Office of the Information Commissioner
Queensland

Level 7
133 Mary Street
Brisbane Q 4000

PO Box 10143
Adelaide Street
Brisbane Q 4000

Phone (07) 3234 7373
www.oic.qld.gov.au

ABN: 70 810 284 665

5 August 2022

Privacy and Right to Information Reforms
Strategic Policy and Legal Services
Department of Justice and Attorney-General
GPO Box 149
BRISBANE QLD 4000

By email:

PrivacyandRTIreforms@justice.qld.gov.au

Submission to the Department of Justice and Attorney-General on the Consultation Paper – Proposed changes to Queensland's Information Privacy and Right to Information Framework.

The Queensland Office of the Information Commissioner (**OIC**) welcomes the opportunity to provide a submission in response to the Department of Justice and Attorney-General on the Consultation Paper – Proposed changes to Queensland's Information Privacy and Right to Information Framework (**Consultation Paper**).

About the OIC

OIC is an independent statutory body that reports to the Queensland Parliament. We have a statutory role under the *Right to Information Act 2009* (**RTI Act**) and the *Information Privacy Act 2009* (**IP Act**) to facilitate greater and easier access to information held by government agencies. We also assist agencies to understand their obligations under the IP Act to safeguard personal information they hold.

OIC's statutory functions include mediating privacy complaints against Queensland government agencies, issuing guidelines on privacy best practice, initiating privacy education and training, and conducting audits and reviews to monitor agency performance and compliance with the RTI Act and the IP Act. Our office also reviews agency decisions about access and amendment to information.

General comments

OIC's submission addresses each of the Questions in the Consultation Paper and proposes additional reforms to the RTI and IP Act in Queensland. OIC notes that most of the proposed reforms to the RTI Act and IP Act outlined in the Consultation Paper have been recommended by a number of reports including:

- the report on the Review of the RTI and IP Act (**Review Report**)[1]

[1] Tabled in the Legislative Assembly 12 October 2017.

- the Crime and Corruption Commission (CCC)'s report, '*Operation Impala, A report on misuse of confidential information in the Queensland public sector*' (**Impala Report**)[2]
- the CCC's report, '*Culture and Corruption Risks in Local Government: Lessons from an investigation into Ipswich City Council*' (**Windage Report**);[3] and
- the Strategic Review of the Office of the Information Commissioner (**Strategic Review Report**).[4]

While OIC welcomes a number of the proposed reforms in the Consultation Paper, it has been OIC's consistent view that enactment of a contemporary legislative privacy framework in Queensland is critical in being able to respond to changing community expectations over privacy and the government's ability to protect them from harm.

Since the introduction of the IP Act in 2009 the privacy environment has changed immensely. The community has become more aware of their privacy rights and expectations have grown in relation to how government agencies manage their personal information. The emergence of new technologies, such as artificial intelligence and the increased use of data and cloud technology will necessitate a strengthened privacy framework to ensure the economic and other benefits these new technologies can deliver are appropriately balanced with the protection of an individual's privacy. OIC has consistently advocated for alignment of privacy laws across national and international jurisdictions, to the greatest extent practicable. It is critical that the IP Act remains fit for purpose in an increasingly interconnected digital world.

The use of Artificial Intelligence (**AI**) is becoming increasingly common across government agencies and the private sector, with levels of automation being provided for in a variety of Commonwealth legislation.[5] The Office of the Australian Information Commissioner's (**OAIC**) submission to the Australian Human Rights Commission (**AHRC**) Human Rights and Technology Issues Paper noted that the increase in the use of AI is 'supported by a fundamental shift in analytical processes, together with the availability of large data sets, increased computational power and storage capacity'. While the use of these technologies provides significant opportunities and benefits for business, government and the community, the use of these technologies also creates privacy risks, particularly where there is a lack of transparency about how personal information is used to make decisions, accountability and human oversight.[6]

Community attitudes to the use of AI technology are changing. Eighty-four percent of Australians think that individuals have a right to know if a decision affecting them is made using AI technology. While 78% of Australians believe that when AI technology is used to make or assist decisions, people should be told what factors and personal information are considered by the algorithm and how these factors are weighed.[7]

---

2 Tabled in the Legislative Assembly on 21 February 2020.
3 Tabled in the Legislative Assembly on 14 August 2018.
4 Tabled in the Legislative Assembly on 11 May 2017.
5 OAIC, *Submission to the Submission to AHRC Human Rights and Technology Inquiry Issues Paper* cited in Privacy Act Review Discussion Paper, October 2021 at page 137; See *Migration Act 1958* (Cth); *Australian Citizenship Act 2007* (Cth); *Social Security Administration Act 199*9 (Cth).
6 OIAC, Australian Community Attitudes to Privacy Survey 2020, page 86.
7 Ibid.

The General Data Protection Regulation (**GDPR**) specifically protects the rights of data subjects not to be subject to a decision solely based on automated processing where that decision has a significant impact on them, subject to limited exceptions, including where the data subject has consented.[8] It also creates right for individuals who are affected by automated processing.[9]

The issue of Automated Decision Making (**ADM**) was addressed in the Privacy Act Review Discussion Paper (**Discussion Paper**). The Discussion Paper proposal is to require privacy policies to include information on whether personal information will be used in ADM which has a legal, or similarly significant effect on people's rights.[10] It is OIC's view that the significant impacts ADM can have on an individual's privacy and other rights warrant specific protections and a strengthened legislated privacy framework. Protections such as mandatory Privacy Impact Assessments and notice of processing are important in building trust through transparency as governments increasingly look to automate government processes and pursue digital transformation. This is critically important, particularly following examples such as Robodebt and the adoption of AI technology in the detection of distracted drivers.

While OIC considers the technology neutral principles-based framework underpinning the IP Act provides flexibility to respond to new and emerging technologies, the existing regulatory framework requires updating and strengthening to ensure it strikes the right balance between competing rights and interests in an increasingly complex and digitised economy characterised by seamless data flows across borders.

Inconsistencies in privacy legislation across Commonwealth, State and Territory jurisdictions, lead to gaps in privacy protections afforded to individuals, including limiting opportunities for individuals to take timely action to mitigate damage and seek recourse in the event of a data breach. OIC notes that there is currently an absence of existing privacy legislation in South Australian and Western Australia. Sharing of personal information between jurisdictions is problematic where there is variance between, or absence of, legislated privacy safeguards across jurisdictions.

The Australian Government has recently committed to 'sweeping reforms' to data privacy laws in the life of the current Parliament and noted that the 'Commonwealth Privacy Act is out of date and in need of reform for the digital age'.[11] The current review of the *Privacy Act 1988* (Cth) (**Privacy Act**) may lead to greater alignment with the GDPR, further widening the gap between Commonwealth, State and Territory privacy legislation.

The impact of lack of nationally consistent privacy laws is not limited to the protection of an individual's privacy. The current patchwork of privacy laws across Australian jurisdictions presents ongoing challenges for regulatory compliance for government agencies and businesses and the implementation and success of a range of national data sharing and other initiatives. For example, the data sharing scheme under the *Data Availability and Transparency Act 2022*, National Driver Licence Facial Recognition Solution, Digital Identity and NAPLAN.

---

8 Article 22, GDPR.
9 Article 21, GDPR.
10 Proposal 17.1 at page 14.
11 https://www.afr.com/politics/federal/dreyfus-pledges-sweeping-data-privacy-reforms-20220627-p5awvw.

Community expectations around privacy and the handling of their personal information are changing. Key findings of the Australian Community Attitudes to Privacy Survey 2020 shows that privacy is a major concern for 70% of Australians while 87% want more control and choice over the collection and use of their personal information.[12] Meeting community expectations becomes critical for consumers, business and governments in building trust. Striking the right balance in a strengthened privacy framework will assist in meeting changing community expectations around personal information handling.

All agencies must protect individual's personal information. Failure to do so exposes individuals to risk, erodes trust, jeopardises public uptake of services, and damages and agency's reputation. OIC's report *10 years on: Queensland government agencies' self-assessment of their progress in right to information and information privacy* (**10 years on**)[13] provides important insights into agencies level of maturity with their information access and privacy obligations. While the report showed agencies reporting positive progress towards achieving compliance with some key responsibilities, a key finding of the report was that to manage emerging risks that come from new technologies, new types and sources of information and new privacy challenges, agencies should undertake a number of actions. This includes building privacy impact assessments (**PIA**) into all project design and management frameworks.[14] The report found that just over a quarter of agencies taking a privacy-by design approach and embedding PIAs into their project management framework.[15] Undertaking PIAs is core business for any agency when it is managing personal information.

Similarly, the community has high expectations about their right to access government-held information. The 2021 Cross Jurisdictional Information Access Study found the importance of the right to access information is consistently recognised by respondents in each jurisdiction ranging from 85% to 90% in 2021, consistent with 85% to 93% in 2019.[16] The results of the 2021 study reinforce the continuing importance the community places on the right to access government information, and the duty of governments to promote and enable this significant right.

Timely, easy access to information through administrative release unless there is a good reason not to, reinforces the importance of the RTI push model of information access. Recent increases in delays in decision making about access applications have led to community and media concerns about secrecy, transparency and impacts on applicants, where the utility of released information can be substantially reduced. 23%of OIC external review applications in 2021-22 resulted from agencies failing to make decisions within statutory timeframes (deemed decisions), consistent with 2020-21, however significantly higher than 2018-19 (10%).

The Review Report key recommendations included streamlining the right of access and amendment in the RTI Act to provide a single right of access, no new exemptions or exclusions and that the flexible public interest balancing test

---

12 https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey

13 Tabled in the Legislative Assembly on 13 June 2019.

14 Executive Summary, page 1.

15 Page 30.

16 https://www.oic.qld.gov.au/__data/assets/pdf_file/0008/49994/cross-jurisdictional-information-access-study-2021-qld.PDF

allows for adequate protection of information where required, and a number of refinements to improve administration of the Act for community and agencies.

Since the Review Report the *Human Rights Act 2019* (Qld) (**HR Act**) Act was introduced in Queensland, further increasing community expectations about information rights.

The HR Act places obligations on Queensland Government departments and agencies, local councils, and organisations providing services to the public on behalf of the state government to act and make decisions which are compatible with the rights it protects. Right to privacy and reputation is specifically protected under the HR Act.[17] Ensuring there is a comprehensive and clearly identifiable privacy regime assists in ensuring individuals are protected from arbitrary or unlawful breaches of an individual's right to privacy. The HR Act also protects the right to privacy and reputation[18] and the right to freedom of expression[19] which includes the freedom to seek, receive and impart information.

The Coaldrake Review Final Report (**Coaldrake Review**)[20] identified a number of concerns regarding the culture of openness and transparency within government. To this end Professor Coaldrake made a number of recommendations to improve both the availability of government documents and the government response to breaches of personal information. These issues are reflected in recommendations 2 and 10 relating to the release of Cabinet documents within 30 business days and the introduction of a mandatory data breach notification (**MNDB**) scheme in Queensland.

