Consultation Paper

Proposed changes to Queensland's Information Privacy and Right to Information Framework

June 2022

Queensland Government

The Queensland Government is committed to providing accessible services to Queenslanders from all culturally and linguistically diverse backgrounds. If you have difficulty understanding this discussion paper, you can contact us on 13 QGOV (13 74 68) and we will arrange an interpreter to effectively communicate the paper to you.

Message from the Attorney-General, Minister for Justice, Minister for Women and Minister for the Prevention of Domestic and Family Violence

In Queensland, and indeed around the world, technological developments are impacting on information privacy and access to personal information, and it's crucial our legislation remains contemporary and relevant.

After more than a decade of successful operation, Queensland's *Information Privacy Act 2009* and *Right to Information Act 2009* are well-established elements of our integrity framework that have served us well. However, it is important that this legislation continues to meet the needs of Queenslanders in the modern world.

Both pieces of legislation are essential to the functioning of our modern society. The Information Privacy Act provides a right for people to access and to amend their personal information. It also establishes the framework that governs how agencies collect, use, store and disclose personal information.

Importantly, it allows individuals who believe their personal information has not been handled in accordance with the privacy principles to make a complaint. The community needs to have confidence in how government conducts itself, and this framework is critical to gaining and retaining the community's trust in its information-handling practices.

The Right to Information Act is similarly important in our open and democratic society. The object of the Act is to provide *a right of access to information in the government's possession or under the government's control, unless on balance, it is contrary to the public interest to give the access*. A record number of access and amendment applications in the past financial year (2020-2021) shows just how much Queenslanders rely on this important legislation.

In considering potential improvements to the legislation, two recent reports are critical. Following its first statutory review, *the Report on the Review of the Right to Information Act 2009 and Information Privacy Act 2009* (the Review Report)[1] was released in 2017. The Review Report found that while Queensland's framework for right to information and information privacy was working well overall, there were opportunities for improvement.

Respect for personal information goes hand-in-hand with transparency and accountability. In 2020, the Crime and Corruption Commission released *Operation Impala: Report on misuse of confidential information in the Queensland public sector* (the Operation Impala Report).[2]

The report highlighted the serious impacts on individuals of a misuse of personal information by public sector agencies, and the breach of trust represented by that misuse.

[1] Tabled in the Legislative Assembly 12 October 2017.
[2] Tabled in Parliament 21 February 2020.

Both the Review Report and the Operation Impala Report made a number of recommendations. This Consultation Paper accordingly seeks views on whether significant changes should be made to Queensland's legislative framework for information privacy to enhance protections for personal information and remedies to individuals whose privacy is breached. It also proposes a series of reforms to the Right to Information Act and Information Privacy Act, to clarify and streamline the Acts' provisions in accordance with most of the recommendations in the Review Report.

A separate Consultation Paper will seek agencies' views about the benefits and impacts of both a mandatory data breach notification scheme and a single set of privacy principles in Queensland. I invite everyone to contribute to these important issues by making a submission and look forward to having their feedback.

Hon Shannon Fentiman MP
Attorney-General and Minister for Justice, Minister for Women and
Minister for the Prevention of Domestic and Family Violence
June 2022

Contents

Abbreviations

Abbreviation	Definition
ACCC	Australian Competition and Consumer Commission
ACCC Report	Australian Competition and Consumer Commission's report, *Digital Platforms Inquiry – Final Report*
AIC	Australian Information Commissioner
ALRC	Australian Law Reform Commission
APPs	Australian Privacy Principles
CCC	Crime and Corruption Commission
CEN	Charges Estimate Notice
Corporations Act	*Corporations Act 2001*
CP Act	*Child Protection Act 1999*
Criminal Code	*Criminal Code Act 1899*
Mandatory DBN Scheme	Mandatory Data Breach Notification Scheme
EU GDPR	European Union General Data Protection Regulation
HR Act	*Human Rights Act 2019*
ICT	Information and Communication Technology
Impala Report	*Operation Impala, A report on misuse of confidential information in the Queensland public sector*
IP Act	*Information Privacy Act 2009*
IPPs	Information Privacy Principles
IP Regulation	*Information Privacy Regulation 2009*
NPPs	National Privacy Principles
OAIC	Office of the Australian Information Commissioner
Privacy Act	*Privacy Act 1988* (Cth)
QCAT	Queensland Civil and Administrative Tribunal
QGEA	Queensland Government Enterprise Architecture
QHRC	Queensland Human Rights Commission
QLRC	Queensland Law Reform Commission
QPPs	Queensland Privacy Principles
Review Report	*Report on the Review of the Right to Information Act 2009 and the Information Privacy Act 2009*
RTI Act	*Right to Information Act 2009*
RTI Regulation	*Right to Information Regulation 2009*
Strategic Review Report	*Strategic Review of the Office of the Information Commissioner*
Windage Report	*Culture and Corruption Risks in Local Government: Lessons from an investigation into Ipswich City Council*

Introduction

Purpose

The Queensland Government is considering whether certain changes should be made to the framework for information privacy (which regulates how public sector agencies handle personal information) and right to information.

