

Submission to the Department of Justice and Attorney-General

2016 Consultation on the Review of the *Right to Information Act 2009* and *Information Privacy Act 2009*

February 2017

Introductory Overview

The Office of the Information Commissioner's (OIC) statutory functions under *the Right to Information Act 2009* (RTI Act) and *the Information Privacy Act 2009* (IP Act) include assisting in achieving the goal of open and transparent government by promoting better and easier access to public sector information and improving the flow of information to the community balanced with appropriate protections for certain information, including personal information. Through its functions, OIC supports the public sector's corporate governance and accountability framework.

There is increasing recognition in democratic countries across the world of the benefits of openness, transparency and accountability. Greater openness and transparency delivers a range of tangible benefits including greater public engagement, improved service delivery and restoring trust and confidence in government. As noted by the OECD, trust in institutions including government continues to decline and only 40% of citizens trust their government.¹

Queensland's RTI Act recognises that government-held information is a public resource and that openness in government enhances accountability. The RTI Act represents a clear move from a 'pull model' to a 'push model', emphasising proactive and routine release of information and maximum disclosure of information unless to do so would be contrary to the public interest. The RTI Act states that a formal application for government-held information under the RTI or IP Act should only be made as a last resort. Federal, State and Territory governments have their own Freedom of Information or RTI legislation.

At a national level, the Australian Government has committed to membership of the Open Government Partnership (OGP) and public consultation was undertaken to develop Australia's first National Action Plan. The OGP is a voluntary, multi-stakeholder international initiative created to promote transparency.

OIC supports strategies and initiatives, such as Open Data, that maximise disclosure of government-held information to the community and provide appropriate protections for the community's personal information. Release of datasets under open government data initiatives is one mechanism for increasing transparency and accountability of government.

The RTI Act and the IP Act provide a strong foundation for Queensland public sector agencies to adopt a 'push model' approach in conducting their activities. Since commencement of the legislation in July 2009, the Office of the Information Commissioner (OIC) has observed considerable progress in movement to a presumption of pro-disclosure and, importantly, proactive disclosure by

¹ <http://www.oecd.org/governance/trust-in-government.htm>

agencies. This has increased the flow of information to the community as part of how agencies routinely operate and is also evident in the findings of OIC's performance monitoring activities. To ensure this is maintained, it is important that any proposed changes to the RTI Act support this pro-disclosure bias.

It is OIC's view that a number of the issues raised in the 2016 *Consultation on the Review of the Right to Information Act 2009 and Information Privacy Act 2009* (Consultation Paper), such as the operation of the public interest balancing test and current exemptions and exclusions lie at the core of the RTI Act and are inextricably linked to the operation of a number of other provisions in the RTI Act. As such, these issues require proper community consultation. The community will expect to be more fully consulted about any proposed amendments to the RTI Act that have the potential to re-frame the objects and intent of RTI in Queensland and in particular expand the type of information or type of entity or function of an entity exempted from the coverage of the legislation.

OIC notes that the Consultation Paper includes a number of references to the consultation on the review of the RTI and IP Act commenced by the former Government in 2013. Given submissions made to the 2013 consultation were not made publically available and a significant period of time has elapsed since 2013, OIC considers that it is difficult for all stakeholders and the wider community to provide an informed response to a number of questions. For example, a number of issues and perceived difficulties raised during the 2013 consultation process are no longer of relevance as agreed outcomes and determinations have settled processes and clarified application of the RTI Act.

OIC notes that the amount of data being generated, collected and stored has been growing exponentially. It has been estimated that 90% of the data in the world today has been created in the last two years alone.² 'This data comes from everywhere: sensors used to gather climate information, posts to social media sites, digital pictures and videos, and cell phone GPS signals'.³ The challenges posed for privacy and the protection of personal information by the rapid pace of technological change are not unique to the Queensland jurisdiction. OIC notes there is increasing community awareness of privacy issues and concerns as highlighted by the community response to perceived privacy risks arising out of Census 2016 and the decision to keep and use name and address information for data-linking.

As recently noted by the NSW Standing Committee on Law and Justice following an inquiry into remedies into serious invasions of privacy, there remain significant gaps in the coverage afforded to

² <https://www-01.ibm.com/software/au/data/bigdata/>

³ See above

privacy and data protection. OIC notes that a number of jurisdictions have sought to enact legislation to facilitate government's transition to a digital economy.

OIC considers that the review provides an opportunity to modernise Queensland's privacy laws to provide a contemporary legislative framework to manage new and emerging privacy and data protection risks in the face of rapid technological change. The challenges of artificial intelligence and automation as well as international developments such as the adoption of the General Data Protection Regulation in Europe will also place pressure on the Australian and Queensland jurisdictions if a more comprehensive review of the IP Act is not undertaken.

OIC recommends that key features of a contemporary legislative information privacy framework for Queensland include: mandatory data breach notification; replacing the IPPs and NPPs with a single set of privacy principles that align with the Australian Privacy Principles (APPS); provision of appropriate powers for the Privacy Commissioner to undertake preliminary inquiries and conduct investigations; oversight of information sharing arrangements by the Privacy Commissioner; and extending obligations to sub-contractors.

Q1. 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?

***Recommendation** OIC submits that the primary object of the RTI Act remains valid and is increasingly relevant to and consistent with community expectations about open, accountable and transparent government.*

The RTI Act represents a clear move to a 'push' model, requiring government to proactively and routinely release information and to have a pro-disclosure bias when deciding formal access applications, only withholding information where disclosure would, on balance, be contrary to the public interest.

The preamble to the RTI Act states that "Government information will be released administratively as a matter of course, unless there is a good reason not to, with applications under this Act being necessary only as a last resort." A right to information law that strikes an appropriate balance between the right of access and limiting that right of access on public interest grounds is critical to both a robust, accountable government and an informed community. Such laws:

...renew accountable democracy. They stimulate responsible freedom in the media. They obviate the plague of leaks that spring up in a world of too many secrets. They encourage a questioning and self-confident citizenry.⁴

Clear leadership and expectations of the public service are required to create effective right of access to information for the community. These essential elements have been evident in the adoption of the Queensland Government Open Data scheme, which is an effective example of a push model initiative.

The primary object of the RTI Act is perhaps more relevant in 2013 than when the legislation commenced in 2009. It is consistent with current Queensland Government commitments to make the government more open, accountable and accessible for all Queenslanders. The Queensland Government recently partnered with the Open Data Institute Queensland (ODIQ) to develop a comprehensive Open Data Policy for Queensland. Australia recently finalised membership with the Open Government Partnership,⁵ an international platform which promotes government transparency and making governments more open, accountable, and responsive. Australia's first National Action Plan was submitted on 7 December 2016 containing 15 commitments focused on: transparency and accountability in business; open data and digital transformation; access to government information; integrity in the public sector; and public participation and engagement.

International and Australian jurisdictions are progressing to greater openness, particularly in areas such as data, performance, and the use of technology.

Q 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?

Recommendation: *OIC considers that the IP Act effectively meets the primary object.*

A primary object of the IP Act is to 'provide for the fair collection and handling in the public sector environment of personal information'. Overall, OIC considers that the IP Act effectively meets this objective. Fairness is delivered by striking an appropriate balance between enabling the legitimate business of government, including provision of community services, and providing robust protections against the misuse of personal information.

⁴ The Hon Justice Michael Kirby The Seven Deadly Sins, British Section of The International Commission of Jurists Fortieth Anniversary Lecture Series, London, Wednesday 17 December 1997

⁵ <http://www.opengovpartnership.org/country/australia>

The IP Act provides a flexible roadmap that guides agencies in appropriately protecting the community's personal information while ensuring government can effectively carry out its business.

OIC has observed that most agencies have readily adopted the IP Act's privacy protections. In Queensland, the RTI and IP Acts have had a significant impact on cultural change in relation to information rights and responsibilities for the public sector and the community. Information privacy is now protected under a legislative framework which plays a key role in safeguarding the rights of community members' personal information and provides clear principles and rules to guide appropriate behaviour by public sector agencies.

OIC performance and monitoring activities have found that there has been an improvement in reported compliance with obligations across all agencies since the first self-assessed Electronic Audit in 2010. The 2016 Right to Information and Information Privacy Electronic Audit found overall, the 184 responding agencies reported on average 81% full compliance and a further 7% partial compliance in meeting their obligations under the IP Act.

The recommendations in this submission focus on providing a contemporary legislative framework to manage new and emerging privacy risks posed by rapid technological change. This includes proposed amendments to strengthen the existing regulatory framework and greater national harmonisation of Queensland privacy legislation with other jurisdictions such as a single set of privacy principles, extending coverage of the IP Act to sub-contractors, mandatory data breach notification and the transfer of personal information overseas.

OIC notes the Queensland Government is committed to enacting a Human Rights Act in Queensland. The IP Act is not intended to cover the field in terms of privacy protections. Enactment of human rights legislation is viewed by OIC as one of a range of mechanism that may strengthen protection of personal privacy in Queensland.

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?

***Recommendation:** While the scope of the RTI Act is a policy issue for government, OIC recommends that GOCs should not be excluded from the operation of the RTI Act as a matter of course. OIC submits that the framework provided by the Auditor-General Act 2009 may provide a useful model for determining which GOCs and similar entities should be subject to the RTI Act.*

Schedule 1 of the RTI Act excludes certain GOC documents from the Act entirely while for some GOCs access rights to other documents are limited only to those which relate to their community service obligations.⁶

As noted in the Consultation Paper, all GOCs are bound by a regulatory framework that includes the *Queensland Government Owned Corporations Act 1993*, the *Commonwealth Corporations Act 2001* and the Code of Practice for government-owned corporations' financial arrangements and other guidance documents.

While the RIT Act may place limited obligations on GOCs, OIC notes that GOCS are required to comply with the Release of Information Arrangements. The Release of Information Arrangements state that the push model applies to all GOCs, including those excluded from the operation of the RTI Act. It specifically requires GOCs to publish information in a Publication Scheme in line with the requirements of the RTI Act and Ministerial Guidelines.

OIC notes that there are different categories of bodies comprising GOCs and these entities will vary in size, scope, legal structure and corporate governance frameworks. Currently, whether or not a GOC, or similar entity, is subject to the RTI Act depends on the nature of the services that the relevant GOC provides.

It is OIC's view that GOC's and similar entities should not be excluded from the operation of the RTI Act as a matter of course. 'The effect of agency or class-based exclusions is to remove from potential public scrutiny information concerning the conduct of public functions and the use of public money without any balancing of public interests that arise.'⁷ Further OIC notes that the Solomon report recommended that 'all bodies that are established or funded by the government or are carrying out functions on behalf of government, should be covered by FOI, unless it is in the public interest that they should not be covered' (Recommendation 20).⁸ OIC recommends that the framework provided by the Auditor-General may provide a useful model for determining which GOCs and similar entities should be subject to the RTI Act.

The *Auditor General Act 2009* gives the Queensland Audit Office (QAO) the power to conduct financial audits of public sector entities including departments, statutory bodies, and GOC. OIC

⁶ Community service obligations are defined in section 112 of the *Government Owned Corporations Act 1993*

⁷ *Review of the Freedom of Information Act and Australian Information Commissioner Act*, submission Peter Timmins, Hawke review.doc viewed at www.ag.gov.au/consultations/docuemnts/reviewoffoilaws

⁸ *Solomon Report: the Right to Information, Reviewing Queensland's Freedom of Information Act, The report by the FOI Independent Review Panel*, June 2008 at p89

notes that the Auditor-General does not have the same mandate for performance audits regarding GOC's.⁹

In OIC's 2015-16 Annual Report, the OIC decision in *Queensland Newspapers Pty Ltd and Ipswich City Council [2015] QICmr 30* (26 November 2015) was noted as a decision of interest. The decision concerned two applications made under the RTI Act for access to information concerning overseas travel by Council personnel in respect of the business of a Council-owned, Ipswich City Properties Pty Ltd (ICP). The RTI Commissioner accepted the Council's argument that documents held by ICP are not documents of an agency – the Council – for the purposes of the RTI Act and are therefore not subject to the Act due to ICP's status as a separate legal entity possessed of distinct corporate personhood. This is despite the fact that the Council is the sole shareholder of ICP, all of ICP's directors are elected officials or Council employees and the stated reasons for the company's incorporation.

The RTI Commissioner observed that the definition of 'public authority' as contained in section 16 of the RTI Act 'did not appear sufficiently broad to encompass entities such as ICP. The RTI Commissioner did note that council-owned companies such as ICP are directly subject to the oversight of the Auditor-General under the *Auditor-General Act 2009* (Qld).

It should also be noted that where GOC's or similar entities do come under the RTI Act, there are relevant exemptions and public interest balancing tests to ensure that the commercial interests of that entity are protected by factors favouring nondisclosure of information. For example, the information could reasonably be expected to prejudice business affairs or the competitive commercial activities of an agency.