OIC considers further reforms to the RTI and IP Act are required in addition to those reforms outlined in the Consultation Paper.

These further reforms are listed at **Appendix A**.

Resourcing impacts

OIC notes that a number of the proposed reforms, if adopted, will have significant resourcing impacts on OIC. As outlined earlier, OIC is an independent statutory body and forms part of the integrity and accountability framework in Queensland. OIC's statutory functions include mediating privacy complaints against Queensland government agencies, issuing guidelines on privacy best practice, initiating privacy education and training, and conducting audits and reviews to monitor government agency performance, and compliance with, the RTI Act and the IP Act.

Further details in relation to the impacts upon resourcing with respect to its privacy functions are contained in OIC's consultation paper response to the MNDB scheme and a single set of privacy principles.

The proposed reforms have implications for OIC in performing both oversight or regulatory functions, and support functions in which we will provide training, guidance and assistance to agencies and the community about changes to legislation and related matters. The success of the proposed reforms and impact on stakeholders will rely on appropriate resourcing and timeframes for

---

17 Section 25.
18 Section 25, *Human Rights Act 2019*.
19 Section 21, *Human Rights Act 2019*.
20 Let the sunshine in, Review of culture and accountability in the Queensland public sector, Final Report, 28 June 2022.

implementation. Agencies across affected sectors are diverse with substantially different maturity in compliance and practices.

Demand for external review has continued at high levels, year on year, since 2017-18. It remained high in 2021-22 with 605 external review applications received and 650 finalised. The demand for external review is disproportionate to the growth in applications for access under the RTI and IP Acts, which has increased to 18,448 in 2020-21, up from 14,081 in 2008-09 under the FOI Act. The upward trend for external review services, which comprises the largest proportion of our resources, is consistent with other Australian and New Zealand jurisdictions, and may be due to a greater awareness of the right to access.[21]

While under the Queensland push model formal access applications are a last resort, it's important to consider the exponential growth of information since 2009 including that held by government agencies. This means the increase in formal access applications is relatively low in contrast, however OIC considers further improvements to adopt the push model are necessary and legislative reforms can support such change to help reduce further unnecessary demand. Having managed record demand across key functions and services in recent years, OIC is not in a position to manage any additional demand placed on its services, or expansion of functions, or nature of those functions. If functions are allocated without appropriate resourcing, it would also significantly compromise the community's existing rights to information privacy and access government held information given the current record demand for OIC services. This is likely to have implications under the HR Act.

OIC's Submission – Part A

Question 1. Should the definition of personal information in the *Information Privacy Act 2009* (IP Act) be amended to reflect the definition which is currently in the *Privacy Act 1988* (Cth) (Privacy Act)?

In its 2016 submission to the Consultation on the Review of the RTI and IP Act (**2016 Consultation**), OIC recommended aligning the definition of personal information in the IP Act with the definition in the Privacy Act. The Impala Report also recommended that the Information Privacy Principles (**IPPs**) and National Privacy Principles (**NPPs**) in the IP Act be amalgamated and strengthened, having regard to the Australian Privacy Principles (**APPs**) contained in the Privacy Act; and in particular the:

1. definition of "reasonable steps" in the fourth of each set of principles relating to security of data be further defined in accordance with the terms of Article 32 of the GDPR; and
2. definition of "personal information" be amended in the IP Act to accord with the current version contained in the Privacy Act (**Recommendation 16**).

The current 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

[21] For example, in 2020-21, Victorian agencies received 42,249 requests which is the highest number of FOI requests ever received. Office of the Victorian Information Commissioner, *The State of Freedom of Information in Victoria*, February 2020.

whose identity is apparent, or can reasonably be ascertained, from the information or opinion'.[22] The Privacy Act currently defines personal information as 'information or an opinion, about an identified individual, or an individual who is reasonably identifiable:

a) whether the information or opinion is true or not; and
b) whether the information or opinion is recorded in a material form or not.[23]

The review of the Privacy Act commenced in October 2020 with the release by the Australian Government of an Issues Paper. This was followed by release of a Discussion Paper in late 2021. Submissions to the Discussion Paper closed on 10 January 2022. The review of the Privacy Act is yet to be finalised. Within scope of the review of the Privacy Act is the definition of '*personal information*'.

The Discussion Paper proposal is to amend the definition of personal information to make clear that it includes technical and inferred personal information.[24] The proposed changes reflect aspects of the GDPR's definition of personal data in recognition, in part, of harmonising the Australian definition with the GDPR.[25] As noted by the OAIC, the definition of personal information is a foundational concept in the Privacy Act. The OAIC, in their submission to the Discussion Paper, welcomed the Discussion Paper's proposals aimed at modernising the definition of personal information to ensure it remains relevant in the digital age and is interoperable with relevant domestic laws and comparable international privacy jurisdictions.[26] The OAIC recommended:[27]

- changing the word 'about' in the definition of personal information to 'relates to' (Recommendation 2)
- including a non-exhaustive list of technical data that may be captured by the definition of personal information in the explanatory memorandum for these amendments, rather than the Privacy Act (recommendation 3); and
- consider alternatives for meeting the objectives of proposal 2.3,[28] including requiring entities to have regard to OAIC guidelines when carrying out their functions or activities.

The Privacy Act has continued to evolve while the IP Act has not been reviewed since it was enacted in 2009. The current review of the Privacy Act is significantly progressed and any proposed amendments to the Privacy Act could be in force before proposed amendments to the IP Act. OIC has consistently advocated for harmonisation of privacy laws across jurisdictions, including alignment of the definition of personal information in the IP Act with the Privacy Act.

As such, OIC supports amending the definition of personal information in the IP Act to reflect the definition in the Privacy Act. OIC further recommends that the Queensland Government continue to consult and liaise with the Australian Government regarding progress of amendments to the definition of personal information in the Privacy Act and align the definition of the personal information

---

22 Section 12.
23 Section 6, Division 1, Part 11.
24 2.1-2.3, Discussion Paper, Privacy Act Review, page 26.
25 2.1-2.3, Discussion Paper, Privacy Act Review, page 26.
26 OAIC submission to Discussion Paper December 2021, page 29.
27 OAIC submission to Discussion Paper OAIC submission to Discussion Paper December 2021, page 32.
28 Proposal 2.3 (Discussion Paper) define 'reasonably identifiable' to cover circumstances in which an individual could be identified, directly or indirectly. Include a list of factors to support this assessment.

in the IP Act with any updated or revised definition in the Privacy Act arising out the review of that Act. As noted earlier, the Australian Government has committed to reforms of the Privacy Act. This will assist in ensuring the definition of personal information in the IP Act is contemporary and remains fit for purpose in the digital age.

Question 2. Should the proposed Queensland Privacy Principles (QPPs) be adopted in Queensland?

Question 3. If not, in what ways should they be changed?

A key component of a contemporary legislative privacy framework is consolidation of the IPPs and NPPs into a single set of privacy principles. Consolidation of the privacy principles will reduce complexity and confusion, simplify the application of privacy laws and foster national and international consistency in privacy regulation. A single set of privacy principles was recommended by OIC in its submission to the 2016 Consultation and by the Impala Report (Recommendation 16). This issue has previously been considered by the Australian Law Reform Commission (**ALRC**).[29]

Previous consolidation of Commonwealth privacy principles

The Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) was assented to on 12 December 2012, implementing a number of the ALRC's recommendations in the 2008 '*For your information'* report. In its report, the ALRC considered whether it is preferable to maintain two separate sets of similar, but sometimes inconsistent privacy principles, or to create a unified set of privacy principles.[30]

In response, a very large number of stakeholders submitted that it would be desirable to consolidate the IPPs and NPPs to create a single set of privacy principles, which would generally be applicable to organisations and agencies. Stakeholders expressed support on the basis that maintaining separate sets of privacy principles creates complexity and confusion in a number of areas. It was submitted that a consolidation of the principles would simplify compliance requirements and, therefore, enhance administrative convenience. In addition, stakeholders expressed the view that establishing a single set of privacy principles would help achieve the desirable goal of national consistency, as well as consistency with a number of key international instruments, in operation at the time, such as the EU Directive, the OECD Guidelines and the APEC Privacy Framework.

The overwhelming majority of stakeholders that expressed a view on this issue were in favour of consolidating the IPPs and NPPs to create a single set of privacy principles that generally would be applicable to organisations and agencies. In addition, there was support for the proposal from each of the various categories of stakeholder—that is, organisations, agencies and others.

[29] Australian Privacy Law and Practice (ALRC Report 108).
[30] https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/18-structural-reform-of-the-privacy-principles/towards-a-single-set-of-privacy-principles/

In the ALRC's view, the IPPs and NPPs should be consolidated to establish the Unified Privacy Principles[31] (**UPPs**) that generally would be applicable to agencies and organisations.

The ALRC expressed the view that a large number of benefits would flow from such a reform. For example, the move to a set of UPPs would foster national and international consistency in privacy regulation. Such a reform also would clarify and simplify the obligations of agencies and organisations with respect to information privacy. This would be advantageous for individuals who interact with these entities, and also for the agencies and organisations themselves, as they would not have to differentiate between the overlapping requirements of the IPPs and NPPs. Where an organisation is acting as a contracted service provider or is involved in a public-private partnership, it would significantly reduce the problems associated with the organisation having to comply with both the IPPs and NPPs. This simplification may go some way to offsetting costs associated with implementing a new regime for privacy regulation.

A key recommendation in the OAIC's submission in response to the Australian Government's Issues Paper on the review of the Privacy Act was to ensure that harmonisation of privacy protections is a key goal in the design of any federal, state or territory laws that purport to address privacy issues (Recommendation 69).[32] The unification of the privacy principles would also ensure a consistent higher standard of protection to be afforded to 'sensitive information' – which includes health related information, DNA and biometric data.

OIC supports 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.

How to adapt the APPs in Queensland

If the government supports the adoption of a single set of privacy principles, a model which could be used is the Australian Capital Territory (**ACT**) Privacy Principles (**TPPs**).[33] The TPPs have been drafted to mirror and align with the APPs. Some of the APPs are not relevant to the regulation of information privacy by ACT public sector agencies and have been omitted.[34] The TPPs commenced on 1 September 2014 and apply to the ACT public sector agencies and contracted service providers (including subcontractors), but only to the extent they perform obligations under a government contract.

Where an APP has not been adopted as a TPP it is noted in the text of the TPPs. Although the TPPs contain minor textual differences to the APPs it is considered that these do not change the intended meaning of the principles. For example, the phrase 'the entity must take such steps (if any) as are reasonable in the circumstances' is used in the APPs while a similar phrase, 'the agency must take reasonable steps', is used in the TPPs. While expressed differently, both requirements could be satisfied by taking no steps if that is reasonable in the particular circumstances.[35]

---

31 These were eventually referred to as the Australian Privacy Principles (**APPs**).

32 https://www.oaic.gov.au/privacy/the-privacy-act/review-of-the-privacy-act/privacy-act-review-issues-paper-submission/executive-summary.