The purpose of this Consultation Paper is to consider:

Part A	**Information privacy reforms** To consider whether key changes should be made to Queensland's information privacy framework to better protect personal information and provide appropriate remedies and responses for the misuse of personal information by public sector agencies.
Part B	**Right to information and information privacy reforms** To consult on proposed changes to Queensland's information privacy and right to information framework to clarify and improve the operation of that framework.

Why are these changes being considered?

A number of reports have made recommendations for change to Queensland's information privacy and right to information framework including:

- the report on the *Review of the Right to Information Act 2009 and Information Privacy Act 2009* (Review Report);[3]
- the Crime and Corruption Commission (CCC)'s report, *Operation Impala, A report on misuse of confidential information in the Queensland public sector* (Impala Report);[4]
- the CCC's report, *Culture and Corruption Risks in Local Government: Lessons from an investigation into Ipswich City Council* (Windage Report);[5] and
- the *Strategic Review of the Office of the Information Commissioner* (Strategic Review Report).[6]

This Consultation Paper considers certain recommendations for change from these reports.

[3] Tabled in the Legislative Assembly 12 October 2017.
[4] Tabled in the Legislative Assembly on 21 February 2020.
[5] Tabled in the Legislative Assembly on 14 August 2018.
[6] Tabled in the Legislative Assembly on 11 May 2017.

Principles relevant to proposed reform

Individuals have a right to have their personal information protected from unlawful and arbitrary interference.

This is consistent with the right to privacy in the *Human Rights Act 2019* (Qld) (HR Act).

Appropriate support, remedies and responses should exist in relation to the misuse/unauthorised disclosure of personal information.

The law should provide a range of means to prevent, reduce or redress serious breaches of privacy and it should facilitate appropriate access to justice for those affected.

Members of the public should have access to information held by government.

This is consistent with the right to freedom of expression in the HR Act and is central to achieving accountability and transparency in government.

Consumers, businesses, and agencies should have clarity about their rights and obligations under privacy and right to information law.

The law should be precise and certain, but also flexible and able to adapt to changes in social and technological conditions.

As far as possible, there should be consistency in privacy rights and obligations across jurisdictions and information types.

Consistency in laws of different jurisdictions will lessen compliance burdens and costs and make it easier for individuals wanting to make a privacy complaint.

How to get involved

You may wish to comment on all of the issues set out in the Consultation Paper, or only the issues that are of particular interest to you. You can provide comments or make a submission by:

Email:
PrivacyandRTIreforms@justice.qld.gov.au

Mail:
Privacy and Right to Information Reforms
Strategic Policy and Legal Services
Department of Justice and Attorney-General
GPO Box 149
Brisbane, Qld 4001

Submissions close at 5pm on 22 July 2022

Privacy Statement: Personal information in your comments or submission will be collected by the Department of Justice and Attorney-General (DJAG) for the purpose of informing reforms to right to information, privacy and other legislation in Queensland. DJAG may contact you for further information on the issues your raise. Your comments or submission may also be provided to others with an interest in the reforms, for example, Parliament's Legal Affairs and Safety Committee. Comments and submissions in relation to this consultation paper will be treated as public documents and may be published on DJAG's website. If you would like your submission, or any part of it, to be treated as confidential, please indicate this clearly. **Please note however that all submissions may be subject to disclosure under the *Right to Information Act 2009*.**

Consultation questions

Below is a list of all the consultation questions in the Consultation Paper. However, any comments on the proposed reforms are welcome.