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?

***Recommendation:** OIC provides in-principle support for the application of the RTI Act and Chapter 3 of the IP Act to documents of contracted service providers. OIC does not recommend placing the responsibility for processing and deciding applications under the RTI Act on the contracted service provider. Any such amendment is likely to impose an unsustainable and administrative burden on the private sector and not-for profit organisations. OIC recommends reviewing the effectiveness of section 6C of the Commonwealth FOI Act to identify any issues with the operation of this provision prior to adopting this approach in the RTI Act.*

⁹ Section 37A(6) and s38 of the *Auditor-General Act 2009*

OIC notes that, while the RTI Act ensures a right of access to government-held information, where government services are contracted out to the non-government sector, it is likely that the community will not have the same ability to access information because it is held outside government. The community not only seek access to information to ensure accountability and transparency in government expenditure and service delivery performance; individuals often seek information about their own interactions with the government agency providing specific services such as public housing.

‘The outsourcing or contracting out of government services has increased significantly over the last quarter century, into areas that were previously considered to be core government functions. The latest OECD survey reports that in 2011, on average across all member countries, 44% of government production costs were consumed by outsourcing, compared with 47% by government employees. On average, outsourcing represented 10% of GDP (OECD 2013)’.¹⁰

Currently, the RTI Act does not apply to documents of contracted service providers performing government functions. In some circumstances documents held by contractors to Queensland government can be sought from a government agency under the RTI Act: if the agency also has possession of the documents or has a legal right to retrieve the documents (“control of the documents”). A government agency will not always have a legal right to the documents and determining whether or not a legal right exists can be time consuming, as can actually retrieving documents from the contractor.

Existing private sector accountability mechanisms do not provide remedies equivalent to the RTI Act’s right of access to government-held information and other administrative law mechanisms.

The Consultation Paper proposed the option of adopting the approach in section 6C of the Commonwealth FOI Act. As outlined in the Consultation Paper, section 6C of the Commonwealth FOI Act requires agencies to take contractual measures to ensure that they receive documents held by contracted service providers who are delivering services to the community for and on behalf of the Commonwealth.¹¹ The Commonwealth provision places the onus on the agency and not the contracted service provider for the processing of applications thereby allowing access to documents without unduly burdening the contracted service provider.

¹⁰Mulgan, R *Transparency and the Performance of Outsourced Government Services*, Occasional Paper No. 5, the Australian and New Zealand School of Government and Office of the Information Commissioner, viewed at https://www.oic.qld.gov.au/data/assets/pdf_file/0003/27444/paper-transparency-and-outsourced-government-services.pdf at p 7

¹¹ *Freedom of Information Amendment (Reform) Bill 2010*, Commonwealth of Australia Explanatory Memoranda viewed at http://www.austlii.edu.au/au/legis/cth/bill_em/foiab2010381/memo_0.html

OIC notes that section 6C of the Commonwealth FOI Act was enacted to implement a recommendation of the 1995 *Open Government* report by the Australian Law Reform Commission and Administrative Review Council on the review of the FOI Act. The report concluded that the use of contractors to provide services to the public on behalf of the government 'posed a potential threat to the government accountability and openness provided by the FOI Act'.¹² 'If an arrangement is underpinned by contract, an agency 'should ensure that suitable arrangements are made for the provision of public access rights.'¹³

The Commonwealth FOI Act does not bring the contractor within the ambit of the Act; rather, the agency must retrieve the documents from the contractor. The requirement to retrieve documents from the contractor is triggered by the receipt of an access application the scope of which includes Commonwealth contract documents and it can only be exercised where appropriate terms exist in the contract.

OIC notes that section 6C of the Commonwealth FOI Act does not apply to contracts for the procurement of services for the agency's use, such as information technology services or cleaning services provided to the agency. Rather, the requirement is concerned with contracting out arrangements involving the provision of services to the public on behalf of the agency.

OIC notes that ensuring documents relating to the performance of government contracted entities can be sought via access applications would be consistent with the approach taken under the IP Act which requires Queensland government agencies to take reasonable steps to bind contracted service providers to the privacy principles.

OIC does not recommend that contractors be made an agency that must process and decide access applications under the RTI Act. Any such amendment is likely to impose an unsustainable and administrative burden on the private sector and not-for profit organisation.

Any amendment needs to ensure that agencies have 'control' and immediate right of access to documents i.e. the Information Commissioner has previously explained that a document will be under the control of an agency where the agency has a present legal entitlement to take physical possession of the document.

OIC recommends the government give favourable consideration to adopting a provision similar to section 6C of the Commonwealth FOI Act after first satisfying itself of the effectiveness of and identifying any issues with the operation of this provision at the federal level.

¹² Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC Report 77 (1995) [15.12].

¹³ See note 1

Q5. Should GOCs in Queensland be subject to the Queensland’s IP Act, or should they continue to be bound by the Commonwealth Privacy Act?

***Recommendation** OIC notes that the Commonwealth Privacy Act provides strong protections for the community in relation to handling and use of their personal information. Should other recommendations regarding amalgamation of the IPPs and NPPs to align more closely with the APPs be accepted, issues raised in the Consultation Paper regarding GOCs not being subject to the IP Act would largely be addressed*

As noted in the Consultation Paper, the Information Privacy Principles (IPPs) under the IP Act do not apply to GOCs and their subsidiaries.

State or Territory organisations that are incorporated companies, societies or associations are deemed to be organisations for the purposes of the Commonwealth *Privacy Act 1988* (Commonwealth Privacy Act) and are subject to the Australian Privacy Principles (APPs) in the Commonwealth Privacy Act.

OIC notes that the Commonwealth Privacy Act provides strong privacy protections for the community in relation to handling and use of their personal information. Should other recommendations regarding amalgamation of the IPPs and NPPs to align more closely with the APPs be accepted, issues raised in the Consultation Paper regarding GOCs not being subject to the IP Act would largely be addressed.

Q 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?

***Recommendation** OIC recommends privacy obligations in the IP Act be extended to sub-contractors. OIC considers that section 95B of the Commonwealth Privacy Act may provide a useful model for extending privacy obligations in the IP Act to sub-contractors.*

Increasingly government agencies are seeking to outsource or contract provision of government services and functions. If the provision of services under the contract or other arrangement involves the exchange or handling of personal information in any way, the IP Act requires the contracting agency to **take all reasonable steps** to ensure the contracted service provider is contractually bound to comply with either the IPPs or NPPs, and with section 33 of the IP Act, which concerns the transfer of personal information outside Australia.

Under the IP Act, the bound contracted service provider obligations apply to contractors only. They do not apply to sub-contractors.

The obligation to bind is not mandatory – agencies are merely required to ‘take all reasonable steps’ to bind the contracted service provider to comply with the privacy principles under the IP Act. Failure to bind a contracted service provider means that an individual, whose personal information is dealt with by a contracted service provider, will not be afforded any privacy protection.

In some instances, a contractor will be separately covered under the Commonwealth Privacy Act. However, section 7(B)(5) of that Act states that there is no coverage when the contract involves a State or Territory government.

OIC recommends that the privacy obligations in the IP Act extend to sub-contractors. OIC notes that Section 95B of the Commonwealth Privacy Act requires an agency entering into a Commonwealth contract to take contractual measures to ensure that a contracted service provider for the contract, or a subcontractor, does not do an act or engage in a practice that would breach an APP if done or engaged in by the agency.

The term ‘contracted service provider’ is defined in s 6(1) of the Commonwealth Privacy Act and includes an organisation that is or was a party to a Commonwealth contract and that is or was responsible for providing services to an agency under that contract. The term also includes a sub-contractor for the contract. The term ‘Commonwealth contract’ is also defined in s 6(1) to mean a contract, to which the Commonwealth, Norfolk Island or an agency is or was a party, under which services are to be, or were to be, provided to an agency.

Q 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?

***Recommendation** OIC recommends a single point of entry for the right of access within the RTI Act. OIC recommends the following consequential changes if access rights for personal information are relocated to the RTI Act, including:*

- *relocating amendment rights for personal information from the IP Act to the RTI Act;*
- *and*
- *mechanisms in the RTI Act to exclude wholly personal applications from application fee and disclosure log requirements.*

OIC supports a single point of entry for the right of access within the RTI Act. When access rights for personal information were located in a separate piece of legislation, the IP Act, it was hoped that doing so would create a simpler and quicker process for applicants and agencies, leaving the RTI Act to deal primarily with government accountability matters.

In practice, however, splitting access rights in this way has not created a simpler or quicker process. In OIC's experience, the threshold question for an access application, 'Under which Act should this application be processed?', has created an unnecessarily burdensome process for agencies, confusion and delay for applicants, and a reviewable decision which must be dealt with before an agency can begin processing the access application.

When agencies receive an access application, they must:

- determine whether the access application has been made under the right Act
- if incorrectly made under the IP Act, follow a formal process with the applicant to alter their application or transfer it to the RTI Act¹⁴
- if incorrectly made under the RTI Act, liaise with the applicant about changing the application to the IP Act; and
- in some circumstances, make a reviewable decision that an access application does not seek personal information and therefore an application purportedly made under the IP Act cannot be dealt with under the IP Act¹⁵.

Section 40 of the IP Act creates a right of access to documents "to the extent they contain the applicant's personal information". OIC has interpreted this section as creating a right of access to an entire document, as long as it contains some amount of the applicant's personal information, and not as a right of access only to the personal information within the document. This means that access to both personal and non-personal information is available under the RTI and the IP Act. The separation of access rights between the RTI and IP Acts also creates inconsistencies in how agencies treat an application. OIC is aware of circumstances where applicants have applied to multiple agencies for the same category of documents and there was no consistency in how the applications were treated, some being assessed as IP applications, some as RTI applications.

The RTI and IP Acts prescribe how an access application is to be processed. Apart from Charges Estimate Notice (CEN) and Schedule of Documents obligations in the RTI Act these provisions are essentially identical. Identical review rights are set out in both Acts, as are the processes to be followed for those reviews. The RTI Act and the IP Act both set out when an agency can refuse to deal with an application and what processes it must first follow: these provisions in the IP and RTI Acts are, again, effectively identical.

The RTI Act sets out when access to a document can be refused. The IP Act does not; instead, it refers IP Act decision-makers back to the RTI Act and requires them to use it to make their IP Act

¹⁴ From RTI Act to IP Act – see section 34 RTI Act. From IP Act to RTI Act – see section 54 IP Act.

¹⁵ Section 54(5)(b) of the IP Act.

access decision. This can be confusing for applicants and can add unnecessary complexity to both the decision making process and to communicating the reasons for a decision.

Given the above, there will be no difference between an access decision made under the RTI Act and one made under the IP Act. It is difficult to see that there are any practical benefits resulting from splitting the access rights into two Acts. The difficulty and time involved with answering the 'Which Act?' question could be removed to the benefit of agencies and applicants, with little to no negative impact on the rights of applicants, by absorbing Chapter 3 of the IP Act's access rights into the RTI Act.

Consequential changes required if IP access rights are relocated to the RTI Act Amendment applications

Chapter 3 of the IP Act also creates a right of amendment of personal information if it is inaccurate, out of date, incomplete, or misleading. The procedures an agency must follow for an amendment application are essentially identical to those for an IP Act access application; many of the access provisions also apply to amendment applications, including the review rights and refusal to deal provisions. If a single point of entry is created in the RTI Act, access rights will be removed from the IP Act but a significant number of the access provisions will need to be retained as they also govern amendment applications.

OIC suggests that, if IP access rights are relocated to the RTI Act, it would be simpler to also relocate amendment rights, which would allow Chapter 3 of the IP Act to be removed entirely.

Application fees and disclosure logs

OIC notes that, in order to avoid any adverse impact from relocating access and amendment rights to the RTI Act, there are two key issues that need to be addressed: application fees for, and disclosure log eligibility of, wholly personal applications.

OIC's suggested approach is to require a valid access application to include an answer to a mandatory question, similar to the beneficiary question for RTI applications in section 25 of the RTI Act. For example, such a question could be similar to:

"Do you only want access to documents that contain your personal information? By answering yes you pay no application fee, but you acknowledge that the agency will not consider any documents that do not contain your personal information."

Applicants must answer either yes or no for the application to be valid.

If they answer yes, the RTI Act should provide that:

- they do not have to pay an application fee
- their application is excluded from the requirement to place application details and released documents on the Disclosure Log; and
- agencies need not provide CENs or Schedules of Documents.

If they answer no, the RTI Act will continue to provide that:

- an application fee is required
- agencies will have to provide CENs and Schedules of Documents; and
- the application would be subject to the Disclosure Log requirements.