33 Schedule 1 of the *Information Privacy Act 2014*.

34 Note: This has resulted in slight inconsistencies in the numbering of the TPPs.

35 https://www.oaic.gov.au/privacy/privacy-in-your-state/privacy-in-the-act/territory-privacy-principles.

While noting that the wording of the proposed QPPs, as outlined in the Consultation Paper, will be subject to further consultation as new legislation is drafted, OIC has identified a number of important omissions and inconsistencies between the proposed QPPs and the APPs and TPPs that in OIC's view will lead to a range of unintended consequences.

At a high level, the more important identified omissions and inconsistencies include:

- numbering differences between QPPs, APPs and TPPs
- omission of reference to a code in in various QPPs including 1 and 5 (see response to Q.6 - recommended inclusion of a Code making Power in the IP Act); and
- QPPs 10 and 11 do not provide the level of detail provided in the corresponding APPs and TPPs.

OIC notes that any difference between the QPPs and APPs could create unintended consequences. These inconsistencies would exacerbate existing difficulties with the current patchwork of privacy laws across jurisdictions presenting a range of challenges and impacts for entities and individuals where data flows freely across borders. Some of these difficulties include:

- increased administrative burden for entities with obligations to comply with both Queensland and Commonwealth privacy laws
- gaps in privacy protections for individuals where personal information is shared across jurisdictions under national data sharing or other initiatives
- lack of ability to draw upon existing resources on the interpretation and application of the privacy principles across jurisdictions; and
- lack of established precedent for interpretation of proposed QPPs; and
- adopting privacy principles that are not fit for purpose in a digital age.

OIC recommends adopting QPPs which mirror the APPs and TPPs in the interests of aligning, to the greatest extent practicable, with the Privacy Act.

Question 4. What are the benefits and disadvantages of defining the factors that must be considered in 'reasonable steps' for proposed QPP 9 in the IP Act?

The IP Act contains a set of rules or 'privacy principles' that govern how Queensland Government agencies collect, store, use and disclose information providing a degree of regulatory flexibility. This principles-based law has the advantage of being technology neutral and provides the required flexibility to adapt to continually changing and emerging technologies without the need to continually amend and update the legislative framework. It also has the advantage of providing an agency with the flexibility to tailor their personal information handling practices to their own business models and the individuals they serve.

Introducing further prescriptive requirements or rules into the privacy principles by defining the factors that must be considered in 'reasonable steps' for proposed QPP9 can provide greater certainty and clarity for agencies. However, if this is not done carefully, it can also impose requirements that are not always appropriate for all agencies regulated by the IP Act and may require ongoing

legislative amendment to respond to continually changing and emerging technologies.

This issue was recently considered in the Privacy Act Review Discussion Paper.[36] The Discussion Paper proposed that some APPs should be amended to include greater legislative guidance as to their application in certain circumstances. The proposals intended to clarify the matters that are relevant to determining what 'reasonable steps' are for the purposes of some APPs by elevating factors from the OAIC's APP guidelines into the law.

For example, the Discussion Paper proposed to amend:

- APP 11.1[37] to state that 'reasonable steps' includes technical and organisational measures (proposal 19.1)
- APP 11[38] to include a list of factors that influence what reasonable steps may be required (proposal 19.2); and
- APP 8 to clarify what circumstances are relevant to determining what reasonable steps are for the purpose of APP 8.1 (proposal 22.6).

In its submission, OAIC considered that 'the proposals to introduce greater prescription in relation to APPs 8 – *cross-border disclosure of personal information* and 11 – *security of personal information* may result in inconsistency with the other APPs that are also centred around the 'reasonable steps' test. Introducing greater prescription in relation to certain APPs may result in a fragmented approach to the broader APP framework that is inconsistent with principles of reducing complexity and improving clarity by*, inter alia*, ensuring that the same concepts are expressed consistently within the same legislation'.[39]

OIC agrees with OAIC's view, as outlined above, and for these reasons considers the disadvantages of legislatively defining the factors that must be considered in 'reasonable steps' outweigh the benefits. Introducing prescriptive requirements into the privacy principles in the IP Act could change the regulatory principles-based model provided under this Act. As such, OIC does not support defining the factors that must be considered in 'reasonable steps' for proposed QPP 9 in the IP Act.

Question 5. Could these factors be applied to other relevant parts of the IP Act?

For the reasons outlined above, OIC does not support defining factors that must be considered 'reasonable steps' into the proposed QPP9 or other relevant parts of the IP Act. Amalgamation of the IPPs and NPPs into a single set of privacy principles and other proposed amendments aimed at harmonising Queensland privacy law with other Australian privacy jurisdictions will assist in providing a larger body of guidance and jurisprudence to aid interpretation and application of key concepts and terms in the IP Act, such as what constitutes 'reasonable steps.'

[36] Privacy Act Review – Discussion Paper https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/.

[37] **APP 11.1 – security of personal information** provides that if an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information: (a) from misuse, interference and loss; and(b) from unauthorised access, modification or disclosure.

[38] APP 11 – security of personal information.

[39] OAIC submission to Privacy Act Review Discussion Paper, page 43.

Question 6. Would statutory guidelines produced by Office of the Information Commissioner (OIC) be more flexible and useful?

OIC's performance monitoring and support functions under the IP Act include issuing guidelines about any matter relating to the Information Commissioner's functions, including guidelines on how this Act should be applied and on privacy best practice generally.[40]

Producing statutory guidelines is consistent with OIC's existing functions under the IP Act and the principles-based privacy framework. Guidelines have the advantage of providing a flexible and efficient response to a dynamic and constantly changing privacy framework. Harmonisation of privacy laws across jurisdictions enables the sharing of resources, including guidelines, resulting in administrative efficiencies and consistency in interpretation and application of the provisions of the IP Act. Aligning a single set of privacy principles in Queensland with the APPs would allow agencies and individuals to draw upon a larger body of guidelines and resources, including broader jurisprudence on what constitutes 'reasonable steps.'

The OAIC, in response to the proposal to include greater legislative guidance as to the APPs application in certain circumstances, submitted that the aims of these proposals could be more broadly achieved by requiring APP entities to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act.

Code making power

While OIC considers statutory guidelines provide the required flexibility to respond to a constantly changing environment, it is OIC's view that the effectiveness of statutory guidelines could be strengthened by amending the IP Act to provide for a complementary code making power.

Part IIIB of the Privacy Act provides creates a framework for the development, registration and variation of codes about information privacy (**APP codes**). An APP code can set out how the APPs are complied with and may impose additional requirements to those imposed by the APPs.[41] Any additional requirements must not be contrary to, or inconsistent with the APPs.[42] A code can be targeted at:

- a specified type of personal information
- a specified activity or specified class of activities of an APP entity
- a specified industry or profession, or specified class of industries or professions; or
- APP entities that use technology of a specified kind.[43]

There is currently in force a code which applies to the Commonwealth Government Agencies. The *Privacy (Australian Government Agencies — Governance) APP Code 2017* commenced on 1 July 2018 (**the Code**). The Code is a binding legislative instrument under the Privacy Act. The Code sets out specific requirements and key practical steps that agencies must take as part of complying with APP 1.2. 'It requires agencies to move towards a best

[40] Section 135(1)(c) IP Act.
[41] Privacy Act (n 16) Part IIIB (Privacy Act Review Issues Paper, October 2020, page 22).
[42] Section 26C(3)(a) (Privacy Act Review Issues Paper, October 2020, page 22).
[43] Section 26C(4).

practice approach to privacy governance to help build a consistent, high standard of personal information management across all government agencies.[44] The Code requires agencies to:

- have a privacy management plan
- appoint a Privacy Officer, or Privacy Officers, and ensure that particular Privacy Officer functions are undertaken
- appoint a senior official as a Privacy Champion to provide cultural leadership and promote the value of personal information, and ensure that the Privacy Champion functions are undertaken
- undertake a written PIA for all 'high privacy risk' projects or initiatives that involve new or changed ways of handling personal information
- keep a register of all PIAs conducted and publish this register, or a version of the register, on their websites; and
- take steps to enhance internal privacy capability, including by providing appropriate privacy education or training in staff induction programs, and annually to all staff who have access to personal information.[45]

Agencies will still need to take other steps under APP 1.2 to ensure compliance with all the APPs. The Code is flexible and scalable, taking into account an agency's size, and the sensitivity and amount of personal information it handles.[46]

Part 7 of the *Information Privacy Act 2014* (ACT) provides for the development of codes of practice about information privacy. The provisions have been developed based on the APP codes under the Privacy Act. The provisions have been adapted as appropriate to the small scale of the Territory, given that the TPP codes will only apply to public sector agencies and contracted government service providers.

As noted earlier, OIC's 10 years on report showed that just over a quarter of agencies taking a privacy-by-design approach and embedding PIAs into their project management frameworks. Government departments (around 50%) and HHSs (around 60%) have higher rates of integrating privacy-by-design approaches into their operations. However, these practices should be core business for all agencies.[47]

The Privacy Act is currently being reviewed with a number of proposals to improve the OAIC's ability to make codes.[48] OIC recommends any proposed code making power under the IP Act takes into account recommended changes arising out of the review of the Privacy Act.

---

44 https://www.oaic.gov.au/privacy/privacy-for-government-agencies/australian-government-agencies-privacy-code.

45 https://www.oaic.gov.au/privacy/privacy-for-government-agencies/australian-government-agencies-privacy-code.

46 https://www.oaic.gov.au/privacy/privacy-for-government-agencies/australian-government-agencies-privacy-code.

47 Page 30.

48 Privacy Act Review Discussion Paper – see proposals 3.1 and 3.2, page 37 https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf.

Question 7. Should the Information Commissioner be given a power to conduct an 'own motion' investigation into whether there has been a breach of the privacy principles?

OIC supports the proposal for it to be provided with clear own motion investigation powers. As noted in the Consultation Paper this recommendation was made in both the CCC's public report – Operation Impala and in the Review Report.

It is considered that such a clear power is necessary in order for OIC to properly exercise its functions as a regulator and ensure compliance by agencies with the privacy principles. OIC currently has powers to conduct reviews[49] and compliance audits[50] of relevant entities. OIC also has the capacity to issue compliance notices[51] However, certain minimum requirements must be met prior to the exercise of these powers. The powers do not provide OIC with sufficient capacity to examine the cause and associated risks from privacy breaches which do not meet the threshold of being satisfied on reasonable grounds that *a serious or flagrant contravention of the agency's obligation to comply with the privacy principles or is of a kind that has been done or engaged in by the agency on at least 5 separate occasions within the last 2 years.*

Currently OIC lacks powers to investigate poor practices or issues which fall short of the current requirements to issue a compliance notice. It is important for OIC to have a comprehensive view of the privacy landscape including the risks that cause privacy breaches.