Part A: Proposed Privacy Reforms

Definition of Personal Information

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)?*

A Single Set of Privacy Principles

2. *Should the proposed Queensland Privacy Principles (QPPs) be adopted in Queensland?*
3. *If not, in what ways should they be changed?*

Reasonable Steps for the protection of personal information

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?*
5. *Could these factors be applied to other relevant parts of the IP Act?*
6. *Would statutory guidelines produced by Office of the Information Commissioner (OIC) be more flexible and useful?*

Enhanced powers for the Information Commissioner to respond to privacy breaches

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

Mandatory data breach notification (DBN) scheme

11. *Is the mandatory DBN scheme as outlined in this Consultation Paper suitable for adoption in Queensland?*
12. *If not, in what ways should it be changed?*
13. *Would the Information Commissioner require any additional powers to monitor and provide oversight to the mandatory DBN scheme?*

Criminal sanctions for misuse of personal information by public officers

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?*
15. *Do you have any other comments about this issue?*

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

Feedback is sought on the proposed right to information and information privacy reforms, including to both the IP Act and the RTI Act outlined in this part.

Queensland's Information Privacy and Right to Information Framework

The RTI Act and the IP Act

Queensland's framework for right to information and information privacy includes the RTI and IP Acts. The *Right to Information Act 2009* (RTI Act) provides a right of access to government information unless, on balance, it is contrary to the public interest to release the information. The IP Act contains privacy principles governing the collection, storage, transfer, use and disclosure of personal information in the public sector. It also provides a formal mechanism for a person to apply to access or amend their own personal information.

The OIC is an important part of Queensland's information privacy and right to information framework. The OIC is an independent body established to promote access to government-held information and protect personal information held by the public sector.

The importance of right to information and information privacy regulation

Right to information and freedom of information laws

Right to information and freedom of information laws play an important role in modern democratic societies. They are recognised as a means of achieving greater participation in government decision-making and greater accountability by government for the decisions they make. The repealed *Freedom of Information Act 1992* (the FOI Act) was passed following recommendations made by the Fitzgerald Inquiry,[7] the Electoral and Administrative Review Commission[8] and the Parliamentary Committee for Electoral and Administrative Review.[9]

Following an extensive review of Queensland's freedom of information laws by a panel of experts chaired by Dr David Solomon, AM[10] the FOI Act was replaced by the RTI Act and the IP Act.

All Australian jurisdictions, as well as many other countries, have right to information or freedom of information legislation. Its democratic purpose is to confer a legal right of access to information held by the government unless disclosure is contrary to the public interest.

It is broadly acknowledged that this legislative right:

- provides a mechanism for individuals to see what information is held about them on government files and to seek to correct that information if it is wrong or misleading;
- enhances the transparency and accountability of policy-making, administrative decision-making and government service delivery; and

[7] Report of A Commission of Inquiry pursuant to Orders In Council, delivered 3 July 1989.
[8] Report on Freedom of Information, 1990.
[9] Freedom of Information for Queensland, Review No 6, 18 April 1991.
[10] The Right to Information - Reviewing Queensland's Freedom of Information Act, June 2008.

- provides for a community that is better informed and thus able to participate more effectively in the nation.[11]

Privacy legislation

Closely related to the right to information held by government are specific rights in relation to the handling of personal information by government. All Australian jurisdictions, except Western Australia and South Australia, have privacy legislation that regulates the handling of personal information by government.

Other applicable laws/frameworks

The HR Act

Queensland's HR Act protects 23 human rights. The right to privacy (section 25) protects privacy in a broad sense, including personal information and data collection. Individuals have a right not to have their privacy unlawfully or arbitrarily interfered with. This means any interference with their privacy must not only be lawful but also not capricious, unpredictable, unjust or unreasonable (in the sense of not being proportionate to a legitimate aim that is sought). The protection of the right to privacy expresses the fundamental values of 'physical and psychological integrity, and the autonomy and inherent dignity of the person.'[12] There is a strong connection between dignity, personal identity and autonomy and a person's name, including the collection and use of personal information.[13]

The right to freedom of expression (section 21) includes the right to seek and receive information from government.[14] The importance of freedom of expression to a democratic system of government is recognised in both human rights and the common law where it has been stated that: 'In a democracy it is the primary right: without it an effective rule of law is not possible.'[15]

The HR Act requires each arm of government to act compatibly with human rights. This means that parliament must consider human rights when proposing and scrutinising laws, that courts and tribunals must, so far as is possible to do so, interpret legislation in a way that is compatible with human rights, and that public entities must act and make decisions in a way that is compatible with human rights.