This approach would retain the benefits which arise from personal information access rights being contained in Chapter 3 of the IP Act and remove the disadvantages. There would be no obligation on an agency to engage in further consultation with the applicant or answer the threshold question prior to processing the application: if the applicant has indicated they only want documents that contain their personal information, agencies only consider documents that contain personal information within the scope of the request. If the applicant has not limited their application solely to documents that contain their personal information, agencies consider all documents within the scope of the request.¹⁶

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

***Recommendation:** OIC notes that mandating the requirement to provide a Schedule of Documents in the RTI Act may not provide sufficient discretion for decision-makers, however it is OIC's view that to do so is good practice.*

As noted previously, it is difficult for OIC to provide a fully informed response to this issue given the responses to the 2013 consultation were not publically available.

Under section 36 of the RTI Act, an agency is required to give the applicant a Schedule of Documents unless the applicant agrees to waive the requirement. A Schedule of Documents gives a brief description of the classes of documents relevant to the application in the possession, or under the control, of the agency or Minister and sets out the number of documents in each class.

The purpose of requiring a Schedule of Documents was to ensure the applicant receives what they are actually seeking, as it:

¹⁶ In the latter case, it would be irrelevant if all documents in scope prove to only be ones which contain the applicant's personal information; the application would be processed in the same way as any application that requested documents some of which would not contain the applicant's personal information.

- gives the applicant an indication of the nature and extent of documents held by the agency that relate to their application,
- encourages dialogue between the agency and the applicant; and
- allows the applicant to decide which of the listed documents they want to access.

These opportunities are intended to cut processing time, reduce the costs of providing the material, and reduce disputes. The recommendation to require a Schedule of Documents was based on the assumption that decision-makers already prepare a Schedule of Documents drawn from the documents' metadata.

OIC understands that electronic document management systems, which would arguably allow quick and simple generation of Schedules based on document metadata, are not universal across agencies and that significant amounts of documents are only available to decision-makers in hard copy. As a result, creating a Schedule of Documents at an early stage of the process can be time-consuming, as it requires a decision-maker to go through each document by hand and manually create the Schedule. OIC notes that the preparation of a Schedule of Documents is part of processing the application and, as such, that time spent on it is something the applicant pays for.¹⁷

Generally, most applications relate to a specific subject matter or entity, rather than to specific kinds of documents, and applicants may not be aware of which agency documents may contain the information they are seeking. As such, a Schedule of Documents that lists how many of what type of documents relate to a broad subject may be of limited assistance to an applicant in narrowing the scope of their application.

While, OIC notes that that mandating the requirement to provide a Schedule of Documents in the RTI Act may not provide sufficient discretion for decision-makers, OIC considers that preparing and providing such a schedule is good practice.

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?

***Recommendation:** OIC recommends lifting the threshold in section 37 of the RTI Act from 'concerned' to 'substantially concerned', reinstating the narrower test for required consultation with third parties about intended release of documents.*

Section 37 of the RTI Act requires an agency to consult with a third party where the release of information may reasonably be expected to be of concern to the third party. Consulting under this

¹⁷ RTI Regulation 2009, section 5(4)

section grants decision-makers an additional ten business days to decide an application; however only one period of ten business days applies regardless of the number of third parties with whom the agency must consult.

Prior to the RTI Act, the requirement to consult had a higher threshold of 'substantially concerned'. OIC considers that the change to a lower threshold has resulted in a significant increase in the number of third parties required to be unnecessarily consulted by both agencies and the OIC. Consequently, this has caused a delay in the processing of access applications initially and during review.

The pro-disclosure bias of the RTI Act, the starting point that all information is to be disclosed, and the proviso that information can only be withheld from release if disclosing it would be contrary to the public interest create a high threshold for refusing access to information. The comparatively low threshold for third party consultation creates an imbalance where the threshold at which agencies are required to consult is much lower than the threshold at which agencies are permitted to withhold.

In the matters coming to OIC on external review, the requirement to consult at the current threshold of concern appears to have a substantial resource impact on agencies. Also, it may contribute to an unnecessary delay that can result in deemed decisions, generating additional work for decision-makers, and creating unrealistic expectations in the minds of consulted third parties who are not necessarily aware of the pro disclosure bias and consequent high public interest in releasing information. In addition to those unrealistic expectations, it also impacts on consulted third parties' time as they are required to respond to consultation requests even when there is little real chance that their submissions will a) have any relevance to the grounds for refusal set out in the legislation and/or b) raise sufficient concern to displace the RTI Act's pro-disclosure bias.

Accordingly OIC recommends amending the threshold in section 37 of the Act from 'concerned' to 'substantially concerned', reinstating the narrower test for required consultation with third parties about intended release of documents.

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?

Recommendation: OIC recommends retaining the right of review for a party who should have been but was not consulted about an application **as there are instances where a review has value.**

The RTI Act provides a third party with a right of review in relation to a decision to disclose a document, if an agency or Minister should have taken, but has not taken, steps to obtain the views of a relevant third party.¹⁸

As noted in the Consultation Paper, a third party may not know that a decision to disclose a document has been made until after the document has been disclosed, raising questions about the value of a review right in these circumstances.

While OIC notes that, in most circumstances, a review right will be futile in circumstances where the document has been disclosed, OIC recommends retaining a right of review for a third party who should have been but was not consulted about an application due to its value in some instances. For example, in some instances when a matter comes on external review, documents may not have been released and are able to be retrieved.

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

***Recommendation:** OIC notes that the public interest test provides agencies with sufficient flexibility to make decisions that reflect the extent of their concerns regarding disclosure of documents. In the event a new exempt information category is considered, careful consideration and proper consultation with the community would be necessary to ensure it is consistent with the overall objects of the RTI Act.*

An agency may refuse access to a document to the extent that it comprises exempt information.¹⁹ Exempt information is information which Parliament has considered would, on balance and in all circumstances, be contrary to the public interest to release.²⁰ The various types of exempt information are set out in schedule 3 of the RTI Act.²¹

It is OIC's view that Queensland's exempt information provisions have been carefully considered and align to a great extent with those found in other Australian jurisdictions.²² In relation to the RTI Act exempt information provisions which have been considered by OIC in its decisions, it is OIC's view that they can generally be applied without giving rise to ambiguity or unnecessary complexity. In

¹⁸ Schedule 6, RTI Act, *reviewable decision*

¹⁹ Sections 47(3)(a) and 48 of the RTI Act.

²⁰ Section 48(2) of the RTI Act.

²¹ Section 48(4) of the RTI Act.

²² OIC notes that: some of the exempt information provisions are treated as PI factors favouring nondisclosure in other Australian jurisdictions; and other exempt information provisions have no counterpart in some (and in some instances all) of the other Australian jurisdictions – presumably leading to consideration of such types of information in the context of those jurisdictions' public interest test equivalents instead.

relation to the exempt information provisions which have not yet been addressed in OIC decisions²³OIC can discern no issues which might impede their satisfactory operation.

OIC considers that the public interest balancing test provides agencies with significant flexibility to make decisions that reflect the extent of their concerns regarding disclosure of documents. The public interest balancing test complements the existing categories of exempt information Parliament has decided would be contract to the public interest to disclose. While some may seek the certainty of an explicit exemption, such provisions do not have the flexibility of the public interest test, which is an effective tool which allows decision makers to take into account and balance all public interest factors both favouring and not favouring disclosure that are relevant to the particular circumstances of each case.

The RTI Act represents a clear move to a 'push' model, requiring government to proactively and routinely release information and to have a pro-disclosure bias when deciding formal access applications, only withholding information where disclosure would, on balance, be contrary to the public interest.

In the event a new exempt information category is considered, careful consideration and proper consultation with the community would be necessary to ensure it is consistent with the overall objects of the RTI Act.

As mentioned previously, without access to the 2013 public submissions OIC is not in a position to respond to any particular arguments for or against the reduction or expansion of exemptions.

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?

***Recommendation:** It is OIC's view that the public interest balancing test (PIBT) is working well. Any proposed changes to the current PIBT will require extensive consultation given the fundamental importance of the test to the operation of the RTI Act.*

As noted previously, given submissions to the 2013 consultation were not made publically available OIC is not in a position to comment on 2013 responses regarding simplification of the public interest balancing test (PIBT).

In its submission to the 2013 review of the RTI Act and Chapter 3 of the IP Act, OIC noted that the PIBT was working well. While OIC recommended combining the factors in schedule 4, Parts 3 and 4 into a single list of public interest factors and that consideration be given to grouping the combined

²³ That is, schedule 3, sections 4, 4A, 4B, 5, 9 and 10(5) of the RTI Act

factors into related groups²⁴, a substantial period of time has elapsed since OIC made this recommendation in 2013. During this period of time, a body of OIC decisions and case law has developed to provide guidance to decision-makers in the application of the PIBT under the RTI Act.

The PIBT lies at the very core of the RTI Act and is integral to decision-making under the Act. The PIBT is also inextricably linked to the operation of a number of other provisions in the Act. OIC considers that any proposed changes to the current PIBT will require extensive consultation given the fundamental importance of the test to the operation of the RTI Act. Any proposed amendments to the PIBT require careful consideration to ensure there are no unintended consequences and the existing test is not being re-framed with this approach. It should also be noted that these PIBT factors are not exclusive. Further, OIC notes that the Consultation Paper proposes condensing Part 3 and Part 4 factors into a single list of factors favouring non-disclosure as one option to simplify the PIBT. The Consultation Paper provides the following example to demonstrate the significant overlap between existing Part 3 and Part 4 factors:

Part 3, Item 3 Disclosure of the information could reasonably be expected to prejudice the protection of an individual's right to privacy and the harm factor in Part 4, Item 6 Disclosing personal information. Part 4 Item 6 states:

(1) Disclosure of the information could reasonably be expected to cause a public interest harm if disclosure would disclose personal information of a person, whether living or dead.

(2) However, subsection (1) does not apply if what would be disclosed is only personal information of the person by whom, or on whose behalf, an application for access to a document containing the information is being made.

Given the nuances between these Part 3 and Part 4 factors, OIC does not consider that they overlap or are duplicated. 'Personal information' and 'Privacy' are conceptually different factors and deletion of either the Part 3 or Part 4 factor, or minor wording amendments, will result in an altered PIBT and possibly unintended consequences

For example, in its decisions OIC is able to distinguish between routine personal work information of a public servant and the sensitive nature of medical records by relying on the weight to be attributed to both factors, including the high degree of privacy in the case of the latter, in comparison to the low degree of privacy in the case of the former.

²⁴ Recommendation 7.3, Office of the Information Commissioner Queensland, Submission to the Department of Justice and Attorney-General Discussion Paper, Review of the Right to Information Act 2009 and Chapter 2 of the *Information Privacy Act 2009*, November 2013.

It is OICs view that deleting or merging an existing Part 3 or Part 4 factor to consolidate these factors into a single list is an overly simplistic approach and fails to recognise the nuances between the existing Part 3 and part 4 factors in the RTI Act. Further, the unintended consequences of making minor amendments to the existing wording of the current factors in part 3 and Part 4 requires careful consideration to ensure the existing test is not being reframed with this approach.

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.

Recommendation: OIC considers no changes to the language used in the thresholds or any other changes to the thresholds are required.

OIC notes that varying thresholds must be satisfied before particular public interest factors in schedule 4 become relevant, for example ‘contribute to’²⁵ has a lower threshold than ‘ensure’²⁶. Also, various public interest factors in schedule 4 link two consequences with the word ‘and’ in doing so, this requires that both consequences be satisfied before the factor becomes relevant, for example ‘promote open discussion of public affairs and enhance the Government’s accountability’²⁷

OIC considers it is important to note that the factors in schedule 4 are non-exhaustive.²⁸ This means that, even where a high threshold or multiple-consequence factor in schedule 4 is not applicable, the decision-maker can consider a similar public interest factor with a lower threshold, for example:

- ‘enhance effective oversight of expenditure of public funds’ rather than ‘ensure effective oversight of expenditure of public funds’²⁹; or
- ‘enhance the Government’s accountability’ rather than ‘promote open discussion of public affairs and enhance the Government’s accountability’³⁰.

Consequently, the higher thresholds and multiple-consequences specified in some schedule 4 public interest factors are, in practical terms, not critical issues; they do not preclude consideration of similar public interest factors with lower thresholds or those encompassing only one consequence.

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?

²⁵ Schedule 4, part 2, items 2, 13 and 15 to 19 of the RTI Act.

²⁶ Schedule 4, part 2, item 4 of the RTI Act.

²⁷ Schedule 4, part 2, item 1 of the RTI Act

²⁸ Given the wording of section 49(3)(a),(b) and (c) of the RTI Act.

²⁹ Schedule 4, part 2, item 4 of the RTI Act.

³⁰ Schedule 4, part 2, item 1 of the RTI Act.

Recommendation: *OIC considers no changes to the public interest factors are required.*

In its decisions, OIC has identified and considered public interest factors other than those listed in schedule 4. As well as the public interest factors mentioned above (similar to existing public interest factors but with lower thresholds or involving only a single consequences), OIC's decisions have included consideration of public interest factors not present in schedule 4, such as supporting informed consumer choices³¹ and enabling royalty recipients to access information otherwise unavailable to them regarding royalty calculations³².