By way of example, a member of public locates a USB drive in a public place which contains personal information of other people and which appears to have come from a government agency. The member of the public contacts OIC and advises that it is now in their possession and seeks advice on what to do with the device and what action OIC will take. It is not known how the USB came to be where it was located or whether it was a government employee who lost it. There is no privacy complaint as the people whose personal information is on the USB are not likely to be aware about the loss of data. OIC has no powers to investigate the circumstances giving rise to the notification it has received or determine if there has been a breach of the privacy principles. This may be an appropriate matter for OIC to commence an own motion investigation.

Own motion powers would also help OIC to be more proactive in the event that reports or information about suspected breaches of privacy principles are reported to OIC through mechanisms which do not amount to a privacy complaint.

Question 8. Should the Information Commissioner be given a power to make declarations, based on the Commonwealth model, after an own-motion investigation has been conducted?

[49] Section 135(1)(a)(i), IP Act.
[50] Section 135(1)(b(iii), IP Act.
[51] Section 158, IP Act.

OIC supports the proposal for it to be given the power to make a declaration following an own motion investigation or in relation to a privacy complaint. However, it also recognises the importance of not duplicating the function of Queensland Civil and Administrative Tribunal (**QCAT**) in this regard. One of the principal drivers for the recommendation by the CCC in its report was to make it easier for complainants affected by a breach of privacy to obtain a remedy.

Three of the reasons behind this, according to the report, were:

- the length of court proceedings
- power imbalances between self-represented litigants, as compared to agencies' engagement of senior legal representation, and
- costs associated with court proceedings.

OIC considers that there are two possible resolutions to this proposal. The first would be to confer on the Information Commissioner a power to make a determination and relevant orders, in the first instance, in relation to a privacy complaint with a right to appeal to QCAT by either party which may be dissatisfied with the Commissioner's determination. This would assist in ensuring a more consistent approach to privacy complaints across different agencies, no duplication of the function of OIC and QCAT, and preserve appeal rights for the affected parties.

Taking on this new function would have resource implications for OIC which would need to be sufficiently addressed to be effective. The alternate resolution would be to provide the Information Commissioner with a subset of the remedies available to QCAT and encourage a timely and efficient resolution of the "less serious" privacy breaches.

Privacy complaints received by OIC generally fall into one of three categories regarding the reason for the complaint not being resolved directly between the agency and the complainant.

The first category is where a complainant's privacy has been breached and there is obvious and clear impact upon the complaint causing damage such as embarrassment, distress, reputational harm or financial loss. Often the agency has acknowledged a breach of the complainant's privacy, has apologised and put in place steps to reduce the risk from reoccurring, however the complainant is seeking additional remedial action which the agency is not prepared to agree to. Often this relates to the payment of financial compensation. These matters could remain to be determined by QCAT. It is considered that decisions by OIC in these types of matters are more likely to be the subject of an ongoing appeal or review by complainants that do not receive the sum of damages that they are seeking.

The second category is where the agency has not accepted that it acted in a way that constituted a breach of the privacy principles and the complaint then refers their complaint to OIC for mediation. In circumstances where OIC forms the view that there was a breach of the complainant's personal information, negotiations will successfully recommence with the agency involved.

The last category is similar to the first, but the breach may involve a "technical breach" where there is no, or 'nominal damage or inconvenience' suffered by the complainant. The agency acknowledges that a breach occurred but does not consider that financial compensation is warranted.

One of the main reasons that accepted privacy complaints do not resolve is because the parties are unable to agree on whether or an amount of compensation that should be paid in response to a privacy breach. At times this is the result of complainants seeking compensation in relation to trivial (less serious) breaches. Providing Information Commissioner with the power to make a determination that a person's privacy has been breached and a capacity to compel the agency to take remedial action (other than financial compensation) could facilitate a timely resolution of less serious complaints. A determination of this type by OIC would minimise any further need by the agency to take part in ongoing mediation. OIC would anticipate that the complainant would still be able to exercise a right to have the decision of OIC reviewed in an appropriate forum.

Question 9. Should the OIC have the power to intervene in tribunal or court proceedings, involving the IP Act?

OIC supports the recommendation to provide OIC a clear legislative basis to appear as a friend of the court, with leave, in relation to privacy complaints that were not able to be mediated between the complainant and the relevant agency.

OIC is capable of providing assistance to the tribunal in relation to relevant guidelines issued by OIC and its experience with how other regulators have applied similar privacy principle obligations. This information may be useful guidance for the tribunal.

Although QCAT is intended to operate without the formality of a court proceeding, the findings from Operation Impala were that complainant's still found the process difficult to navigate and time consuming. It is not intended that the role of OIC is to represent the interests of the complainant, however OIC's experience in dealing with complaints is that some complainants have difficultly aligning their concerns with the relevant obligations imposed by the privacy principles. OIC may be able to assist the tribunal elicit a nexus between the complainants concerns the relevant obligations under the privacy principles. It is not intended that OIC would be a party to proceedings. This function would also be consistent with other jurisdictions including New South Wales and Victoria.[52]

Question 10. Do you have any other comments about the powers and roles of the OIC, including the current range of support services provided by the OIC?

OIC has identified in previous annual reports the increase in time to deal with accepted privacy complaints. These delays have, in the main, been due to waiting long periods of time for responses for information from both the complainant and agencies. There is a requirement under section 168(2) for complainants to comply with reasonable requests from the Information Commissioner and cooperate with the Information Commissioner's dealing with the complaint. In the event that the complainant does not act reasonably the Information Commissioner may exercise a discretion to decline to continue to deal with their complaint. However, when there are delays in obtaining responses from agencies, there are no comparable powers for the Information

[52] *Privacy and personal Information Protection Act 1988* (NSW), section 55(6); *Privacy and Data Protection Act 2014* (Vic), section 74.

Commissioner to motivate the agency to prioritise its request for information. There is explicit provision under section 96 of the RTI Act requiring participants in an external review, including agencies, to comply in a timely way with a reasonable request made by the Information Commissioner for assistance in relation to the review.

Appropriate powers for the Information Commissioner to encourage a timely compliance with requests for information could include a time frame within which agencies are required to respond to requests consistent with section 116 in the IP Act and an obligation on OIC to report agencies compliance with this requirement to its parliamentary oversight committee. The obligation could also include an ability for OIC to extend the time within which the agency is to respond in appropriate circumstances.

Question 11. Is the mandatory DBN scheme as outlined in this Consultation Paper suitable for adoption in Queensland?

Question 12. If not, in what ways should it be changed?

The introduction of a mandatory data breach notification scheme in Queensland was recommended by OIC in its submission to the 2016 Consultation, the Impala Report[53] and by the Coaldrake Review which recommended *a MDBN scheme be established in Queensland, forthwith*.[54] OIC notes that the Premier and Minister for the Olympics, the Honourable Annastacia Palaszczuk in response to the Coaldrake Review stated that 'we will accept all of his recommendations and we will implement them lock, stock and barrel'.[55]

As noted earlier, OIC continues to advocate for nationally consistent privacy laws. This includes aligning a mandatory data breach scheme in Queensland with critical elements of the MNDB scheme under the Commonwealth Privacy Act such as definitions, timeframes, and thresholds. Greater alignment between the various notifiable data breach schemes allows jurisdictions to draw upon shared regulatory guidance and tools to assist agencies and entities comply with their regulatory obligations and minimise the risk of harm to individuals in the event of a data breach. It is OIC's position that any MNDB scheme should mirror the Commonwealth MNDB scheme to the extent of relevance to the Queensland jurisdiction.

OIC notes that the following elements of the mandatory DBN scheme outlined in the Consultation Paper appear to align with the MNDB scheme under the Commonwealth Privacy Act:

- **Definition of *eligible data breach*** i.e., there is unauthorised access to, or disclosure of, personal information held by an organisation or agency (or information is lost in circumstances where unauthorised access to

[53] Recommendation 12 – that a mandatory data breach notification scheme be implemented in Queensland and that OIC be responsible for developing the scheme, and receiving and managing the notifications.
[54] *Let the sunshine in*, Review of culture and accountability in the Queensland public sector, Final Report, 28 June 2022.
[55] https://statements.qld.gov.au/statements/95531

disclosure is likely to occur and this is likely to result in serious harm to any of the individuals to whom the information relates[56]

- **Serious harm not defined in legislation**. The relevant sections of the Privacy Act list a range of factors to consider[57] including, in addition to those listed in the Consultation Paper, *any other relevant matters*[58]
- **Exception for remedial action** i.e., an eligible data breach would not occur if an agency acted quickly to take remedial action and as a result of the remedial action a reasonable person would conclude the breach is not likely to result in serious harm (for example where an email containing personal information has been sent to the wrong recipient and the agency immediately contacts the recipient and confirms that the email has been deleted)[59]
- **Timeframe for assessment of suspected eligible data breaches** i.e., requiring expeditious assessment of suspected eligible data breaches, which agencies must take reasonable steps to complete within 30 days[60]
- **Notification requirements** including content and method of notification; [61] and
- **Exceptions to compliance** including for law enforcement-related activities,[62] where compliance would be inconsistent with secrecy provisions[63] and where the Commissioner declares that notification is not required.[64]

OIC supports alignment of the above elements with the Commonwealth scheme. Consistency with legislative definitions, thresholds for notification and procedural matters for notification provides greater clarity and certainty in interpretating and applying the MNDB scheme in Queensland. OIC recommends any proposed changes to the Commonwealth Scheme arising from the Privacy Act Review are taken into account when developing the Queensland scheme.

If the mandatory DBN scheme were introduced, it would increase the need for provision in the IP Act for representative actions. 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. OIC considers amending the IP Act to provide for representative actions is critical to support the proposed introduction of a mandatory DBN scheme in Queensland (see **Appendix A).**

OIC would welcome being consulted closely throughout the process of development of a MNDB scheme in Queensland as implementation of this recommendation progresses.

Question 13. Would the Information Commissioner require any additional powers to monitor and provide oversight to the mandatory DBN scheme?

56 Section 26WE Privacy Act.
57 Section 26WG Privacy Act.
58 Section 26WG(j) Privacy Act.
59 Section 26WF Privacy Act.
60 Section 26WH Privacy Act.
61 Section 26WL Privacy Act.
62 Section 26WN Privacy Act.
63 Section 26WP Privacy Act.
64 Section 26WQ Privacy Act.

The Consultation Paper proposes that OIC would have an oversight role for the Mandatory NDB scheme with functions and powers to monitor and ensure compliance with the scheme. In addition to OIC's existing powers and functions, the Consultation Paper proposes new regulatory powers for OIC including:

- giving a written notice to an agency directing the agency to prepare a statement about a data breach; [65]and
- recommending that an agency notify individuals in relation to a data breach.[66]

OIC supports the new regulatory powers for OIC outlined above. OIC considers the following additional powers are required:

- own Motion Power (see responses to Questions 7 to 11 above); and
- power of entry and inspection to premises[67]; and
- the power to compel the production of a report from an agency about a breach which overrides a claim of legal professional privilege.