The Privacy Act

Queenslanders' privacy is also protected by the Privacy Act, which contains Australian Privacy Principles (APPs) which protect personal information where it is collected and handled by 'APP entities'. These 'APP entities' include Commonwealth agencies and organisations, businesses with an annual turnover of more than $3 million, private sector health service providers, credit reporting bodies and businesses that sell or purchase personal information. The Privacy Act does not generally apply to Queensland agencies, however Government Owned Corporations (GOCs) under the *Government Owned Corporations Act 1993* are APP entities and are subject to the APPs.

---

[11] OAIC, Freedom of Information Guide (www.oaic.gov.au/freedom-of-information/guidance-and-advice/foi-guide/part-a-freedom-of-information-past-and-present/#_ftn17); Electoral and Administrative Review Commission, Report on Freedom of Information (December 1990).
[12] *Re Kracke and Mental Health Review Board* (2009) VAR I, 27 (Bell J, 29); VSC 52 (Bell J, 129-130).
[13] *DPP v Kaba* [2014] VSC 52.
[14] *XYZ v Victoria Police* [2010] VCAT 255, 554 (Bell J).
[15] *R v Secretary of State for the Home Department; Ex parte Sims* [2000] 2 AC 115 (Lord Steyn, 126).

Other confidentiality provisions

Many legislative provisions across the Queensland statute book also regulate how information is collected, stored, used and disclosed. These provisions generally prohibit the use or disclosure of personal information gained in the administration of the legislation unless an exception applies.[16]

Information Security Policy

Queensland Government departments and statutory bodies are required to consider the Queensland Government Enterprise Architecture (QGEA) – the digital and Information and Communication Technology (ICT) strategies, policies and publications that guide agency digital and ICT investments. The Information Security Policy (IS18:2018) under the QGEA *seeks to ensure all departments apply a consistent, risk-based approach to the implementation of information security to maintain confidentiality, integrity and availability.*

The Information Security Policy requires departments to meet stringent information security requirements. These include compliance with the Queensland Government Information Security Classification Framework, a data encryption standard, and an Authentication Framework.[17] They must also implement an Information Security Management System to protect all information, application and technology assets.

[16] Examples include *Hospital and Health Boards Act 2011* (s 142); *Child Protection Act 1999* (ss 186 to 189B); *Fisheries Act 1994* (s 217B).
[17] Other statutory bodies under the *Financial and Performance management Standard 2019* must also have regard to certain elements of the policy.

Part A: Proposed Privacy Reforms

This part seeks feedback on whether key changes should be made to **Queensland's information privacy framework** to **better protect an individual's personal information** and provide appropriate **remedies and responses** for the misuse of personal information by public sector agencies.

Information Privacy – Key themes and developments

Common themes in privacy

A number of recent reports both in Queensland and elsewhere have raised common themes about the handling of personal information by public sector agencies.[18] These include:

- the increasing breadth of personal information held by public sector agencies (including personal details such as residential addresses, phone numbers, emails, court orders, information about children, medical information and financial information);
- growing community expectations that personal information should be respected and kept private by agencies authorised to collect, store and use it;
- the serious impacts on individuals of misuse of personal information by public sector agencies, and the breach of trust represented by that misuse; and
- that personal data is an increasingly valuable commodity and may be sought and exploited by commercial enterprises seeking market advantage or an extended consumer base, or even stolen or appropriated for use in criminal activity such as identity fraud and cybercrime.

The Impala Report detailed the serious impacts that a data breach can have on an individual including embarrassment, distress, reputational harm and financial loss. It also highlighted the case of *Zil v Queensland Police Service* [2019] QCAT 79 which involved a police officer's disclosure of Zil's residential address to her ex-husband where there was a history of domestic violence. Misuse of confidential information in cases of domestic and family violence can not only impact a person's safety and cause distress and psychological harm but, as the Impala Report detailed, may also have other wide-ranging impacts including incurring costs associated with moving to a new house; children having to change schools; and change of employment.[19]

The Impala Report recommended legislative change (including to the IP Act) to provide enhanced remedies and responses for victims of the misuse of confidential information.

The Review Report also made a number or recommendations for legislative change or further research into whether changes should be made to Queensland's framework for protection of personal information.

[18] Impala Report; *For Your Information: Privacy Law and Practice*, Report 108, 2008 (ALRC 2008).
[19] Impala report, p 45.