OIC notes that, when the public interest test was introduced, there was some concern that listing public interest factors in schedule 4 could reduce flexibility or freeze the public interest concept in time. However, it was also noted that listing the factors would improve agencies' decision making and result in more uniformity of decision making across agencies.

In OIC's experience, the lists act as prompts which assist decision-makers and parties to identify all public interest factors relevant to a particular application. In this sense, it is arguable that expansion of the current public interest factors to include additional factors which have been identified and applied could be beneficial.

OIC does not consider it good practice to continually expand the schedule 4 factors to include new factors identified and applied by decision-makers. The public interest factors listed in schedule 4 are non-exhaustive. Consequently, parties can raise, and decision-makers can consider, any relevant public interest factor, including those not listed in schedule 4.

OIC is also concerned that adding public interest factors to schedule 4 could reinforce misconceptions that the factors are exhaustive or discourage decision-makers from identifying and applying new factors relevant to their applications. Further, doing so could give rise to the mistaken impression that there were two tiers of public interest factors: those which are listed in schedule 4 and those which are not. This could arguably result in factors listed in schedule 4 being given greater weight than new, decision-maker identified, factors simply because they were 'important enough' to be included.

Decision-makers could also find it difficult to determine whether particular public interest factors were not listed in schedule 4 because they had never before arisen, arose so infrequently their

³¹ *Seven Network Operations Limited and Safe Food Production Queensland; Food business* (Third Party) (Unreported, Queensland Information Commissioner, 10 February 2012) and *Nine Network Australia Pty Ltd and Brisbane City Council* (Unreported, Queensland Information Commissioner, 7 June 2012).

³² *Gordon Resources Limited and Department of Employment, Economic Development and Innovation* (Unreported, Queensland Information Commissioner, 21 September 2011).

inclusion in schedule 4 was not considered justified, or were awaiting inclusion via an appropriate Bill.

In OIC's view, the non-exhaustive nature of the public interest factors provides an effective and flexible framework for applying and balancing public interest factors within the specific context of an access application. Given that the RTI Act's public interest balancing text already grants a decision-maker the capacity and flexibility to consider any public interest factor OIC does not consider it necessary to add new public interest factors to schedule 4.

As noted previously by OIC, it is OIC's view that the public interest balancing test is working well. A substantial period of time has elapsed since the 2013 consultation by the former Government on the review of the RTI and IP Acts. During this period of time, a body of OIC decisions and case law has developed to provide guidance to decision-makers in the application of the public interest balancing test under the RTI Act.

In addition, OIC considers that its training and resources assist decision-makers to identify and consider public interest factors not listed in schedule 4. OIC's resources can be quickly updated when new public interest factors are identified, to explain them and discuss the types of information or circumstances in which they may become relevant.

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?

***Recommendation:** No recommendation. However, OIC considers that removing the requirement to include on a disclosure log an applicant's name and whether they have applied on behalf of another entity is consistent with the purposes of a disclosure log*

The rationale for disclosure logs is that if one person has expressed an interest in accessing particular documents then the same documents might be of interest to the wider community. Disclosure logs provide access to information for people who want to access the same documents as a previous applicant, and who would otherwise have needed to submit their own formal access application, with the associated costs and timeframes.

Disclosure logs also provide an opportunity for the agency to publish documents with associated supporting information, explaining issues of public interest in greater depth.

It is OIC's view that removing the requirement to include on a disclosure log an applicant's name and whether an applicant has applied on behalf of another entity is consistent with the purposes of a disclosure log.

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

***Recommendation:** No recommendation. OIC's desktop audit program between 2012 and 2016 has focussed on local governments, hospital foundations and hospital and health services. While OIC has no independently verified information about departments' implementation of their compliance obligations, it reported on the agencies self-assessed progress in 2016*

As noted in the Consultation Paper, prior to 2012 all agencies were subject to the same requirements. Amendments in 2012 required departments and Ministers (but not other agencies, such as statutory bodies and councils) to publish more information on their disclosure logs, including the date of each valid application received and details of the information for which the applicant has applied.³³

The current disclosure log requirements do not oblige agencies to place the actual documents that have been accessed on the disclosure log. The amendments place new obligations on certain agencies, namely departments and Ministers, to publish on the disclosure log the applicant's name and the actual documents that have been accessed through right to information applications, with appropriate deletions, as soon as practicable after the documents have been released to the applicant.

The amendments also require right to information applications to indicate whether access is sought for the benefit of, or use by the applicant or another entity. If access is sought for the benefit of, or use by an entity other than the applicant then the name of the entity is also to appear on the disclosure log after the applicant has accessed the documents. .

In addition departments and Ministers are , as soon as practicable after an application has been made, required to include on the disclosure log details of the information being sought and the date the application was made

OIC has not desktop audited departments since the 2012 amendments, so have no independently verified information about their implementation of their compliance obligations with regards to disclosure logs.

During 2015–16, OIC conducted the *2016 Right to Information and Information Privacy Electronic Audit*, which captured public sector agencies' self-assessment of their progress in complying with the

³³ *Right to Information and Integrity (Openness and Transparency) Amendment Act 2012*

legislation and associated guidelines. 184 agencies responded to the audit, the third in a series which has been conducted in 2010 and 2013. The comparative results were presented to Parliament in a report in August 2016. All Queensland Government departments completed the 2016 self-assessment. An analysis of the responses reported to the 2016 self-assessed electronic audit found agencies and departments continued to report high levels of compliance with disclosure log obligations.

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

***Recommendation:** OIC notes that the proposal to extend disclosure log requirements to agencies such as local councils and universities is likely to have significant resourcing impacts and recommends agencies are consulted in detail about this proposal*

As noted previously, prior to 2012 all agencies were subject to the same disclosure log requirements under the RTI Act. Amendments in 2012 required departments and Ministers (but not other agencies, such as statutory bodies and councils) to publish more information on their disclosure logs, including the date of each valid application received and details of the information for which the applicant has applied.

Section 78A of the RTI Act provides that an agency (i.e. other than a Department or Minister) *may* include in a disclosure log a copy of a document or details identifying a document that does not contain personal information of the applicant and which has been accessed by the applicant within the access period. The decision to publish documents through a disclosure log is therefore at the discretion of each agency.

While it is not mandatory for agencies other than departments and Ministers to maintain a disclosure log,³⁴ the Ministerial Guidelines state that ‘departments and Ministers should consider publishing as much information as possible in a disclosure log’ to support openness and accountability.

It is OIC’s view that the legislation and Ministerial Guidelines would be clearer if they mandated that agencies list documents in the disclosure log and provided agencies with a discretion to link directly to documents. As a general comment, the Ministerial Guidelines would assist agencies more effectively if statements that agencies ‘should’ do something were resolved as being mandatory or discretionary.

³⁴ See section 78A(1) of the RTI Act

OIC notes that proposal to extend the disclosure log requirements that apply to departments and Ministers to other agencies such as local councils and universities is likely to have a significant resourcing impact on these agencies. Accordingly, it is OIC's view that these agencies should be consulted in detail before consideration is given to amending the disclosure log requirements for agencies in the RTI Act to align with the obligations placed on departments and Ministers.

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

***No Recommendation:** No recommendation however OIC considers the requirement for information to be published on a disclosure log 'as soon as practicable' after the applicant accesses the document within the access period provides agencies with the required flexibility to comply with their disclosure log obligations under the RTI Act.*

As noted previously, the RTI act contains tools to facilitate the push model such as requiring agencies to publish disclosure logs and publications schemes. Disclosure logs contain information about previous formal RTI access applications made to the agency and copies of documents released as a result. Section 78(3) of the RTI Act requires publication on a disclosure log of a copy of the document and names of applicants and entities 'as soon as practicable' after the applicant accesses the document.

OIC notes that the Consultation Paper states that prior to the 2012 amendments, the RTI Act specified that documents should not be placed on the disclosure log until at least 24 hours after the documents were accessed. OIC considers further information is required about the perceived difficulties with the current provision before consideration is given to amending the existing legislative requirements under the RTI Act.

While changes to timeframes for publication of information on disclosure logs is a matter of policy for Queensland Government, it is OIC's view that the requirement for information to be published on a disclosure log 'as soon as practicable' is reasonable and provides the required flexibility for agencies with regards to publication.

As noted in the Ministerial Guidelines for *publication schemes and disclosure logs* 'what as 'soon as practicable' means must be considered on a case by case basis'³⁵ having regard to all the circumstances. For example, this time period could be longer for applications involving many documents requiring extensive redaction, compared with applications for one document that does not require redaction.

³⁵ Ministerial Guidelines for *publication schemes and disclosure logs*

While 'as soon as practicable' is not defined in the RTI Act, OIC notes additional guidance is provided on OIC's website and in the Ministerial Guidelines. If it is considered further clarification around the meaning of 'as soon as practicable' is required, OIC recommends consideration be given to updating the Ministerial Guidelines and/or the development of policies and procedures which addresses the meaning of 'as soon as practicable' to provide greater guidance to agencies to facilitate compliance with disclosure log obligations. Alternatively, the Ministerial Guidelines could clarify that agencies must publish a description of an accessed document in the disclosure log as soon as possible, and that agencies can link directly to documents 'if practicable', where agencies may develop an administrative procedure to define 'practicability' in their own circumstances.

OIC notes that the Consultation Paper refers to relevant NSW legislative provisions which provide that information is only included on the disclosure log if an agency considers that it may be of interest to other members of the public.³⁶

OIC does not support amending the RTI Act to require agencies to only record information in the disclosure log if an agency considers that it may be of interest to other members of the public. The rationale for disclosure logs is that if one person has expressed an interest in accessing particular documents then the same documents might be of interest to the wider community. Disclosure logs provide access to information for people who want to access the same documents as a previous applicant, and who would otherwise have needed to submit their own formal access application, with the associated costs and timeframes. Disclosure logs also provide an opportunity for the agency to publish documents with associated supporting information, providing a single point of truth and explaining issues of public interest in greater depth.

Disclosure logs are part of proactive disclosure of information under the RTI Act. Allowing agencies to decide what documents might be of interest to the wider community is contrary to the 'push model' and objects of the RTI Act. As noted in a number of compliance reviews undertaken by OIC, as part of its performance monitoring and review functions, agencies do not necessarily know what information the community wants.

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

***Recommendation:** OIC recommends retaining the legislative requirement for a publication scheme. OIC does not consider it necessary to prescribe the classes of information that must be included in any publication scheme.*

³⁶ *Government Information (Public Access) Act 2009 (NSW) s25.*

Under the RTI Act, agencies are required to maintain and populate a publication scheme in accordance with the RTI Act and Ministerial Guidelines. Publication schemes are specifically required by the RTI Act as a push model strategy for disclosure other than by a formal application under the Act, as applications are intended as a last resort. Publication schemes set out the kinds of information that an agency should make routinely available.³⁷

Most agencies satisfy the publication scheme requirements by publishing a publication scheme on their website, often linking to specific information required under the Ministerial Guidelines.

Analysis of the *OIC 2016 Right to Information and Information Privacy Electronic Audit* in which agencies self-assessed their progress in meeting their obligations under the RTI Act and the IP Act, found that overall, the 184 responding agencies reported on average 81% full compliance and a further 7% partial compliance, which together is an increase of 3 percentage points since 2013.

While agencies reported high levels of full compliance in application handling, the report noted the need for agencies to focus on proactive disclosure strategies, with four key areas for improvement identified - governance, administrative access arrangements, community consultation and performance monitoring. In 2016, 15% of agencies reported they do not have a publication scheme, compared to 25% in 2013.

Responding agencies reported progress on the 2013 results across all topics except in internal reviews (decrease of 2 percentage point) and community consultation (no change).

The most progress, between 8 and 10 percentage points for full or partial compliance or related performance, occurred in the areas of policy development and oversight, publication scheme, administrative access arrangements and staffing resources.

OIC noted in its submission to the 2013 consultation that OIC considers over time, the need for legislatively structured publications schemes will be succeeded by consistent user environment standards, which will ensure agencies satisfy these objectives and allow agency website to adopt contemporary design standards better suited to achieve this purpose.

OIC notes that increasingly Queensland Government is moving towards adopting a 'one-stop shop' approach to make it easier to access government information and services. This includes the creation of a personalised online 'my account' and access to more than 250 new and/or improved services online.³⁸ Requiring a publication scheme that is agency based with prescriptive classes of

³⁷ Ministerial Guidelines, page 3

³⁸ <https://www.qld.gov.au/dsiti/initiatives/one-stop-shop/progress/>

information may no longer work or align with future changes to online delivery of government information and services.

OIC notes that while publication schemes are an important push model strategy, prescriptive requirements about the classes of information required for a Publication Scheme may be replaced with a legislative requirement for an agency to publish significant, accurate and appropriate information about the agency on the agency website that is easy to navigate and accessible.