A response to a breach of personal information may at times be significant and give rise to complex considerations of legal liability for the breach. Liability for a breach of privacy can be significant in terms of both compensating people adversely affected by the breach and in conducting remedial efforts to mitigate the cause of the breach. Liability in some circumstances, particularly if a number of other parties are involved in the breach, such as a contracted service provider, may give rise to complex legal considerations involving contractual interpretation and an analysis of ICT processes.

OIC is aware that it is common for agencies to seek reports and advice from law firms into the circumstances giving rise to a breach and that such reports may be subject to claims of legal professional privilege. OIC considers that it ought to have access to those reports to ensure that responses to privacy breaches are being dealt with in a transparent and accountable manner. It would also increase public trust that agencies are managing their personal information appropriately. However, OIC also recognises that the implications for agencies and other companies may be that privilege is deemed to be waived if the report is shared with another entity. To mitigate this risk OIC proposes that where it exercises a power to obtain information relevant to its functions that an entity may not claim legal professional privilege to resist providing OIC with a copy of the report and that the report should otherwise maintain its status to others as being privileged.

Question 14. Is a new criminal offence required to prosecute offences for misuse of confidential information, or are existing provisions in the *Criminal Code Act 1899* (Criminal Code) and other legislation adequate?

The protection of confidential information, including the community's personal information, which is collected by public sector agencies is critical for

[65] See Section 26WR of the Privacy Act and section 59X(2) of the Privacy and Personal Information Protection Amendment Bill 2021 (NSW).
[66] See section 26WR(2) of the Privacy Act and section 59X(3) of the Privacy and Personal Information Protection Amendment Bill 2021 (NSW).
[67] See section 59Z of the Privacy and Personal Information Protection Amendment Bill 2021 (NSW).

maintaining trust in government and engagement by the community with the services agencies provide. Misuse of confidential information can occur for a range of reasons, including human error, an external actor breaching an agency's network or deliberate misuse by public sector employees. It is important that agencies take steps to minimise the risks of misuse of confidential information, but if it occurs there needs to be an appropriate mechanism to deal with the conduct and provide an appropriate criminal sanction if the conduct involves a breach of the trust by a public sector employee.

It is important that public sector employees understand that deliberately breaching other people's privacy is serious and it will be taken seriously by their employer through suitable disciplinary action and criminal charges where appropriate.

OIC agrees with the proposition in Operation Impala that misuse of confidential information should be protected and be subject to criminal sanctions regardless of whether the information is obtained from a computer, a paper file or some other source. The current criminal sanctions as outlined in the Consultation Paper do not appear to be fit for purpose and it is likely that there will remain gaps in the laws which do not adequately cover all the circumstances where there is a misuse of confidential information. OIC supports the imposition of a new criminal offence as recommended in Operation Impala.

Part B: Further proposed right to information and information privacy reforms

Making applications

A single right of access (Review Report, Recommendation 2)
In its submission to the 2016 consultation, OIC recommended a single point of entry for the right of access within the RTI Act. OIC recommended 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 continues to support a single right of access and notes the proposed reform is a Review Report recommendation. OIC considers a single right of access will reduce duplication and complexity resulting in greater efficiencies in processing applications.

Access applications and amendment applications – Forms (Review Report, appendix 3)
The proposal seeks to remove the requirement for applications to be in the approved form. Access applications would still need to be in writing, provide sufficient information concerning the document sought to enable the agency to identify it, and state an address to which notices may be sent. Amendment applications would still need to:

- be in writing

- provide sufficient information concerning the document to enable the agency to identify it
- state an address to which notices may be sent
- state the information the applicant claims is inaccurate, incomplete, out of date or misleading
- state the way in which the applicant claims the information is inaccurate, incomplete, out of date or misleading
- if the applicant claims the information is inaccurate or misleading, state the amendments the applicant claims are necessary; and
- if the applicant claims the information to be incomplete or outdated, state the other information the applicant claims is necessary.

It is further proposed that the power under section 192 of the RTI Act and section 200 of the IP Act for the chief executive to approve forms could be retained. A standard form could continue to be used for online applications and by agencies if desired. OIC notes that removal of the requirement for applications to be in the approved form is a Review Report recommendation.

In its submission to the 2013 review of the RTI Act and Chapter 3 of the IP Act (**2013 Consultation**), OIC recommended amending the RTI Act to allow agencies the flexibility to create their own application forms that comply with requirements set out in the relevant Regulation. OIC recommended retaining the whole of government forms for use by agencies who choose not to develop their own form.

OIC further submitted specifying the information that must be collected by any agency-developed application form will allow the maximum amount of flexibility for agencies while simultaneously limiting the number of non-compliant applications. For the above reasons, and as a way of ensuring consistency between the processes, OIC suggests the same approach be adopted for amendment applications. OIC supports the proposal as it is largely consistent with OIC's earlier submission.

Evidence of Identity - Agents (Review Report, recommendation 23, appendix 3)

The proposal seeks to amend the RTI Act to remove the requirement that agents must provide evidence of identity in all cases and instead, provide that an agency or Minister must not give access to a document containing personal information of the applicant, unless the agency or Minister is satisfied of the identity of the agent. The requirement to provide evidence of the agent's authorisation would be retained. OIC notes that the proposal to remove the requirements for agents to provide evidence of identity in all cases is a Review Report recommendation. In its submission to the 2013 Consultation, OIC recommended that the requirement to provide evidence of identity and authority be removed for legal representatives who have been retained by the applicant to act on the applicant's behalf. OIC did not recommend removing it for other agents.

Evidence of Identity – Applicants (Review Report, recommendation 23, appendix 3)

The proposal seeks to amend the RTI and IP Regulations to expand the list of qualified witnesses who can certify evidence of identity documents to include police officers, medical practitioners, registered nurses and registered teachers. This would make it easier for applicants to certify copies of identification documents.

OIC supports the proposed amendment.

Processing applications

Definition of processing period (Review Report, recommendation 23, appendix 3)

Proposal for change – A single period of time for processing applications.

Amendments are proposed to the RTI Act to provide for a single period of time for processing applications, which is increased to include any further period in which the agency is entitled to continue working on the application (i.e., replace the concept of a further specified period with an extension of the processing period). The processing period would be defined to include any additional time granted to an agency to make a considered decision under section 35. Any further time granted by an applicant, or time in which an agency is permitted to continue processing an application because the applicant has not refused the extension, would form part of the processing period.

In its submission to the 2016 Consultation, OIC recommended 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.

OIC notes this is a Review Report recommendation. OIC supports the proposal, noting it is largely consistent with OIC's previous submission, subject to the below addition.

OIC recommends amendment of 'processing period' also captures the decision-making period applicable to non-compliant applications (section 33(6) of the RTI Act and section 53(6) of the IP Act). Currently a 'processing period' is not enlivened where an application is not made in a form complying with application requirements, meaning that if an agency fails to issue a decision under 33(6) or 53(6), there is no reviewable decision in respect of which an applicant can seek review.[68] To remedy this, OIC recommends the processing period commence

[68] This issue was ventilated in Powell and Thwaites [2017] QCA 200 at [152] where the Court of Appeal observed: *Section 22 relevantly defines the processing period as a period of 25 business days from the day the application is received by the agency. It does not distinguish between a duly made application and an application having some formal defect. And that distinction would be problematic, because according to s 43(3), evidence of identity need not be provided with the application but could be provided within a further 10 business days. Nor does the definition of the processing period distinguish between the receipt of an application which the agency considers to be compliant and that of an application which it believes, rightly or wrongly, to be non-compliant.* A non-compliant application is not in this context a nullity: it still requires the action of the agency, under s 53 [of the IP Act] to dispose of it by a reviewable decision of the agency.

from the date an application is *received* (whether valid or not) and be suspended (similar to how a CEN suspends the processing period) by consultation with the applicant about what is required to make the application valid. As with all other matters, if the agency does not make a decision within the processing period, a deemed decision will be taken to be made, enlivening review rights to OIC. OIC notes that if this amendment is made, section 33(4) and 53(4) would need to be omitted as they would be redundant.

Application outside scope of Act – Timeframes (Review Report, recommendation 2)
Proposal for change – Extend the timeframe for a decision

An amendment to the RTI Act is proposed to extend the timeframe for a decision that a document or entity is outside the scope of the Act from 10 business days to 25 business days. This timeframe would not be able to be extended in the same way that the processing period for access decisions can be extended, which reflects the current position in the Act.

OIC supports simplifying the process for applicants and agencies with one timeframe for decision making. We also note that 10 business days can be inadequate for decisions of this nature. Where an application involves both documents that are within and outside the scope of the Act, the Act does not provide for an application to be 'split'.

Schedule of relevant documents (Review Report, recommendation 3)
Proposal for change – Remove the mandatory requirement for a schedule of documents

An amendment is proposed to the RTI Act to remove the mandatory nature of the requirement for applicants to be provided with a schedule of relevant documents, giving agencies and Ministers a discretion whether to provide one.

OIC notes this is a recommendation of the Review Report. In its submission to the 2016 Review OIC noted 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.

OIC does not object to the proposal.

Charges estimate notices (CENs) – Not required when no charges apply (Review Report, recommendation 23, appendix 3)
Proposal for change – No requirement for a CEN where no charges apply.

It is proposed to amend the RTI Act so that agencies are not required to give applicants a CEN where no charges apply.

OIC notes this is a Review Report recommendation.

CENs – Applicants limited to two (Review Report, recommendation 23, appendix 3)
Proposal for change – Limit of two CENs

An amendment is proposed to clarify that applicants are limited to two CENs. Any narrowing of the second CEN would not require a third CEN to be issued.

OIC notes this is a recommendation of the Review Report.

Additional time for documents sent by post (responding to Review Report, recommendation 11, appendix 3)
Proposal for change – Amendment to the definition of processing period

It is proposed to amend the definition of processing period in section 18, item 2, so that for decision notices that are only posted, five business days do not count towards the processing period. This would ensure that the processing period allows time for postal delivery times, which are beyond the control of the agency. It would also reduce the risk of a deemed decision. Applications which are emailed would not be affected.

OIC notes that this amendment will require agencies to treat applications differently and reprogram existing case management systems for a separate category of postal applications. While rare, OIC has also been advised of cases where decisions have been made and emailed on the last day of the processing period, documents later provided by the agency and subsequently found that the decision email was never sent due to problems with the server.

A key objective is to provide certainty for applicants, agencies and OIC whether the statutory timeframe for the decision has expired so appropriate action can be taken. An alternative approach could be to require that decisions are made within the processing period and that they be sent to the applicant as soon as practicable, or another appropriate period.

Public interest balancing test (Review Report, recommendation 7)
The proposal for change to amend the RTI is to make it clear that the factors listed in schedule 4 are not an exhaustive list of things that can be considered when applying the public interest test.

