assess the situation.[124]

Notification

- If the assessment results in the entity being aware there are reasonable grounds to suspect that there may have been an eligible data breach, the entity must prepare a statement setting out:
  - the breach that has happened
  - the information involved
  - the recommendations affected individuals should take in response, and
  - the contact details of the entity

  A copy is sent to the Commissioner (sections 26WK and 26WL).
- If practicable, the entity must take such steps as are reasonable to notify contents of the statement to each individual to whom the information relates and/or who are at risk from the breach. If not practicable, then the entity shall publicise the statement on the website etc. (section 26WL).
- Notification is required unless an exception applies. The Commissioner can direct an entity to notify.[125]

Exceptions to notification

- Notification requirements do not apply to an enforcement body if to notify would be likely to prejudice enforcement activities (section 26WN).
- Notification requirements do not apply if to do so is inconsistent with a secrecy provision of a law of the Commonwealth (section 26WP).
- An entity can apply to the Commissioner for an exception from the notification requirement, either permanently or for a specific period. The Commissioner can also act on his or her own initiative. The declaration of an exception can only be made if the Commissioner is satisfied it is reasonable in the circumstances to do so, having regard to the public interest or advice from an enforcement body or the Australian Signals Directorate, or other relevant matters (section 26WQ).

Enforcement framework

- The Commissioner can investigate possible noncompliance with the mandatory data breach notification scheme, and, after providing the entity with a chance to make a

---

124 M Neilson, Australian Parliamentary Library, 'Privacy Amendment (Notifiable Data Breaches) Bill 2016', *Bills Digest No. 52*, 8 December 2016, p 12.

125 Where more than one entity holds the same records, if one entity notifies the individuals of the breach the other entities holding the same records are not required to notify.

submission, may make a determination requiring the entity to notify in accordance with the requirements ((section 26WR).[126]

- The Bill seeks to amend section 13 of the *Privacy Act 1988* so that a failure to comply with notification obligations will be deemed an 'interference with the privacy of an individual' triggering the Commissioner's powers of investigation and remedial action. The Commissioner can make determinations, and seek enforceable undertakings.
- In the case of serious or repeated noncompliance, the Commissioner can apply to a court for a civil penalty.
- The Administrative Appeals Tribunal has power to review decision of the Information Commissioner about declaring a notification exemption or giving a direction to notify a breach (amended section 96).

Observations on the 2016 Commonwealth Bill

Some commentators argue that the 2016 Bill takes a more cautious approach than the 2015 Exposure Draft of the Serious Data Breach Notification Consultation Bill and the earlier 2013 Bill, as follows:

- The 2016 Bill adopts a higher threshold test for deciding if there is an 'eligible data breach'[127]

The notification threshold in the 2015 Exposure Draft Bill was to notify where there was a '*real risk of serious harm*'.

The 2016 Bill requires breach notification where a reasonable person would conclude that the access, disclosure or loss would *be likely to result in serious harm*. It is arguable that this is a higher threshold than 'real risk of serious harm', particularly when combined with the list of factors in section 26WG. Various submissions to the 2015 consultation bill said that even though 'real risk' was explained to mean 'risk that is not a remote risk', this still was too vague.[128]

The test of 'real risk serious harm' could lead to entities taking a narrow interpretation resulting in difficulty in identifying all the individuals who may be at risk of serious harm, issues of 'notification fatigue' and 'over notification' and individuals being informed even when they cannot take any steps to mitigate their risks. [129]

---

126 An exception applies if likely to compromise enforcement related activity of an enforcement body or inconsistent with a secrecy provision.

127 There is also an issue created by allowing entities to avoid having to notify if they take remedial action before any serious harm has occurred: M Neilson, Australian Parliamentary Library, 'Privacy Amendment (Notifiable Data Breaches) Bill 2016', *Bills Digest No. 52*, 8 December 2016, p 15.

128 M Neilson, Australian Parliamentary Library, 'Privacy Amendment (Notifiable Data Breaches) Bill 2016', *Bills Digest No. 52*, 8 December 2016, pp 10-11, citing Australian Bankers' Association, *Submission to the AGD Inquiry into mandatory data breach notification exposure draft*, p 4.