While OIC recommends retaining the legislative requirement for a publication scheme, OIC does not consider it necessary to prescribe the classes of information that must be included in any publication scheme.

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?

***Recommendation:** OIC considers that amending the legislation to make internal review mandatory may not significantly impact on demand for external review. OIC recommends broadening OIC's remittal power in specified circumstances. OIC considers that including the power to remit for certain external reviews to agencies for decision would contribute to reducing demand for external review and the more efficient and effective use of government resources. By giving the OIC the discretion to remit certain external reviews back to agencies for decision it allows OIC to the option of dealing with the external review if it considers that it would be inefficient or impractical to remit the external review back to the agency. Alternatively, to remit the external review back to the agency to ensure agencies take responsibility for access decisions where it can be done in an efficient and effective manner.*

In its 2013 submission to the review of the RTI Act and Chapter 3 of the IP Act, OIC submitted that consideration be given to making internal review mandatory to increase the efficiency and effectiveness of review under the RTI Act.

This recommendation was made as part of a broader strategy for managing external review demand. As noted in OIC's 2015-16 Annual Report, OIC has continued to deal with a high number of external review applications (OIC closed 407 matters including a number of high profile, complex and sensitive applications).³⁹

³⁹ https://www.oic.qld.gov.au/_data/assets/pdf_file/0011/31502/2015-16-oic-annual-report.pdf at p4

However, since that time a body of OIC decisions and case law has developed to guide agencies in the management of access applications meaning that increasingly the more complex matters are coming on external review.

OIC submits that resource implications of policy changes with RTI and IP extend beyond internal review. OIC considers that if the RTI Act was amended to make internal review mandatory it may not have a significant impact on demand for external review. It is OIC's experience only a relatively small number of internal reviews have resulted in a changed outcome for applicants. Further, OIC considers that in some circumstances mandatory internal review is likely to be of little value and, as noted in the Consultation Paper, lacks the required flexibility to take into account the individual circumstances of each application. For example, mandatory internal review is likely to be counter-productive where an applicant has lost trust with the agency as part of dealing with the initial access application.

A remittal power

OIC currently has a narrow power to remit matters back to an agency: it can only do so if the agency requests further time to deal with the application.⁴⁰ It has no power to remit on its own initiative. In terms of a power to remit, OIC notes that:

- New South Wales' Information Commissioner may make a recommendation that the relevant agency reconsider a decision⁴¹ ; and
- Victoria's Information Commissioner may, with the agreement of the applicant, refer a matter back to the relevant agency for a fresh decision⁴²

The Australian Information Commissioner submitted to the Hawke Report that it should have a remittal power for deemed decisions, where an agency has commenced, but not managed to complete, processing a very large request. The Hawke Report made recommendations consistent with the Australian Information Commissioner's submissions in this regard, that the Australian Information Commissioner has an express power to remit a matter for further consideration by the original decision-maker.⁴³

OIC recommends that OIC has a discretion to remit in certain circumstances, for example:

- where further searches instigated by OIC have located documents and a de novo decision regarding those documents is required

⁴⁰ Section 93(1)(b) of the RTI Act

⁴¹ Section 93 of the *Government Information (Public Access) Act 2009* (NSW)

⁴² Section 49L of the *Freedom of Information Act 1982* (Vic).

⁴³ Pages 30-31 and recommendation 4 of the Hawke Report.

- the agency decision/s addressed a jurisdictional or threshold issue and a de novo decision regarding substantive issue of access to the documents is now required.

OIC also recommends excluding, from both existing and any additional remittal powers, the requirement that an agency must apply for further time before OIC can remit.

OIC considers that including the power to remit for certain external reviews to agencies for decision would contribute to reducing demand for external review and the more efficient and effective use of government resources.

OIC recognises that the ability to remit part of a decision back to the agency and retain the remainder at external review could potentially cause confusion as a result of different review rights.

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?

***Recommendation:** OIC considers the current model of mandatory external review prior to right of appeal to QCAT is efficient and effective.*

When conducting an external review, OIC undertakes a merits review of the access application. OIC does not have a complaints function in relation to how the agency conducted itself in dealing with the access application as is available in some other jurisdictions (for example, Commonwealth, Victoria and New South Wales).

Currently, a participant in an external review may appeal an OIC decision to QCAT on a question of law only.⁴⁴ A judicial member of QCAT exercises the tribunal's appeal jurisdiction in such matters.⁴⁵ The option of judicial review remains open to external review participants⁴⁶(although none have exercised this option since commencement of the RTI Act and QCAT Act).

In OIC's view, QCAT's merits review of an agency's initial or deemed decision would be an inefficient use of QCAT's resources. For example, where sufficiency of search was at issue in the review, the applicant would not have had the opportunity to raise these issues with the agency. The sufficiency of an agency's searches is the second most commonly considered issue in OIC decisions. If applicants could appeal directly to QCAT, QCAT would, on a frequent basis, be required to engage with agencies to ensure that searches were sufficient in the same manner as OIC.

⁴⁴ Section 119(1) of the RTI Act.

⁴⁵ Section 119(4) of the RTI Act.

⁴⁶ Under part 3 of the Judicial Review Act 1991 (Qld).

OIC notes that there has been some suggestion that agencies simply provide QCAT with a declaration stating that they have conducted all relevant searches. However, in OIC's experience, due to, in many cases, the inadequacies of agency record keeping systems and search processes, most applicants would find this proposed solution unconvincing.

OIC has developed processes for efficiently and effectively, but comprehensively, ensuring that reasonable searches, consistent with agency obligations, are conducted. OIC staff have a good working knowledge of government business and record keeping requirements and practices, which facilitates this process.

Similarly, many external reviews involve large numbers of documents and issues. OIC staff have particular expertise in dealing with the provisions of the RTI Act and in utilising informal resolution techniques. These enable optimal results for the parties to the review by identifying key issues for each party and 'reality testing'—where OIC officers ensure that the views of each party accord with the reality of the Act—consistent with legislative requirements.

Appealing an agency's decision directly to QCAT may require QCAT to make de novo decisions, in the same context as OIC is often required to⁴⁷ regarding at least some of documents sought. In OIC's view this does not comprise an efficient use of QCAT's resources.

Where an external review is resolved by decision, the external review function is complemented by the assistance and support functions of the OIC, in particular, extensive online guidance which includes the annotated legislation. OIC is able to ensure that external review decisions are written in plain English, without an emphasis on technical aspects of the legislation, to assist applicants and third parties to understand the reasons for decision. OIC guidelines and annotated legislation present the technical aspects of OIC views on the application of the legislation, and are available for agency decision-makers and other interested parties, such as researchers in other jurisdictions, to draw on.

Such an approach is consistent with evolving community expectations about government in general, as recognised in a recent speech by the Australian Information Commissioner:⁴⁸

Complaint and investigation bodies, such as ombudsman and commissioners, now receive and conduct reviews in a more responsive, engaged, interactive and informal manner.

Tribunals and courts resolve an increasing proportion of applications by alternative dispute

⁴⁷ For example, because the decision was deemed, the decision did not address additional documents located as a result of further searches, or the decision dealt with jurisdictional or threshold issues only.

⁴⁸ Prof John McMillan, Australian Information Commissioner (2013), *Administrative Law in an Interconnected World*, AIAL National Administrative Law Forum, Canberra, 18 July 2013.

resolution rather than formal hearings and, as noted earlier, have embraced technology in the registry and the hearing room...

... it is questionable whether people will have the time and interest to wade through lengthy and complex reasons statements in order to understand the principles applied to resolve a dispute. Shorter, clearer, crisper reasons may be required. Equally, the statements of reasons in individual cases may have diminishing importance in developing administrative law principles and jurisprudence. Many people prefer the option of visiting an administrative justice agency's website to read a coherent and comprehensive set of guidelines that explain the principles to be applied from one case to the next.

Educational and precedent information, once available only in (sometimes quite lengthy or dense) decisions is now available in a number of different ways, suitable not only for decision-makers and reviewers, but also for applicants and members of the community.⁴⁹ As noted above, OIC produces extensive online resources that are used during the course of external reviews to explain technical aspects of the legislation to applicants, agencies, and third parties. This approach has proven to be a highly effective and efficient way to meet varying needs previously met only by complex external review decisions.

Wherever possible, OIC resolves reviews informally to maximise efficient use of public monies while providing effective outcomes for parties. In the 2015-16 financial year, 88% of external review applications were resolved informally⁵⁰ and 72% of applicants⁵¹ and 91% of agencies⁵² were satisfied with OIC's performance. Given that only a small number of reviews result in decisions, OIC's online resources play a critical role in capturing and communicating educational and precedent material drawn from OIC views formed in all external reviews, not just those resolved by formal decision.

OIC does not consider that enabling applicants and relevant third parties to appeal directly to QCAT, requiring QCAT to undertake significant merits reviews, is a more efficient and effective model than external review by OIC.

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

⁴⁹ For example, OIC produces a number of targeted guidelines to assist decision-makers dealing with applications, which may refer to OIC decisions, Annotated Legislation, or other OIC guidelines, with complementary information sheets intended for applicants receiving such a decision.

⁵⁰ Page 12 of OIC Annual Report 2015-16

⁵¹ Page 16 of OIC Annual Report 2015-16

⁵² Page 16 of OIC Annual Report 2015-16

Recommendation: *OIC submits that it does not require additional powers to obtain documents as part of its performance monitoring, auditing, or reporting functions*

Under section 131 of the RTI Act, the OIC has a range of performance monitoring functions, including the power to monitor, audit, and report on agencies' compliance with both the RTI Act and Chapter 3 of the IP Act. Since 2009, OIC has undertaken numerous performance monitoring activities, including Desktop Audits of agency websites, self-assessment activities, and agency specific audits. All of these activities have been reported to Parliament.⁵³ The OIC has not encountered a situation in conducting its performance monitoring and auditing functions which would have required or benefited from additional powers to obtain documents.

OIC submits that it does not require additional powers to obtain documents as part of its performance monitoring, auditing or reporting functions. The RTI Act contains sufficiently broad powers for OIC to carry out its functions under the Act including its performance, monitoring, auditing or reporting 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?

Recommendation *OIC recommends streamlining annual reporting requirements for agencies and submits that OIC enter into detailed discussions with the Department of Justice and Attorney-General regarding transferring responsibility for reporting to OIC.*

Under the RTI and IP Acts, agencies are required to report on their RTI and IP applications as set out in the RTI and IP Regulations.

OIC is a key user of the RTI and IP Act Annual Report data, primarily in its performance monitoring and reporting functions to:

- assess relative risk of agency non-compliance
- select agencies for compliance audit; and
- prepare desktop audit and other reports.

OIC also uses the RTI and IP annual report data to:

- assess agency throughput

⁵³ See list of Reports to Parliament here <<http://www.oic.qld.gov.au/about/our-organisation/key-functions/compliance-and-auditreports>>.

- identify application handling issues for individual agencies and broader trends, including areas in which agencies or the community require additional support; and
- identify opportunities to improve the administration of the RTI and IP Acts.

However, currency of available data significantly undermines the utility of such data; for example, OIC's 2015-2016 performance monitoring activities are based on the 2014-15 financial year data from the most recent Annual Report. OIC appreciates the work involved by agencies and the Department of Justice and Attorney-General in producing the Report, however the value of such effort is significantly diminished by the lack of currency of the data.

OIC recommends that the information agencies are required to report annually be revised to minimise administrative burden, improve utility of data, and facilitate timeliness of reporting.

OIC notes that in other jurisdictions the body equivalent to OIC collects and compiles data on the use of right to information. Western Australia, for example, requires the Information Commissioner's Annual Report to include specific data about the number and nature of applications dealt with by agencies under the Act during the year. To facilitate this, agencies are required to provide this data to the Information Commissioner. The Commonwealth Information Commissioner performs a similar function, collecting and compiling agency and Ministerial data relating to FOI applications received during the year.

Streamlining the reporting criteria

OIC is aware that annual reporting requirements can be onerous for agencies, particularly where agencies do not have efficient systems in place to collect and report on such data

In using the data, particularly in its performance monitoring functions, OIC has considered that some data currently required is neither useful nor necessary to enable the assessment of agency performance. For example, section 8 of the RTI Regulation requires agencies to report on the total number of times they rely on a refusal provision in Section 47(3) of the RTI Act. This is done on a 'by page' basis, i.e. the number of refusal provisions used on each page. OIC notes that in many cases a decision-maker will refuse access to a particular kind of information (for example, an individual's name) that appears multiple times in the documents.

OIC suggests that reporting on the total refusal provisions used for an application as a whole could significantly reduce the administrative burden for some agencies, as they could be drawn from the refusal provisions listed in the decision notice or agency's case management system, and increase the data's usefulness.