OIC supports the amendment to include an express statement to that effect.

Exemptions

Proposal for change – A new exemption for matters affecting relations with government
The proposal seeks to create a new exemption for matters affecting relations with other governments. As outlined in the Consultation Paper, the exemption would apply if disclosure of the information could reasonably be expected to cause damage to relations between Queensland and another government, or divulge information communicated in confidence by or for another government.

The Consultation Paper further notes that it is anticipated that this would protect communications in circumstances where disclosure may:

- cause difficulties in negotiations or discussions that are under way; or
- adversely affect the administration of a joint Commonwealth-State program; or
- affect the level of trust or cooperation in relationships between governments; or
- prejudice the supply of information between jurisdictions. The new exemption would be included in schedule 3.

In other jurisdictions where this information is exempt, the exemption is subject to a public interest test.

OIC observes that Schedule 4, part 4, item 1 of the RTI Act already provides that disclosure of information affecting relations with other government would raise a public interest factor favouring nondisclosure because of the public interest harm in disclosure. This harm factor is based upon the previous exemption in the section 38 of the repealed FOI Act, which exempted this category of information.

Schedule 3 of the RTI Act sets out the type of information which Parliament has considered to be 'exempt information' because its disclosure would, on balance, be contrary to the public interest. For example, Schedule 3, section 8 of the RTI Act provides that information will be exempt from release if its disclosure would found an action for breach of confidence.[69]

Where exemptions do not apply, a decision maker considers public interest factors favouring disclosure and non-disclosure and subsequently balances such interests. The identified concerns regarding disclosure of sensitive information, as outlined in the Explanatory notes, is relevant to some factors favouring nondisclosure in the public interest in Schedule 4, Part 3 and Part 4 of the RTI Act.

The former Attorney-General tabled the Review Report in Parliament in October 2017 following a comprehensive review, including public consultation. This Review Report recommended there be no further exemptions or exclusions and, in fact, recommended the removal of an existing exemption (Recommendation 6).[70] The Review Report concluded that 'the RTI Act already contains sufficient exemptions and exclusions and the flexible public interest balancing test allows for adequate protection of information where required. To add 'tailored' exemptions or exclusions directed at certain documents or agency functions may suggest that the RTI Act does not adequately protect other types of information.'[71]

In June 2008 the report on the wide-ranging review of the FOI Act by an independent panel chaired by Dr David Solomon AM was delivered (**the Solomon Report**). The Solomon report recommended an overhaul of Queensland's FOI laws including very limited exclusions and fewer legislated exemptions under the new RTI Act. In the Solomon Report, the Panel specifically argue against including exclusions to allay concerns about disclosure where exemptions or the public interest test can easily protect sensitive information.[72]

OIC provided submissions to the relevant Committees on the Mineral and Energy Resources (Financial Provisioning) Bill 2018[73] and the Brisbane Olympic and Paralympic Games Arrangement Bill 2021[74] raising concerns about proposed amendments to the RTI Act which sought to exclude certain documents from the operation of the RTI Act and noted in both submissions that the proposed amendments are inconsistent with the comprehensive Review Report tabled by the Attorney-General in October 2017 and the Solomon Report.

---

69 An action for breach of confidence can be an action for an equitable breach of confidence or a breach of a contractual obligation of confidence.

70 The only changes to exemption provisions were an amendment to an exemption provision to increase disclosure, and removal of the investment incentive scheme exemption.

71 Review Report, page 20.

72 FOI Independent Review Panel, The Right to Information: Reviewing Queensland's Freedom of Information Act, June 2008, (The Solomon Report), pages 100-104.

73 OIC Submission to the Economics and Governance Committee - March 2018

74 OIC Submission to the Economics and Governance Committee - Nov 2021

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. This is clearly reflected in the reservations made about the scope of exclusions and exemptions by the above reviews and more recently reflected in the recommendations and comments made in the Coaldrake Review.

The Coaldrake Review noted that the 2008 Solomon Report remains relevant for the way it sets out the 'purpose and principles underlying right to information' and 'some of the issues identified in that report, particularly those relating to culture remain relevant today.' The Final Report further noted that 'it is hoped that acceptance of this Review's recommendations, particularly the more ready release of Cabinet documents, and its comments on the need for greater scrutiny over what is deemed commercial-in-confidence, will provide the impetus for a cultural shift toward much more openness in government.[75] Importantly the Coaldrake Review commented that the 'community certainly tires very quickly when politicians, of any colour and in any jurisdiction, hide behind Cabinet or 'commercial-in-confidence' to fend off legitimate questioning on even routine matters.[76]

For the reasons outlined above, OIC does not support the creation of a new exemption for matters affecting relations with other governments.

Internal and external reviews

Review rights – courts and tribunals
OIC notes it is proposed to remove the right to internal and external review in relation to courts and tribunals exercise of judicial functions. The scope of the RTI Act is a policy matter for government. OIC notes that the right to appeal to the QCAT Appeal tribunal is retained.

Timeframes for internal review
The proposal seeks to amend the RTI Act to allow agencies to extend the time in which agencies must make internal review decisions, either by agreement with the applicant, or where third-party consultation is required. OIC does not object to the proposed amendment to the RTI Act if it is considered necessary to provide greater clarity and certainty for agencies and applicants and further notes it is a Review Report recommendation.

Disclosure of documents to other parties at external review
OIC supports the proposed amendment to the RTI Act to allow the Information Commissioner to disclose documents during an external review to third parties, to facilitate the resolution of an external review, including the proposal for the basis for such disclosure to correspond to section 37(1) and (2) of the RTI Act for an agency at first instance.

However, consistent with OIC's submission to the 2016 Consultation, OIC does not support changes to existing requirements regarding release of documents once an external review is finalised – that is – documents are released to an applicant by the agency on finalisation of the external review.

---

[75] Coaldrake Review Final Report 28 June 2022, page 29.
[76] Coaldrake Review Final Report 28 June 2022, page 28.

Release of documents following information resolution settlement
OIC supports the proposal to amend the RTI Act to clarify that an agency may release documents following an informal resolution of a review if it is considered necessary to provide further certainty and clarity to agencies and to provide a legislative basis for the release of documents in these circumstances.

Application of the RTI and IP Act

Prescribing entities under the RTI Act
This proposal seeks to amend section 16 of the RTI Act which sets out the definition of 'public authority'. OIC supports the proposal to include criteria to provide guidance on whether to prescribe an entity as a public authority under a regulation. Following the decision in *Davis v City North Infrastructure Pty Ltd* [2011] QSC 285, *Corporations Act* companies are excluded from the definition of public authority, whereas the proposal for change indicates that the amendment would clarify these companies can be prescribed. The factors listed in the consultation paper reflect the elements which would ordinarily be taken into consideration when considering the common law authorities on the definition of 'public authority'. The proposed amendment will assist increased transparency of State and local government-controlled entities which are performing public functions.

Contracted service providers
The proposal seeks to amend the IP Act to extend obligations in the IP Act to subcontractors. Contracted service providers would be required to take all reasonable steps to ensure a subcontracted service provider is contractually bound to comply with the privacy principles. Once bound the subcontractor would assume the policy obligations as if it were the agency. In the event of a breach, the privacy complaint would be made against the subcontractor. If the contracted service provider does not take all reasonable steps to bind the subcontractor to comply with privacy principles, the contracted service provider would be liable for any privacy breaches committed by the subcontractor.

The proposal mirrors the current provisions under Chapter 2, Part 4 of the IP Act with regards to requirements for binding a contracted service provider if the provision of services under the contract or other arrangement involves the exchange or handling of personal information in any way.

OIC supports extending obligations under the IP Act to subcontractors. This position is consistent with OIC's recommendation to the 2016 Consultation and notes it a Review Report recommendation. In its 2016 submission, OIC noted it considered section 95B of the Privacy Act may provide a useful model for extending privacy obligations to sub-contractors.

Organisations established by letters patent
Following the decision in *Stanway v Information Commissioner & Anor* [2017] QCATA 30, OIC wrote to the then Attorney-General to outline the implications of the decision for entities established by letters patent which OIC had previously considered excluded from the scope of the RTI and IP Acts. OIC maintains the view that if these entities were to fall within the scope of the RTI Act, dealing with access applications would impose an unsustainable administrative burden on these entities. OIC supports the proposal for change and considers that *'entities incorporated by way of letters patent'* be added to schedule 2, part 1 of the RTI Act.

Privacy Complaints – Requirements (Review Report, recommendation 17)
The proposal seeks to amend the IP Act to specify that privacy complaints to agencies are required to be in writing, state the name and address of the complainant, give particulars of the act or practice complained of and be made within 12 months of the complainant becoming aware of the act or practice the subject of the compliant. It is further proposed to provide for agencies to accept a complaint older than 12 months if it is reasonable in the circumstances.

OIC notes this is a Review Report recommendation. The proposal to specify how a privacy complaint must be made to an agency mirrors the requirements under section 166(1) of the IP Act for a privacy complaint made or referred to the Information Commissioner. The requirements proposed to be specified in the IP Act are largely consistent with other Australian privacy jurisdictions. OIC notes NSW[77] and the ACT[78] provide that a complaint can be oral or in writing and most jurisdictions include a requirement for necessary assistance to be provided to assist a person formulate a complaint.

OIC supports proposed amendments to the IP Act to specify requirements for making a privacy complaint to an agency. OIC recommends further consideration is given to whether imposing a requirement for a complaint to be in writing in consistent with the obligations placed on agencies under the HR Act. OIC recommends placing specific obligation on an agency to provide assistance, where necessary. OIC also recommends consideration is given to require the complaint to include complainant's telephone number.[79]

It is further proposed to provide for agencies to accept a complaint older than 12 months if it is reasonable in the circumstances. This is consistent with OIC's discretionary power to not accept complaints where more than 12 months has passed since the complainant first became aware of the practice the subject of the complaint.[80]

Privacy complaints – Timeframes (Review Report, recommendation 18)
The proposal seeks to allow agencies to request extensions of time for resolution of privacy complaints with the agreement of the complainant. OIC considers it is currently open to agencies to request extensions of time for resolution of privacy complaints with the agreement of the complainant under existing provisions of the IP Act. The IP Act does not impose time limits on an agency when dealing with a privacy complaint. The time limit of 45 business days under s166(3)(b) sets a minimum period of time that must elapse before an individual can make a privacy complaint to the Commissioner following the making of a complaint to the relevant entity. While OIC does not consider the proposed amendment is necessary, OIC does not object to the proposal if it is considered it will provide greater certainty for agencies and complainants.

OIC supports the proposal to amend the IP Act to allow a complainant to refer their complaint to OIC after they receive a written response from an agency in relation to their privacy complaint without having to wait for the 45 business days to expire. This will provide greater certainty and clarity to agencies and

[77] Section 45(3) *Privacy and Personal Information Protection Act 1988*.
[78] Section 35(1)(a) and section 35(2) *Information Privacy Act 2014.*
[79] As in section s35(1)(b) of the *Information Privacy Act 2014* (ACT).
[80] Section 168(1)(f) of the IP Act.

complainants about referral of privacy complaints to OIC and provide OIC with a discretion to accept privacy complaints based on specific circumstances. OIC notes the proposal is a Review Report and Strategic Review Report recommendation. It is also consistent with OIC's recommendation in its submission to the 2016 Consultation.