129 M Neilson, Australian Parliamentary Library, 'Privacy Amendment (Notifiable Data Breaches) Bill 2016', *Bills Digest No. 52*, 8 December 2016, pp 10-11, citing Australian Bankers' Association, *Submission to the AGD Inquiry into mandatory data breach notification exposure draft*, p 4.

The test of *likely to result in serious harm* seems to impose a higher threshold and might result in fewer notifications of breach. It appears that the different threshold was to provide more certainty for entities who need to decide when to notify a data breach. It may also meet with more favour to some businesses who may find it less burdensome to comply with by requiring fewer notifications.[130]

The Australian Privacy Commissioner appeared to approve of the 2015 consultation draft Bill providing entities with the autonomy to make their own reasonable assessment of whether a data breach is serious.[131] It may be that the Commissioner takes the same view towards the 2016 Bill given it still allows autonomy despite the Bill's higher threshold for notification.

A number of business groups (e.g. Australian Industry Group, Digital Industry Group Inc which includes Google, Twitter, Facebook, Microsoft etc) believe the voluntary notification scheme already in place is effective.[132]

Queensland Office the Information Commissioner's Submission to the Serious Data Breach Notification Consultation Bill

The Queensland OIC provided a submission to the Serious Data Breach Notification Consultation Bill which made the following points:[133]

- the OIC, in principle, supports the introduction of a legislative mandatory breach notification scheme
- a mandatory scheme strengthens existing regulatory framework and brings Australia into line with other countries such as the UK, USA and the EU
- there is no requirement under the IP Act for notification of affected individuals or the Information Commissioner of a privacy breach but there are notification obligations as part of incident reporting under IS18
- the OIC encourages data breach notification by agencies and has issued guidelines to assist (as discussed earlier)
- introduction of a legislative mandatory breach notification scheme:
    - allows affected individuals to take remedial action to lessen adverse impacts such as financial loss or identity theft
    - provides an important transparency measure for agencies with which the community entrusts their personal information. Breaches, especially concerning electronically stored information, reduces citizens' confidence and trust in government

---

130 M Neilson, Australian Parliamentary Library, 'Privacy Amendment (Notifiable Data Breaches) Bill 2016', *Bills Digest No. 52*, 8 December 2016, p 11.

131 Office of the Australian Information Commissioner, Submission to the Attorney-General's Department on the *Discussion paper – Mandatory data breach notification* (Discussion Paper), 3 March 2016.

132 'Data breach notification bill receives bipartisan backing', *Computerworld*, 7 February 2017.

133 Queensland Office of the Information Commissioner *Submission to the Serious Data Breach Notification Consultation Bill*, March 2016.

  - increases citizens' confidence that they will be made aware if there is a breach of their personal information because doing so is mandatory and this also reassures them that government sees that the protection of personal information is important
- because data breaches can have significant costs for agencies, mandatory notification may encourage agencies to improve their data handling and security practices
- if the threshold for notification is set too high, it may mean only the most egregious of breaches are notified because of the financial and reputational costs for agencies once a breach becomes public through the agency having notified. However, if set too low, it may increase the regulatory burden on agencies and may even worsen the impact of the breach
- the OIC supports the exceptions to notification, stating that they were limited and provided flexibility.
- to date, only a small number of Queensland agencies and their contracted service providers have reported data breach notifications to the OIC. One possible explanation for the relatively low number is that data breach is a relatively rare occurrence in Queensland. However, as noted by the OIC, the absence of reliable data and lack of mandatory legislative notification obligation makes it difficult to state with certainty the actual number of breaches in Queensland.

Notifications of data breaches to the Office of the Information Commissioner

- If it was considered desirable to legislate for notification of privacy breaches in Queensland the threshold suggested by the Commonwealth would appear to mirror the current practice in Queensland. However, it is considered unnecessary to require agencies to notify the OIC in each case that a decision is made to notify individuals of a breach. The breach may be easily and quickly resolved between the agency and the individual to the individual's satisfaction with no further action being necessary. Arguably, it would not be necessary to also notify the OIC in such circumstances and would be administratively burdensome with little benefit for the community. It is recognised however that there will be situations where the OIC should be notified about a data breach, such as where the breach is significant and impacts on a high number of individuals (e.g. the recently reported 2013-14 Yahoo breaches). The OIC could issue guidelines to assist agencies determine the types of breaches which would warrant OIC notification.