OIC suggests that it would be beneficial to require reporting on data relating to push model initiatives and proactive release of information, to reflect the emphasis of the RTI Act that applications are intended as a last resort. OIC also suggests that data on application brought forward, withdrawn, transferred or finalised and details of applications withdrawn or transferred be added to the Regulation's reporting requirements to increase the accuracy and utility of data.

OIC notes streamlining the reporting requirement will require amendment to the classes of information currently specified in the Regulation for inclusion in the Annual Report.

Privacy Complaint reporting

OIC notes that it is required to report on the number of privacy complaints received and the outcome of those privacy complaints dealt with by the Commissioner.⁵⁴ However, OIC notes there is no corresponding requirement placed on Ministers or agencies to report on the number of privacy complaints received and the outcome of those complaints. As noted previously, OIC relies on RTI and IP Act Annual Report data for the performance of its statutory functions, particularly its statutory performance monitoring and support functions. Under the IP Act, OIC's performance monitoring and reporting functions include conducting compliance audits to assess relevant entities' compliance with the privacy principles and conducting reviews into personal information handling practices of relevant entities.⁵⁵

OIC suggests that data on the numbers of privacy complaints made to agencies, including the outcome of these complaints, be added to the Regulation's reporting requirements.

External review reporting

Agencies are required to report on details of external review applications made from their decisions, including the number of applications, whether they were preceded by an internal review, and how the decision made on external review compared with the decision made by the agency.⁵⁶

OIC notes that it is required to report on external review matters received and decisions made by the Commissioner.⁵⁷ Having OIC report on external review data instead of agencies would provide greater efficiency, reduce the administrative burden reporting places on agencies, and limit the potential for inaccurate or inconsistent data.

⁵⁴ Section 5 of the *Information Privacy Regulation 2009*

⁵⁵ Section 135(1)(a)(i) and 135(1)(b)(iii) *Information Privacy Act 2009*

⁵⁶ Section 8 of the *Right to Information Regulation 2009* and Section 6 of the *Information Privacy Regulation 2009*

⁵⁷ Section 7 of the *Right to Information Regulation 2009* and Section 5 of the *Information Privacy Regulation 2009*.

OIC recommends that alternative approaches to collection and reporting of data be investigated to ensure data is available online as soon as possible after each financial year, consistent with the push model and open data initiatives.

OIC submits that alternative approaches could include providing OIC with additional resources to assume responsibility for collecting and compiling data from agencies for the purposes of producing the RTI and IP Act Annual Report. This approach is consistent with other jurisdictions and would result in greater efficiencies, reduce the administrative burden on agencies, and limit the potential for inaccurate or inconsistent data.

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?

***Recommendation:** OIC recommends amalgamating the IPPs and the NPPs to create a single set of privacy principles that align with the APPs to the extent of their relevance to the Queensland jurisdiction*

Adopting a single set of privacy principles in Queensland would ensure consistency of privacy obligations across all Queensland government agencies.

Currently, the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) create two separate sets of privacy obligations and privacy rights under the IP Act. The NPPs apply to health agencies; the IPPs apply to all other agencies. OIC also notes that the IPPs apply to personal information contained in a document while the NPPs apply to all personal information, regardless of whether or not it is contained in a document.

Further, OIC notes there is a lack of consistency between the privacy principles in the IP Act and the APPs. The Australian Law Reform Commission (ALRC) has recommended harmonised privacy principles across Australian jurisdictions.

The existence of two different sets of principles also impacts on contracted service providers. Under Chapter 2, part 4 of the IP Act contractors can be bound to comply with the privacy principles. Health agencies bind their contractors to the NPPs; all other agencies bind their contractors to the IPPs. This means different obligations will apply to the contractor depending on which agency with whom they contract.

OIC considers that a single set of privacy principles which applied to all Queensland government agencies would eliminate these issues. As part of simplifying compliance, OIC suggests that section

33, which is a privacy principle as defined in schedule 6 of the IP Act, be included in the single set of privacy principles, rather than remaining as a section in chapter 2.

The APPs grew out of recommendations made by the ALRC in Report 108; *For Your Information: Australian Privacy Law and Practice* (the Report), which was the culmination of a twenty-eight month inquiry into the Commonwealth Privacy Act. This inquiry considered the extent to which the Commonwealth Privacy Act and related laws provided an effective privacy protection framework for Australia and canvassed the issue of national consistency.

The threshold issue considered by the ALRC was whether or not national consistency was important. Numerous stakeholders submitted to the review that it was, identifying the inconsistency of privacy regulation of the private sector, including the private health sector, as the cause of unnecessary compliance burden and expense.

Aligning amalgamated IPPs and NPPs with the APPs has a number of advantages including greater national consistency in privacy regulation. As noted by the ALRC, 'inconsistency and fragmentation in privacy regulation causes a number of problems, including unjustified compliance, burden and costs, impediments to information sharing and national initiatives, and confusion about who to approach to make a privacy complaint'.

OIC recommends consolidating the IPPs and NPPs to create a single set of privacy principles aligned to the APPs to the extent of their relevance to the Queensland jurisdiction. OIC notes that the APPs are intended to apply to a broader range of entities, including private entities with a turnover in excess of three million dollars per year, health care providers and Commonwealth government agencies. In contrast, Queensland's IP Act applies only to Queensland government agencies.

The Territory Privacy Principles (TPPs) contained in Schedule 1 of the Information Privacy Act 2014 (ACT) may provide a useful model. The TPPs commenced on 1 September 2014. The TPPs apply to ACT public sector agencies and contracted service providers (including subcontractors), but only to the extent they perform obligations under a government contract.

The TPPs are similar to the APPs however those APPS not relevant to regulation of information privacy by ACT public sector agencies have not been included in the TPPs. The TPPS also contain minor textual differences to the APPs which do not change the intended meaning of the principles.

As part of simplifying compliance, OIC further recommends that section 33 (transfer of information outside Australia), be included in the single set of privacy principles, rather than remaining as a section in chapter 2 of the IP Act modelled on APP8 (cross-border disclosure of personal information) of the Commonwealth Privacy Act (Refer to response to Q27).

In the short-term, amalgamating the IPPs and the NPPs to align with the APPs is likely to place an increased administrative and financial burden on agencies to implement a revised set of privacy principles across agencies. However, OIC considers harmonised privacy principles are likely to result in reduced compliance costs and administrative burden on agencies in the longer term due to greater national consistency in privacy regulation.

Schedule 1: documents but not information

Schedule 1 of the IP Act lists documents to which the privacy principles do not apply. These are documents which arise out of the specific situations set out in Schedule 1. For example, Schedule 1, section 3 of the IP Act excludes a document to the extent it contains personal information arising out of a complaint under the *Police Service Administration Act 1990*, part 7 or a complaint, or an investigation of misconduct, under the *Crime and Corruption Act 2001*. To be excluded under this section the document must have arisen out of the complaint investigation; only the document, not the personal information within it, is excluded from the privacy principles. This creates the situation where information extracted from the excluded document is once again subject to the privacy principles. An obvious example of this is verbal communications such as interviews and conversations, which because the exchange is not in documented form, do not fall under the exemption in Schedule 1.

OIC suggests that schedule 1 be amended to clarify that it is the personal information which arises out of these situations, rather than the documents, to which the privacy principles do not apply.

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

***Recommendation:** OIC supports national consistency in privacy laws where possible and practicable. OIC recommends that the definition of 'personal information in the IP Act should be the same as the definition in the Commonwealth Act provided there are no unintended consequences for the RTI Act.*

The definition of personal information in the IP Act is 'information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion'.

The Commonwealth Privacy Act defines personal information as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

OIC supports national consistency in privacy laws where possible and practicable. OIC considers that amending the definition of personal information to replicate the Commonwealth definition would not significantly change the scope of what is considered to be personal information in Queensland for the purposes of privacy principles. Accordingly OIC recommends that the definition of ‘personal information’ in the IP Act should be the same as the definition in the Commonwealth Privacy Act, provided there are no unintended consequences for the RTI Act.

The definition of personal information in the IP Act is not only used for the privacy principles. It is also used for Chapter 3 of the IP Act, which contains access and amendment rights, and for the purposes of the RTI Act.

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?

***Recommendation:** OIC does not consider that the IP Act inappropriately restricts the sharing of information and does not support modifying the existing exceptions or adopting a ‘use’ model within government. OIC considers the NZ model for Approved Information Sharing Agreements may provide a useful model to facilitate the sharing of information between or within agencies for the purposes of delivering public services*

The IP Act creates a right for individuals to access and amend their own personal information and provides rules or ‘privacy principles’ that govern how Queensland government agencies collect, store, use and disclose personal information. These principles support the flow of personal information where it is necessary or directly related to fulfil the function or activity of the agency.

It is OIC’s view that the IP Act does not act as a barrier to information sharing, rather it provides a framework to facilitate the appropriate sharing of personal information. These rules are set out in the Information Privacy Principles, National Privacy Principles, and Chapter 2 of the IP Act. OIC’s experience is that the privacy principles have sufficient flexibility to allow the flow of information for legitimate purposes. The capacity of OIC to grant applications for waiver and modification (see following discussion) caters for exceptional circumstances.

Waiver and modification

Section 157 of the IP Act allows an agency to apply to OIC for a waiver or modification of the privacy principles in situations where the principles are preventing an agency’s activities. In order to be granted, non-compliance, or complying in a different way, with the privacy principles must outweigh the public interest in complying with the privacy principles as they appear in the IP Act.

Since July 2009, OIC has received only six formal applications under section 157 for a waiver of the privacy principles. All of these applications were made because the agency considered that it was in a unique situation which could not be reconciled with the existing privacy principles. Decisions giving an approval for a waiver or modification of privacy principles are published on OIC's website.

The IP Act does not limit the entities with whom information can be shared. Rather, it regulates the situations in which information can be shared. The circumstances in which an agency is permitted to share personal information with a third party include the following:

- Where it is necessary for law enforcement activities.
- Machinery of Government changes brought about by an Administrative Arrangements Order or other legislation.
- Minimising threats to individuals or to the public, such as dealing with emergency or disaster situations.
- Briefing Ministers in relation to their portfolio responsibilities.
- Responding to or discussing personal information published by the individual.
- Where the individual consents to the sharing or was made aware when the information was collected that the information sharing was going to occur.
- Where the sharing is authorised or required by law.

Notwithstanding commonly-held misconceptions about privacy, OIC submits that a range of factors other than privacy prevent information being shared by government such as risk-aversion, cultural and organisational factors, and legislated confidentiality and secrecy provisions restricting or prohibiting the use or disclosure of personal information, many of which contain criminal sanctions in the event of a breach.

The IP Act relies on a set of rules or principles to regulate the management of personal information to allow flexible application to a broad range of situations as opposed to detailed rules prescribed in a legislated information sharing framework. Overly prescriptive legislated information sharing provisions may have the unintended consequence of prohibiting the flow of information due to a lack of flexibility in responding to situations not contemplated by the legislation.

It is OIC's experience that the privacy principles have sufficient flexibility to allow the flow of information for legitimate purposes and appropriately balance the information privacy rights of individuals with other public interests and does not support the inclusion of additional exceptions. Further exceptions are likely to result in weakening of the privacy regulatory regime in Queensland.

OIC notes the Consultation Paper proposes adopting a 'use' model within government whereby the sharing of information is regarded as a 'use' of information rather than a 'disclosure'. OIC does not support this proposal. The concepts of 'use' and 'disclosure' have a defined meaning for the purposes of the privacy principles and are fundamental to the application of the IP Act. Modifying the meaning of these concepts for application to a specific context, such as the sharing of information within government, is likely to lead to confusion and inconsistency with privacy legislation in other jurisdictions.

OIC notes that Part 9A of the *Privacy Act 1993* (NZ) provides for Approved Information Sharing Agreements (AISAs). An AISA is a legal mechanism that authorises the sharing of information between or within agencies for the purposes of delivering public services. Information sharing agreements are approved by Order in Council.

Published guidelines on AISAs by the NZ Privacy Commissioner note the following:

- An AISA authorises agreed departures from the privacy principles (except principles 6 and 7 – access and correction rights) if there is a clear public policy justification and the privacy risks of doing so are managed appropriately. Non-government agencies can be involved, but the AISA has to be linked to a public service mandate and must involve a government department as the 'lead agency'.
- An AISA does not provide an exemption from the Privacy Act – the Act continues to apply although in a modified form. Individuals whose information is shared may raise complaints with the Privacy Commissioner. An AISA cannot override any statutory prohibition on information sharing – legislative amendment is required to resolve a statutory impediment.
- AISAs are listed in Schedule 2A of the Privacy Act. The lead agency for the AISA must publish a copy of the agreement online, and must report on activity as specified by the Privacy Commissioner (s96U).
- The Privacy Commissioner may publish a report about an AISA or the consultation process relating to that agreement (section 96P). The Privacy Commissioner may on his or her own initiative, conduct a review of the operation of an AISA (s96W) and may report to the relevant Minister on the findings of the review (section 96X).