Privacy complaints – applications to QCAT (Review Report, recommendation 18)

Sections 175(b) and 176(1) of the IP Act do not currently impose an express time limit for a complainant to ask OIC for their privacy complaint to be referred to QCAT. OIC notes that the proposal is a Review Report recommendation and largely consistent with OIC's submission to the 2016 Consultation.

OIC supports the proposed amendment to the IP Act to impose an express time limit for a complainant to ask OIC to refer their privacy complaint to QCAT. In the interests of timeliness and efficiency in dealing with the complainant's privacy complaint, OIC proposes a timeframe of 28 days for the complainant to ask the Information Commissioner to refer a privacy complaint to QCAT for hearing from the day the Commissioner gives written notice that the Information Commissioner does not believe the complaint can be resolved by mediation. A time period of 28 days is consistent with the relevant provision in the *Judicial Review Act 1991*.[81] OIC also supports the proposal to provide a discretion for the Information Commissioner to extend the timeframe if reasonable in the circumstances.

The imposition of a time limit of 28 days in which an applicant can request the Information Commissioner refer a privacy complaint to QCAT for hearing will assist in facilitating a timely resolution of privacy complaints and prevent a situation from arising where a complainant requests OIC refer a privacy complaint several years after being advised of their rights to have their complaint referred to QCAT.

This issue recently arose in the matter of *Saunders v Department of Housing and Public Works* [2022] QCAT 159 in which there was a time period of at least 6 years and 10 months between the applicant being advised of his rights and a request that OIC refer the matter to QCAT. This case considered the issue of whether the time limit set out in section 38(4) of the *Acts Interpretation Act 1954* (Qld) (**AI Act**), namely 'as soon as possible', applies to the time within which a complainant may request the Information Commissioner to refer a privacy complaint to the QCAT upon being given advice of his or her rights to do so pursuant to sections 175(b) and 176(1) of the IP Act.

It was held that section 38(4) of the AI Act does apply to a request by a complainant to refer a complaint to QCAT made under ss 175(b) and 176(1) of the IP Act. It was held that Mr Saunders, who took almost seven years to refer his complaint to QCAT, did not request referral 'as soon as possible' and that QCAT had no jurisdiction in relation to his complaint. The tribunal decision noted that it may be desirable that the IP Act be amended to provide complainants with certainty in relation to the applicable time limit. The tribunal also noted that this is a matter for consideration by others.[82]

---

[81] Section 26(2).

[82] *Saunders v Department of Housing and Public Works* [2022] QCAT 159 at para [6.0].

NPPs and health agencies (Review Report, recommendation 22)
As outlined in the Consultation Paper, the IP Act currently provides that a law enforcement agency is not subject to IPP 2, 3,9,10, or 11 if the law enforcement agency is satisfied on reasonable grounds that noncompliance is necessary for specified law enforcement activities. The proposal seeks to provide an equivalent law enforcement exemption from compliance with the NPPs for health agencies with law enforcement functions.

Law enforcement agency is defined in schedule 5, paragraph (b) of the IP Act as:

(i) the Queensland Police Service under the Police Service Administration Act 1990 (Qld); or
(ii) the Crime and Misconduct Commission under the Crime and Misconduct Act 2001 (Qld); or
(iii) the community safety department; or
(iv) any other agency, to the extent it has responsibility for—

(A) the performance of functions or activities directed to the prevention, detection, investigation, prosecution or punishment of offences and other breaches of laws for which penalties or sanctions may be imposed; or
(B) the management of property seized or restrained under a law relating to the confiscation of the proceeds of crime; or
(C) the enforcement of a law, or of an order made under a law, relating to the confiscation of the proceeds of crime; or
(D) the execution or implementation of an order or decision made by a court or tribunal.

OIC does not object to the proposal if it is considered it is necessary for health agencies to undertake law enforcement related activities.

IPP 4 – Element of reasonableness (Review Report, recommendation 21)
The proposed amendment to require agencies to take reasonable steps in relation to the protection of personal information will be redundant should the proposed QPPs be adopted in Queensland (see QPP7). OIC supports amalgamating the IPPs and NPPs into a single set of privacy principles consistent with recommendations by the Review Report, Impala Report, OIC's submission to the 2016 Consultation and previous ALRC reports and reviews.

If a single set of privacy principles are not adopted in Queensland, OIC supports the proposed amendment to make it clear that an agency is required to take reasonable steps. Although OIC notes that this amendment may not be required as IPP 4 (2) only requires the protection referred to in (1) to be 'the level of protection that can reasonably be expected…".

Transferring personal information outside Australia (Review Report, recommendation 15)
The proposed amendment to regulate *disclosure of personal information* outside Australia rather than *transfer* of information will be redundant should the proposed QPPs be adopted in Queensland (see QPP9). OIC supports amalgamating the IPPs and NPPs into a single set of privacy principles consistent with recommendations by the Review Report, Impala Report, OIC's submission to the 2016 Consultation and previous ALRC reports and reviews.

If the IPPs and NPPs are not amalgamated, OIC supports the proposed amendment.

Definition of generally available information (Review Report, recommendation 20)
The proposal seeks to amend the definition of the IP Act to be consistent with the definition of generally available publication in the Privacy Act, while ensuring that generally available publications which are purely digital (for example, web pages, Twitter feeds, blog posts and Facebook posts) are captured in the definition.

OIC also notes the proposal is a Review Report recommendation. OIC supports the proposal which is consistent with the recommendation made by OIC in its submission to the 2016 Consultation.

Other issues

Disclosure logs – which documents to publish (Review Report, recommendation 8)
The proposal seeks to amend the RTI Act so that departments and Ministers are subject to the requirements that applied before the 2012 amendments. It is further proposed that disclosure log requirements are supported by Information Commissioner guidelines rather than Ministerial guidelines[83]

OIC supports the proposed amendments.

Disclosure logs – Information about applicants (Review Report, recommendation 9)
The proposal seeks to amend the RTI Act to remove the requirement to include on a disclosure log an applicant's name and whether an applicant has applied on behalf of another entity.

In its submission to the 2016 Consultation OIC, while not making an express recommendation about the above proposal, noted 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.

OIC notes it is a Review Report recommendation and does not object to the proposed amendments.

Publication Schemes (responding to Review Report, recommendation 10)
The proposal seeks to amend the RTI Act to require agencies to maintain a publication scheme without prescribing requirements for information to be published in a publication scheme or under specific 'classes' of information. It is also proposed to amend the RTI Regulation to require agencies to publish information they hold that is significant, appropriate and accurate. OIC notes it is proposed to remove the requirement to comply with the Ministerial guidelines.

The proposal is largely consistent with OIC's submission to the 2016 Consultation. OIC recommended retaining the legislative requirement for a publication scheme however did not consider it was necessary to prescribe the classes of information that must be included in any publication scheme.

OIC supports the proposed amendments.

[83] Section 78B RTI Act.

Annual reporting requirements (Review Report, recommendation 12; Strategic Review Report, recommendation d))

The proposal seeks to amend the annual reporting requirements by transferring legislative responsibility for preparing the annual reports from the responsible Minister to the Information Commissioner. It is further proposed that the information which must be included in the annual report continue to be prescribed under the RTI and IP Regulation.

This proposal is largely consistent with OIC's recommendation in its submission to the 2016 Consultation. However, in its submission OIC further recommended that OIC enter into detailed discussions with the Department of Justice and Attorney-General regarding transferring responsibility for reporting to OIC. This will allow issues such as identified resourcing impacts on OIC, a suitable transition period and potential ICT solutions to be addressed to ensure an efficient and seamless transfer of reporting requirements to OIC.

The 2017 Strategic Review of OIC subsequently recommended that 'OIC be funded and supported to administer the collection and collation of performance reporting by agencies under the Acts. Reporting requirements should be rationalised to maximise value and minimise collection effort'.[84]

With regards to the type of information prescribed under the RTI and IP Regulation, the matters listed in the Consultation Paper are largely consistent with OIC's submission to the 2016 Consultation. In particular, OIC welcomes the inclusion of reporting requirements for agencies and Ministers on the number of privacy complaints received by each agency and the outcomes of these complaints and data relating to push model initiatives and proactive release of information.

A significant development since the 2016 Consultation is release of Australia's first Open Government National Action Plan 2016-2018 (**NAP**).[85] This NAP included a commitment to develop uniform metrics on public use of freedom of information (FOI) access rights (Commitment 3.2) to promote the importance of better measuring and improving our understanding of the public's use of rights under freedom of information laws.

The Information and Privacy Commission NSW (IPC) led the development of the metrics on behalf of and with the involvement of the Commonwealth, state and territory Information Access Commissioners and Ombudsmen within the remit of their jurisdictions (the Association of Information Access Commissioners – AIAC). NSW IPC updates the dashboard each year once all jurisdiction data has been reported.[86]

The current Queensland annual reporting requirements for the RTI and IP Acts do not align with some elements of the metrics reported on under commitment 3.2. For example, Metric 1: Type of applicant, Metric 3: release rates, Metric 4: Refusal rates and Metric 5: Timeliness. This is due in part to the number of access applications received by Ministers and agencies in a financial year are currently not broken down by applicant type and current reporting of the combined total number of *pages* considered and percentage of *pages* released in full or part.

---

84 https://documents.parliament.qld.gov.au/tp/2017/5517T698.pdf, recommendation d.

85 https://ogpau.pmc.gov.au/sites/default/files/publications/australias-first-open-government-nap.pdf.

86 https://www.ipc.nsw.gov.au/sites/default/files/2022-.06/OGP_Metrics_all_jusridictions_all_years_June_2022.pdf.

This limits the utility of the data reported on the metrics due to differences in data compared to other jurisdictions. Aligning the data to the metrics will also decrease the potential to infer adverse perceptions about the operation of the Queensland legislation where people do not understand the differences in how the metrics are calculated due to the limitations of the data (despite notations). OIC recommends aligning the prescribed matters required to be reported on the Annual Report under the RTI Regulation with the metrics under Commitment 3.2 of the NAP.[87] OIC has previously raised this matter with the former Attorney-General and Minister for Justice.[88] OIC notes that some of proposed prescribed data appears to align with required metrics. Timeliness data is an area Queensland is currently unable to report on in the metrics, and of key concern to many stakeholders given the increase in decisions not made within statutory timeframes and being reviewed by OIC.

The proposed prescribed data includes data relating to RTI Act push model initiatives. Administrative access data is a key area to consider given the critical impact on the community and as a driver for demand to the last resort of formal access applications under the push model.