While OIC does not consider the IP Act inappropriately restricts the sharing of information, OIC considers the adoption of the NZ model for approved information sharing arrangements, including appropriate legislative oversight by the Privacy Commissioner, may address some of the current identified issues with information sharing.

OIC notes a similar scheme is provided for in the *Victorian Privacy and Data Protection Act 2014*. Division 6 of this Act provides for an Information Usage arrangement (IUA). An IUA is an arrangement that sets out acts or practices for handling personal information for public purposes where any of the acts or practices modify the application of an IPP (other than IPPs 4 and 6), provides that the practice does not need to comply with a specified IPP (other than IPPs 4 and 6) and/or permits handling of personal information for the purposes of an information handling provision. An IUA may only be approved by relevant Ministers, provided the Commissioner has first approved the draft IUA.

In order to approve an IUA, the Commissioner must be satisfied that the public interest in the organisation handling personal information in the way specified by the IUA substantially outweighs the public interest in complying with the specified IPP or code.

OIC's preferred model is the information sharing framework provided for in the NZ legislation. OIC notes there are some limitations to this model. While AISAs are an enabling tool to allow agencies to collaborate and share information, an AISA does not override any statutory prohibition on information sharing. Further, an AISA does not compel an agency to share information, rather it provides the mechanism to permit an agency to share information.

As noted in OIC's Annual Report 2015-16, sharing of personal information held by government agencies with other government agencies and other entities continues to be a key issue.

Increasingly agencies seek to address perceived barriers in information sharing in the IP Act through legislative amendment. In some instances, this leads to a weakening of privacy protections afforded to individuals by the IP Act.

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?

***Recommendation:** OIC recommends amending section 33 to regulate 'disclosure' of information out of Australia rather than 'transfer' outside Australia. OIC also recommends incorporating section 33 of the IP Act into a unified set of privacy principles.*

Agencies are required to comply with all the privacy principles. This means that the obligation to comply with section 33 is in addition to the obligation to comply with the IPPs or the NPPs.

Section 33 of the IP Act regulates the transfer of personal information out of Australia. Any transfer of personal information must comply with these rules or the transfer will be a breach of the obligation to comply with the privacy principles.

The word 'transfer' is not defined in the IP Act. The Macquarie Dictionary defines transfer as, relevantly, to convey or remove from one place, person, etc to another. As such, personal information will be transferred out of Australia when the information travels from Australia to another country. OIC considers that the broad meaning of the word 'transfer' creates unnecessary complexity for agencies and leads to outcomes potentially not contemplated by the legislation at the time of enactment of the IP Act. OIC submits that this is due, in part, to rapid technological change which has significantly altered the speed and means by which government information can be disseminated. It is noted that in 2009 when the RTI and IP Acts came into force, contemporary technological mainstays such as smartphones, tablets, ubiquity of cloud services and social media were either yet to be introduced into mainstream society or were in their infancy. Every time that a Facebook posting is made, every time a Google search takes place – personal information is transferred overseas.

The term 'disclosure' is defined in section 23(2) of the IP Act: information is disclosed if the entity the information is being given to does not know it and is not in a position to find it out and the agency ceases to have control of the information. OIC recommends amending section 33 to regulate the 'disclosure' rather than 'transfer' of personal information outside of Australia. This would remove the apparent absurdity where information that is in the public domain in Australia – and so could not qualify under the definition of 'disclosure' in section 23(2) - can still nonetheless be 'transferred overseas' in potential breach of section 33.

OIC recommends further amendments to section 33 modelled on APP 8 in the Commonwealth Privacy Act.

The *Commonwealth Privacy Amendment (Enhancing Privacy Protection) Bill 2012* amended the Commonwealth Privacy Act to substitute disclosure for transfer in its equivalent provision to section 33 to implement the government's response to recommendations contained in the 2008 report of the Australian Law Reform Commission (ALRC), "*For Your Information: Australian Privacy Law and Practice*". APP 8 regulates the 'disclosure' of personal information to overseas recipients replacing NPP 9 which restricted the 'transfer' of personal information overseas.

As noted by the Office of the Australian Information Commissioner (OAIC), the privacy protections in the Commonwealth Privacy Act 'recognises the global interdependence of today's economy, underpinned by the flow of information, including personal information, across national borders. At the same time, cross-border transfers of personal information are known to be a source of significant community concern. OAIC further notes, that 'the framework provided by the Privacy Act

addresses the balance between this community concern and the need to send personal information overseas for legitimate business purposes’.

OIC notes that APP 8 and s16C apply when an APP entity discloses personal information overseas. These two provisions read together create a framework for the cross-border disclosure of personal information where the disclosing entity remains accountable for the subsequent handling of that personal information by the overseas recipient i.e. the disclosing entity will be liable if the overseas recipient handles the information in a way that would breach the APPs. This liability can occur even if an APP entity takes reasonable steps to ensure that the overseas recipient. This is currently not provided for in section 33.

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

***Recommendation:** OIC recommends amending the Act to remove the 45 business day time frame before complaints can be brought to OIC and replace it with a discretion to accept privacy complaints based on specific circumstances*

Under section 166(3) of the IP Act before a complainant can bring their privacy complaint to OIC they must give the agency a minimum of 45 business days, to deal with the complaint to the complainant’s satisfaction.

OIC has identified a number of issues with the current lack of flexibility in the IP Act about the timeframe for complaints to OIC to be lodged. For example, an agency complainant who is dissatisfied with the agency’s response to their privacy complaint must, despite the agency having expeditiously (from the agency’s perspective) dealt with their complaint, wait out the remainder of the 45 business day period before they can bring their complaint to OIC. A complainant who fails to do so will have their complaint declined by OIC and will be advised that they must re-lodge at the 45 business day mark. To this extent a complainant suffers a ‘time penalty’ from the fact that the agency quickly dealt with their complaint.

It is OIC’s view that complainants who have received a final response from the agency should not be asked to wait until the 45 day period has expired before bringing their privacy complaint to OIC.

In the alternative, sometimes 45 business days is an insufficient amount of time in which to deal with some complaints. In these cases, a complainant could prematurely lodge their complaint with OIC on the 45 business-day mark.

OIC recommends giving OIC the discretion to accept or decline complaints based on how the agency is dealing with the complaint rather than by reference to an arbitrary time period.

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

***Recommendation** OIC recommends placing on time limit of twelve months within which a complainant can request OIC refer a privacy complaint to QCAT if OIC is unable to mediate the privacy complaint*

Section 176(1) of the IP Act provides that the Information Commissioner must refer the privacy complaint to QCAT, if asked to do so by the complainant, within 20 business days after being asked to refer it. As noted in the Consultation Paper there are no time limits on when a complainant may request OIC refer a privacy complaint to QCAT.

While OIC notes that lack of a specified time limit has not created any issues to date, OIC submits consideration be given to amending the IP Act to place a time limit of twelve months within which a complainant can request OIC refer a privacy complaint to QCAT if OIC is unable to mediate the privacy complaint. The imposition of a time limit will provide for timely resolution of privacy complaints and prevent a situation from arising where a complainant requests OIC refer a privacy complaint to QCAT several years later.

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

***Recommendation:** OIC considers the IP Act provides sufficient powers for the Information Commissioner to investigate matters potentially subject to a compliance notice under the IP Act.*

The IP Act gives the Information Commissioner the power to issue a compliance notice where there has been a serious or a flagrant breach of the obligation to comply with the privacy principles, or a breach which has occurred five times in the preceding two years.

Under section 197 of the IP Act, if the Information Commissioner is satisfied on reasonable grounds that a person has information relevant the Commissioner's decision to give an agency a compliance notice, the Commissioner may give the person a written notice requiring the person to:

- give the information to the Information Commissioner in written form, or
- attend before the Information Commissioner to answer questions.

The Information Commissioner may administer an oath or affirmation to attend before the Commissioner and may examine the person on oath or affirmation.

Further, section 187 of the IP Act provides that if a person given notice under s197 fails to give information, produce a document or attend before the Information Commissioner without reasonable excuse, a maximum penalty of 100 penalty units applies.

There are very few limitations placed on what the Information Commissioner can require an agency to do in a compliance notice. Section 158(2) sets out that the compliance notice may require an agency to take a stated action, within a stated period, for the purposes of ensuring compliance with the obligation. Section 160 of the IP Act states that an agency that is given a compliance notice must take all reasonable steps to comply with the notice. The maximum penalty for non-compliance is 100 penalty units.

As noted in the Consultation Paper, the Information Commissioner's investigative powers for its external review functions permit the Information Commissioner to obtain access to all documents of an agency or Minister, requires agencies or Ministers to conduct searches, examine witnesses, and require information, documents and attendance. OIC considers that section 197 of the IP Act provides similar powers to the investigative powers of the Information Commissioner for its external review functions. For example, Section 197 provides the power to require information, documents and attendance including the power to administer an oath or affirmation and examine the person on oath or affirmation.

OIC notes that it has not issued a compliance notice since enactment of the IP Act. OIC considers it has sufficient powers to investigate matters potentially subject to a compliance notice under the IP Act and does not consider further amendments are necessary.

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

***Recommendation:** OIC recommends clarifying the definition of 'generally available publication'. OIC considers the Commonwealth definition provides a useful model. As noted previously, OIC supports national consistency in privacy regulation*

Schedule 1 of the IP Act lists documents to which the privacy principles do not apply. Section 7 includes generally available publications. A generally available publication is defined in schedule 5 as 'a publication that is, or is to be made, generally available to the public, however it is published'. OIC supports providing greater clarification of the definition of 'generally available publication' in Schedule 5 of the IP Act.

OIC notes that for the purposes of the Commonwealth Privacy Act, 'generally available publication' means a magazine, book, article, newspaper or other publication that is, or will be, generally 'available to members of the public:

- (a) whether or not it is published in print, electronically or in any other form; and
- (b) whether or not it is available on the payment of a fee.

The definition in the Commonwealth Privacy Act is technology neutral and explicitly states that a publication is a generally available publication where or not payment of a fee is required to access it. As noted previously, OIC supports national consistency in privacy laws where possible. OIC submits that the Commonwealth provision may provide a useful model for proposed amendments to the existing definition of 'generally available publication' in the IP Act.

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?

***Recommendation:** OIC recommends amending IPP 4 to require an agency to take reasonable steps to protect information. OIC suggests that this could best be achieved by amending IPP 4 to mirror NPP 4. OIC notes that this issue would be resolved by unifying the IPPs and NPPs into single set of privacy principles.*

IPP 4(1)(a) currently requires an agency that controls a document containing personal information must ensure that information is protected against loss, unauthorised access, use, modification or disclosure, and any other misuse. IPP 4(2) expands on this definition by requiring the protections in IPP 4(1) to include security safeguards adequate to provide the level of protection that could reasonably be expected to be provided. While IPP 4(2) introduces a level of reasonableness in relation to the security safeguards, IPP 4(1) has no explicit reasonableness test.

OIC also notes that this obligation is not consistent with the obligation on health agencies in NPP 4, which requires a health agency to take reasonable steps to protect information, and health agencies are highly likely to hold extremely sensitive information.

OIC recommends that IPP4 is amended to provide that an agency must take reasonable steps to ensure information is protected against loss and misuse. OIC notes that this issue would be addressed by adopting a single set of privacy principles in the IP Act modelled on the APPs in the Commonwealth Privacy Act (to the extent of their relevance).

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

Recommendation: OIC recommends amending IPP 2(2) to omit the words ‘asks the individual’ and replace them with the wording from NPP 1: ‘collects personal information about the individual from the individual’. OIC also suggests making the same amendment to IPP 3(2). OIC notes that should other recommendations regarding amalgamating the IPPs with the NPPs into a single set of privacy principles be accepted, this issue will largely be addressed. As noted previously, OIC supports a unified set of privacy principles that align with the APPs to extend of their relevance to the Queensland jurisdiction

Information Privacy Principle 2 (IPP 2) requires an agency to provide certain information to an individual when it asks that individual for their personal information. Conversely, National Privacy Principle 1 (NPP 1) requires health agencies to provide certain information to an individual when it collects personal information about the individual from the individual.

The use of the word ‘asks’ in IPP 2(2) has created confusion amongst agencies about when the requirements in IPP 2 apply. One interpretation is that IPP 2 applies only when an agency actively obtains information on a personal level. Another interpretation is that it also includes indirect collection, for example through an online agency forms. A broader interpretation is that IPP 2 applies to any collection of information from the individual, including purely passive collections such as CCTV recording.

It does not appear to be consistent with the objects of the IP Act that personal information would be covered by IPP 2 if an officer hands an individual a form and asks them to fill it out, but would not apply to the same form discovered online and completed by the individual.

OIC notes that NPP 1, which governs collection of personal information by health agencies, does not present this issue as it refers to collection rather than using the word ask.

This confusion creates uncertainty for agencies, individuals, and the OIC, particularly in relation to its monitoring and support functions. Additionally, OIC considers that it is appropriate that privacy protections apply to all personal information collected from individual by an agency, regardless of the agency which collects it or the circumstances under which the information was collected.

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

RTI ACT

- **Processing Period** – OIC recommends simplifying the provisions regarding the time an agency has to make a considered decision. For example, this may include:

- a. Single processing period which is extended to include any further period in which the agency is entitled to continue working on an application i.e. replace concept of further specified time with an extension of the processing period
- b. Allow the agency to make a considered decision provided that the agency reasonably believes the applicant would agree, or has agreed to further time i.e. if they ask for an extension after the processing period has ended, and the applicant agrees.
- c. Extend the timeframe for deciding that a document or entity is outside the scope of the Act from 10 business days to the processing period that applies to other types of decisions under the Act.

Minor and Technical Amendments:

- Section 119(5) of the RTI Act provides that an appeal to QCAT on a question of law may only be by way of rehearing. It is readily apparent to OIC why this provision was drafted to include the re-hearing requirement. OIC suggests reviewing this provision to ensure continued relevance of the re-hearing requirement.
- Section 107 of the RTI Act places an obligation on the Information Commissioner to ensure proper disclosure and return of documents. This section was drafted at a time when copies of documents were provided to OIC in hard copy form and the electronic transmission of documents was not contemplated. OIC receives copies of documents electronically and these documents are not reduced to a hard copy. Further, OIC does not hold original copies of documents. OIC recommends updating this provision to provide for the electronic transmission of documents. OIC further recommends providing greater flexibility in this provision to allow OIC to destroy documents when an external review matter is finalised and any applicable review periods have passed.

IP ACT

In addition to those matters outlined above, OIC considers a contemporary legislative framework to manage new and emerging privacy risks and provide the appropriate balance between protecting personal information and continued innovation and growth in Queensland's transition to a knowledge economy requires the following key elements:

- a) **Provision of suitable powers for the Privacy Commissioner to make preliminary inquiries**

Section 167 of the IP Act provides that the Information Commissioner may make preliminary inquiries and the respondent for a privacy complaint to decide whether the commissioner is authorised to deal with the privacy complaint and whether the commissioner may decline to deal with the complaint. This provision, as currently drafted, restricts OIC's ability to undertake broader inquiries of other persons the Information Commission considers may have information relevant to the privacy complaint.

OIC submits section 167 of the IP Act is limiting and recommends providing the Privacy Commissioner with broader powers to request any person to provide information or assistance when undertaking preliminary inquiries. OIC further recommends imposing timeframes on parties, i.e. the complainant and agency, to respond to requests for information or assistance. Broadening the existing powers provided by section 167 of the Act for the purposes of making preliminary inquiries is consistent with other jurisdictions.

OIC notes that relevant provisions in the Commonwealth Privacy Act provides the Commissioner, for the purposes of undertaking preliminary inquiries with the power to make inquiries of the respondent or any other person. This provision is similar to section 38 of the *Information Privacy Act 2014* (ACT) which provides that the Information Privacy Commissioner may make inquiries of the respondent for a privacy complaint, or any other person, for the purpose of deciding whether to deal with the complaint. Section 68 of the Victorian *Privacy and Data Protection Act 2014* provides the Commissioner with the power to require a person information of documents if the Commissioner has reason to believe that a person has information or a document relevant to a conciliation.

The NSW *Privacy and Personal Information Protection Act 1998* provide the Privacy Commissioner, when undertaking inquiries and investigations, with the powers conferred on Royal Commissions.⁵⁸

OIC recommends amending section 167 of the IP Act to provide the Privacy Commissioner with suitable powers to make preliminary inquiries under the IP Act.

b) Mandatory Data Breach Notification

The *Privacy Amendment (Notifiable Data Breaches) Bill 2016* was introduced into Federal Parliament on 19 October 2016. If passed, the Bill will amend the Commonwealth Privacy Act to require agencies, organisations and certain other entities to provide notice to the Australian Information Commissioner and affected individuals of an eligible data breach. The introduction of mandatory data breach notification for those entities currently subject to the Commonwealth Privacy Act sets an important precedent for State and Territory privacy legislation.

⁵⁸ Section 38(1)

While entities subject to the Commonwealth Privacy Act are currently subject to a requirement to protect personal information from misuse, interference and loss, unauthorised access, modification and disclosure under APP11 they are not subject to a mandatory data breach notification requirement under the Commonwealth Privacy Act.

In a submission to the Australian Government's Serious Data Breach Notification Consultation, OIC provided in principle support for a legislated mandatory data breach notification scheme by the Australian Government. OIC noted that the introduction of a mandatory data breach notification scheme serves to strengthen the existing regulatory framework and brings Australia into line with other jurisdictions, including the EU and the new GDPR regulation, the United Kingdom and the United States.

In addition to allowing affected individuals to take remedial steps to lessen the adverse consequences that may arise from a data breach, data breach notification is an important transparency measure for governments. Governments collect and hold vast amounts of personal information on behalf of its citizens and citizens trust that Governments will protect this information from unauthorised access, use and disclosure. Increasingly, this information is held digitally posing significant implications for an individual's privacy in the event of a data breach.

Openness and transparency is an important mechanism for building trust and confidence in government. Given the significant economic and reputational costs associated with data breaches, it is OIC's view that entities may be reluctant to report data breaches unless mandated to do so.

Queensland's privacy principles include obligations which require agencies (and bound contracted service providers) to protect the information they hold from misuse, loss, and from unauthorised access, modification or disclosure. The IP Act also obliges agencies to safeguard the privacy of personal information when transferring information out of Australia. However, the IP Act does not require agencies to notify either affected individuals or the Information Commissioner of a privacy breach.

Queensland State Government agencies have obligations to report information security incidents to the Queensland Government Chief Information Officer as part of the IS18 Information security incident reporting requirements.

OIC also encourages agencies under the IP Act to incorporate data breach notification into its information management processes as a responsible business practice and to communicate with the Queensland Privacy Commissioner when incidents of data breach occur.

To date, only a small number of Queensland State Government agencies and their contracted service providers have reported data breach notifications to the OIC. However, in the absence of reliable data and a legislative framework mandatory reporting of data breaches, it is difficult to state with any certainty the actual number of data breaches in Queensland.

OIC recommends the IP Act be amended to provide for a mandatory data breach notification scheme in Queensland, modelled on the relevant provisions in the proposed Commonwealth Privacy Act amendments to the extent of their relevance to the Queensland jurisdiction. OIC proposes that agencies be mandated to report data breaches to the Privacy Commissioner and the Queensland Government Chief Information Officer.

OIC considers the inclusion of mandatory data breach provisions are important mechanisms for enhancing the regulatory privacy framework of the IP Act to respond to a range of contemporary privacy related risks posed by increased information sharing and technological advances in data analytics including the speed at which large volumes of data can be processed. OIC further considers that mandatory data breach notification will align Queensland with other national and international jurisdictions.

c) Privacy Commissioner Own Motion Powers

OIC notes that the Commonwealth Privacy Act provides that in addition to the Commissioner's power to investigate an act or practice when a complaint has been made (s40)(1)), the Commissioner can also investigate an act or practice on his or her own motion where the Commissioner considers it desirable that the act or practice be investigated (s40(2)).

Own motion investigation powers allow the Commissioner to conduct an investigation without any prior complaint being made (section 40(2)). The exercise of 'own motion powers' is beneficial when used in this context as a means of addressing systemic issues. As noted by the ALRC 'in order to make such investigations effective as a compliance tool, however, it is important that the Commissioner have adequate means to enforce remedies' in the event of a breach.

The IP Act gives the Information Commissioner the power to issue a compliance notice where there has been a serious or a flagrant breach of the obligation to comply with the privacy principles, or a breach which has occurred five times in the preceding two years. As noted previously, section 197 of the IP Act provides the Information Commissioner with the power to compel information if satisfied on reasonable grounds that a person has information relevant to the Commissioner's decision to give an agency a compliance notice.

An agency must comply with a compliance notice, but can appeal against the decision to issue the compliance notice to the Queensland Civil and Administration Tribunal (QCAT).

OIC notes however that the IP Act sets a high threshold for the issuing of a compliance notice limiting the range of circumstances in which the Information Commissioner can investigate an act or practice.

Amending the IP Act to provide the Privacy Commissioner with an 'own motion power' to investigate an act or practice, whether or not a complaint has been made, will strengthen the existing powers in the IP Act to identify and address any systemic issues arising out an act or practice of an agency.

d) Representative Actions

Section 164(1)(a) of the IP Act provides that an 'individual' can complain about an act or practice of an agency in relation to the individual's personal information that is a breach by the agency of their obligation to comply with the privacy principles.

The definition of 'individual' in the *Acts Interpretation Act 1954* (Qld) is 'a natural person'.⁵⁹ A natural person can only be a living person. The IP Act does not contemplate representative actions whereby an individual can make a complaint on behalf of other individuals similarly affected by a privacy breach.

Section 57(3) of the *Victorian Privacy and Data Protection Act 2014* provides that in the case of an act or practice that may be an interference with the privacy of two or more individuals, any one of those individuals may make a complaint on behalf of all of the individuals with their consent.

A similar provision exists in the ACT whereby section 34 of the *Information Privacy Act 2014* provides that if there is a claim of an interference with the privacy of two or more individuals, any of those individuals may make a claim on behalf of all the individuals. OIC notes that the ACT differs from the Victorian provision as there is no consent requirement.

OIC submits consideration is given to amending the IP Act to provide for representative privacy actions modelled on the provisions in the Victorian and ACT legislation.

Role of OIC at QCAT

The IP Act does not currently provide a right for the Privacy Commissioner to be appear and be heard in privacy matters before QCAT.

⁵⁹ Schedule 1, *Acts Interpretation Act 1954*

OIC notes that other privacy jurisdictions including NSW and Victoria provide either a right for the Privacy Commissioner to appear and be heard or joined as a party to proceedings. The NSW Privacy Commissioner is notified of applications to New South Wales Civil and Administrative Tribunal (NCAT) and has a right to appear and be heard in privacy matters before⁶⁰ The Victorian legislation provides that the complainant and respondent are the parties to the complaint. The Commissioner for Privacy and Data Protection may be a party if the Victorian Civil and Administrative Tribunal (VCAT) decides to join the Commissioner, or the Commissioner seeks to be joined.⁶¹

OIC suggests consideration is given to amending the IP Act to provide a right for the Privacy Commissioner to assist the court in a role such as an amicus curiae, where the Commissioner considers it appropriate, and with the leave of the court. The Privacy Commissioner could then assist the Court by providing a submission on a point of law or fact relevant to the privacy complaint or the privacy jurisdiction.

Complainants often find the privacy jurisdiction challenging given the 'principles' based nature of the legislation, leading to an inability for the complainant to clearly articulate the subject matter of the privacy complaint to QCAT. It is OIC's experience that complainants are often not legally represented in matters at QCAT creating further difficulties for less sophisticated complainants appearing at QCAT. Through the performance of OIC's statutory functions, OIC has built up considerable knowledge and expertise with regards to the privacy jurisdiction and continues to provide expert authoritative advice on privacy related matters in Queensland.

Providing a role for OIC at QCAT is consistent with other privacy jurisdictions.

e) Other

Clarification of operation of Section 7(2) of the IP Act

OIC is aware of a reported lack of clarity out the operation of section 7(2) of the IP Act leading to confusion by agencies about the interaction of the IP Act with the other legislation

Section 7(2) of the IP Act provides that the IP Act is intended to operate subject to the provisions of other Acts relating to the collection, storage, handling, access, amendment, management, transfer, use and disclosure of information.

⁶⁰ Section 55(6) *Privacy and Personal Information Protection Act 1988*

⁶¹ Section 74, *Privacy and Data Protection Act 2014*

While OIC does not consider the operation of section 7(2) of the IP Act is unclear, should further clarification be considered necessary, OIC recommends modelling any amendments to section 7(2) on the relevant provision in the Victorian legislation.

Section 6 of the *Privacy and Data Protection Act 2014* (Vic) states:

Relationship of this Act to other laws

(1) If a provision made by or under this Act (other than Division 5, 6 or 7 of Part 3) relating to an Information Privacy Principle or applicable code of practice is inconsistent with a provision made by or under any other Act, that other provision prevails and the provision made by or under this Act is (to the extent of the inconsistency) of no force or effect.

(2) Without limiting subsection (1), nothing in this Act affects the operation of the Freedom of Information Act 1982 or any right, privilege, obligation or liability conferred or imposed under that Act or any exemption arising under that Act.

The explanatory notes that this provision ‘allows relevant aspects of the IPPs to overlay the operation of other Acts where requirements can be observed concurrently’.

Similarly, Section 65(2) of the *Information Act* (NT) provides that if there is an inconsistency between an IPP and another provision of this Act, to the extent of the inconsistency, the other provision applies and the IPP does not apply.