OIC also notes that consultation with affected stakeholders, adequate implementation time and an effective technological solution to collect, assist in analysis and reporting of the data will be critical.

Reports to the Speaker (Review Report, recommendation 11, appendix 3)
The proposed amendment is to ensure consistency between the IP Act and RTI Act with respect to the ability of the Information Commissioner to report on systemic issues. The Information Commissioner currently has the power under the IP Act, but not the RTI Act.

OIC supports this amendment in principle that the Information Commissioner should have a power to report to Parliament under both the IP Act and the RTI Act on systemic issues. However, OIC recommends that consideration be given to amending the reporting function under both the RTI Act and the IP Act be to OIC's parliamentary oversight committee.

This approach is consistent with previous OIC recommendations that section 135(1)(a)(ii) of the IP Act be amended to be consistent with section 131(2) of the RTI Act to refer to reporting to the parliamentary oversight committee.

[87] IPC NSW Metrics on Public Use of Freedom of Information Access Rights.
[88] Correspondence dated 2 March 2017.

APPENDIX A

RTI Act

Remittal power

OIC's submission to the 2016 Consultation recommended that the RTI Act provide OIC with a discretion to remit applications to agencies/Ministers, in certain circumstances, for example:

- where further searches instigated by OIC have located documents and a de novo decision regarding those documents is required
- 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 (e.g. refusal to deal provisions in sections 40, 41 and 43 of the RTI Act).

OIC continues to advocate for inclusion of a remittal power in the above circumstances and also in the case of deemed decisions.

A remittal power would assist in reducing external review demand, promote more timely outcomes for applicants to the extent that agencies/Minister are required to make decisions within a legislative timeframe, and provide agencies/Ministers with a further opportunity to exercise their discretion to release information.

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

Schedule 2, section 195 RTI Act – State Security Operations Group

Schedule 3, section 10(5)(b) of the RTI Act refers to the 'State Security Operations Group'. Queensland Police Service (QPS) has confirmed that the State Security Operations Group (**SSOG**) no longer exists and the functions of the SSOG moved to the Security Investigations Team. OIC recommends consulting with QPS and amending section 10(5)(b) of the RTI Act to remove reference to the SSOG and replace it with the appropriate title to avoid uncertainty around the application of section 10(5)(b) of the RTI Act.

Internal review – sufficiency of search

Since commencement of the RTI and IP Acts, agency decision makers have raised concerns that the legislation does not give them jurisdiction to conduct an internal review solely on the ground of sufficiency of search, i.e., where an applicant contends that more documents should exist.

Agencies have the power to conduct an internal review in relation to a 'reviewable decision'. However, the definition of 'reviewable decision' in schedule 5 of the RTI and IP Acts does not extend to decisions granting full access to documents, but where an applicant alleges more documents should exist.

On external review, OIC gains its jurisdiction on sufficiency of search matters through section 130 of the RTI Act and section 137 of the IP Act which provide for OIC to investigate whether an agency has taken all reasonable steps to

locate relevant documents. OIC considers this jurisdiction should be afforded to agencies as they are best placed to search for more documents responding to an application and allowing them to do so within the timeframe of an internal review would contribute to more efficient outcomes for applicants and limit the number of such applications coming on external review.

OIC recommends that Part 8 of Chapter 3 of the RTI and IP Acts which deal with Internal Review, be amended to expressly provide agencies with this jurisdiction, potentially as a stand-alone section or as an additional "Note" in section 80 of the RTI Act and section 94 of the IP Act.

Appeal to QCAT on a question of law – section 119 RTI Act and 132 IP Act

Section 119(2) RTI Act provides that an appeal of a decision of the information commissioner in an external review may only be on a question of law, while section 119(5) RTI Act provides that the appeal may only be by way of rehearing.

A number of QCAT decisions have expressed unease regarding section 119(5), and then gone on to conclude that – despite its reference to 'rehearing' (which generally relates to questions of fact and can include the hearing of additional evidence) – the basis of an appeal under section 119 is only on a question of law, and in the nature of judicial review.[89] To provide certainty and avoid the need for further consideration of this issue by QCAT, OIC recommends omission of section 119(5). Removal of section 119(5) would not alter the right of appeal in any way.

The QCAT decision in *Walker Group Holdings Pty Ltd v Queensland Information Commissioner (No 2)* [2021] QCATA 84 (19 July 2021) has significant implications for the Information Commissioner's role in appeal proceedings. QCAT found that the Information Commissioner, as the decision-maker of the decisions under appeal under the RTI Act, should *not* have been made a party to the appeal proceedings. QCAT has since issued the decision of *Stiles v Information Commissioner* [2021] QCATA 152, which also removed OIC as a respondent to an appeal under the IP Act (generally following the reasoning in *Walker*). QCAT has issued directions to remove OIC as a party in two further appeal proceedings.[90] There is nothing to suggest that QCAT will resile from this position which, in OIC's view, is the correct position. To ensure that it is clearer to appellants that OIC should not be incorrectly named as a party in appeals, which on each occasion necessitates OIC making a miscellaneous application to be removed, OIC recommends that section 119 RTI Act / 132 IP Act be amended to confirm that the Information Commissioner is not a participant in an external review.[91]

---

89 Thomas J in *Marshall-Holst v Office of the Information Commissioner and Queensland Health (Metro North Hospital and Health Service)* [2017] QCATA 28 at [31]-[33] and *Sibelco v Right to Information Commissioner* [2017] QCATA 59 at [3]-[4] and [19]-[27]; and Daubney J in *Kelson v Queensland Police Service & Anor* [2019] QCATA 67 at [23].

90 Where the other parties had not objected to such removal. In terms of yet to be heard appeals, an oral hearing about OIC's removal application in two related appeals has been set down, while all other appeals await directions.

91 This could be in a new subsection, or perhaps as a note after 119(3)(b) / 132(3)(b) which cross-references section 89 RTI Act / 101 IP Act.

Representative Actions

In its submission to the 2016 Consultation, OIC recommended consideration is given to amending the IP Act to provide for representative privacy actions. Section 164(1)(a) of the IP Act currently 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'.[92] 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. OIC considers this amendment to the IP Act to provide for representative actions is critical to support the proposed introduction of a mandatory DBN scheme in Queensland. This will assist in providing administrative efficiencies for both agencies and complainants, particularly in circumstances where large numbers of individuals are affected by a large data breach. Recent examples in Queensland include the recent data breach by the Queensland State Penalties Enforcement Registry which resulted in Enforcement Notices containing people's personal information to be sent out about unpaid fines to the wrong person.

The proposed amendment is consistent with privacy laws in other Australian jurisdictions. For example, section 57(3) of the *Privacy and Data Protection Act 2014* (Vic) 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 *Information Privacy Act 2014* (ACT)[93] and the Privacy Act[94] provide 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 and Commonwealth provisions differ from the Victorian provision as there is no consent requirement.

Section 167 of the IP Act – preliminary inquires

Section 167 of the IP Act provides that the Information Commissioner may make preliminary inquiries of the complainant 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.

In its submission to the 2016 Consultation, OIC recommended amending section 167 of the IP Act to provide OIC with suitable powers to make preliminary inquiries under the IP Act. OIC recommends amending section 167 to clarify that the Information Commissioner may make preliminary inquiries of the complainant and the respondent or any other person. This is consistent with

[92] Schedule 1.
[93] Section 34(2).
[94] Section 36(2).

relevant provisions of the *Information Privacy Act 2014* (ACT)[95] and section 62(3)(a) and (b) of the *Privacy and Data Protection Act 2014* (Vic).[96]

OIC further recommends that the power to compel documents and/or attendance of any person with relevant information extends to making preliminary inquiries under section 167 of the IP Act. Currently, under section 197 of the IP Act, if the Information Commissioner is satisfied on reasonable grounds that a person has information relevant to a decision about whether to give an agency a compliance notice or the mediation of a privacy complaint, the Information Commissioner may compel production of documents or attendance before the Commissioner.

OIC recommends that the Information Commissioner's power to compel production or attendance extends to preliminary inquiries under section 167 of the IP Act. This will assist in dealing with privacy complaints in a timely manner and support OIC's oversight role of the proposed mandatory DBN scheme in Queensland. As outlined earlier, this is consistent with relevant provisions of Victorian privacy legislation.[97]

Protections for persons compelled to produce information or appear before IC during mediation or compliance notice

Section 197 of the IP Act provides the Information Commissioner with the power to compel a person to provide either written or verbal information relevant to the decision to give an agency a compliance notice or the mediation of a privacy complaint under Chapter 5.

Under section 187 of the IP Act, it is an offence to fail to comply with a section 197 notice without reasonable excuse. OIC recommends reviewing the relevant provisions to ensure a person is provided with the necessary protections when compelled to provide either written or verbal information under section 197 of the Act and consistency with relevant provisions of the RTI Act.

Definition of relevant entity

Currently, *relevant entity* is defined for the purposes of Chapter 5 of the IP Act to mean an agency, in relation to the documents of the agency or a bound contracted service provider, in relation to documents held by the bound contracted service provider for the purposes of performing its obligations under a service arrangement.

IPP11(1) provides that:

> an agency having control of a document containing an individual's personal information must not disclose the personal information to an entity (the **relevant entity**), other than the individual the subject of the personal information unless –

In *Zil v Queensland Police Service* [2019] QCAT 79, the tribunal was not satisfied that IPP 11 had been breached *as the disclosure was to an individual,*

---

95 Section 38 of the Act 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.

96 Section 62(3)(a) and (b) provides that before declining to entertain a complaint, the Information Commissioner may, by notice in writing invite any person to attend before the Information Commissioner or to produce any documents specified in the notice.

97 See section 62(3)(a) and (b).

not as required by that IPP to an entity.[98] This decision has a number of implications for finding there is a breach of IPP11 where there is unauthorised disclosure of personal information by an agency to an individual.

NPP2 does not refer to the term 'entity' or 'relevant entity'. It provides that a health agency must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless -

OIC recommends reviewing the use of the term 'entity' and 'relevant entity' in the IP Act to ensure there are no unintended consequences flowing from the current drafting, noting that this issue would be redundant should the QPPs be adopted in Queensland.

Sections 188 IP Act and 179 RTI Act – Authorised disclosure of information
Currently when officers employed at OIC come into possession of information in the performance of their functions they are not permitted to disclose that information for a purpose other than:

- for the purposes of the Acts, or
- a proceeding arising under the Acts.

Contravening this section is an offence punishable by up to 100 penalty units. On occasions OIC officers receive information from members of the public or complainants which relate to threats of violence against them or others, or self-harm. A strict reading of ss.188 and 179 of the IP Act and RTI Acts respectively do not allow OIC to initiate the disclosure this information for the prevention, detection or investigation of criminal offences, serious improper conduct or to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or the public health, safety or welfare. It is recommended that an exemption should be provided to authorise the disclosure of information in the above circumstances.

Yours sincerely

Rachael Rangihaeata
Information Commissioner

[98] page 12.