Recurring recommendations

This part addresses a number of recommendations arising from the recurring themes in the various privacy reports and reviews including:

- **updating the definition of 'personal information'** to be more flexible and technology neutral (including to capture a variety of technical data collected in relation to individuals) and for consistency with the Privacy Act;[20]
- **a single set of privacy principles** based on the Commonwealth APPs;[21]
- **enhanced powers for the Information Commissioner to respond to privacy breaches** including an own motion power to investigate an act or practice without having received a privacy complaint; and an *amicus curiae* role in relation to privacy complaint proceedings in the Queensland Civil and Administrative Tribunal (QCAT);[22]
- a **mandatory DBN scheme** for Queensland to improve the protections and remedies available to victims who have had their personal information unlawfully accessed and/or disclosed by public sector employees;[23] and
- **a new criminal offence in the Criminal Code** for offending related to misuse of confidential information.[24]

Out of scope

This Consultation Paper **will not** address the following areas/recommendations:

- **A statutory tort for invasion of privacy**
  This was a recommendation made in a number of reports, including the Impala Report.[25] It is understood that as part of the review of the Privacy Act, the Commonwealth Government is considering whether there should be a similar statutory tort in Australia. Consideration at the Commonwealth level would arguably lead to greater consistency and uniformity in approach.
- **A new statutory scheme for civil surveillance**
  This was recommended by the Queensland Law Reform Commission (QLRC) in its report, *Review of Queensland's Laws relating to civil surveillance and the protection of privacy in the context of current and emerging technologies*.[26] While the RTI and IP Acts relate to the handling of personal information by government, the QLRC Report has a much broader scope, focused on privacy of location and space in the broader community as impacted by both the actions of government and private individuals and organisations. Queensland's current legislation, the *Invasion of Privacy Act 1971*, reflects the current regulatory response in this space but is currently limited in its application to listening devices.

[20] Impala Report, recommendation 16(2); Review Report, recommendation 14.
[21] Impala Report, recommendation 13; Review Report, recommendation 13 (*Conduct further research and consultation to establish whether there is justification for moving towards a single set of privacy principles in Queensland, and whether a mandatory breach notification scheme should be introduced*).
[22] Impala Report, recommendation 14(2); Review Report, recommendation 19.
[23] Impala Report, recommendation 12; Review Report, recommendation 13 (see footnote 21).
[24] Impala Report, recommendation 10.
[25] ALRC, *For Your Information: Privacy Law and Practice*, Report 108, 2008 (ALRC 2008); New South Wales Law Reform Commission, Report 120, *Invasion of Privacy*,2009; Victorian Law Reform Commission Report, *Surveillance in Public Places*, 2010. The Terms of Reference for the ALRC's 2014 report on *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123) required the ALRC to design a statutory tort to deal with serious invasions of privacy in the digital era.
[26] Tabled in the Legislative Assembly on 29 June 2002.

Specific issues for consideration – Protection of personal information

Definition of personal information

The definition of personal information is central to the operation of information privacy legislation. It is fundamental to legislative protections offered to individuals, including when they may make a privacy complaint. It is also central to the effective operation of the IP Act, as agencies' obligations arise in relation to personal information.

Section 12 of the IP Act defines personal information as:

> *…information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual* ***whose identity is apparent, or can reasonably be ascertained****, from the information or opinion.*

Issues

When the IP Act was drafted, **the definition of 'personal information'** mirrored the definition in the Privacy Act. However, in 2012, the definition in the Privacy Act was amended to substitute the requirement that personal information be about an individual whose 'identity is apparent, or can be reasonably ascertained,' for the requirement that information be about 'an identified individual, or an individual who is reasonably identifiable'.

This amendment aimed to ensure the definition was 'sufficiently flexible and technology-neutral to encompass changes in the way that information that identifies an individual is collected and handled'.[27] The requirement for identifiability was designed to capture a broader range of information such as online identifiers. Whether an individual is *reasonably identifiable* must be 'based on factors which are relevant to the context and circumstances.'[28]

The Privacy Act is again under review by the Commonwealth.[29] This review as well as the Australian Competition and Consumer Commission's (ACCC's) *Digital Platforms Inquiry – Final Report* (ACCC Report) have raised issues about the definition of personal information, noting that there is continuing uncertainty about the definition, including in relation to whether online identifiers and other technical data collected about individuals are within the scope of the definition. The ACCC recommended that the definition of personal information in the Privacy Act 'be updated to clarify that it captures technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual.'[30]

[27] Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012.
[28] Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012.
[29] *Review of the Privacy Act*, Issues Paper, October 2020; *Review of the Privacy Act*, Discussion Paper, October 2021.
[30] ACCC report, recommendation 16a.

The **European Union General Data Protection Regulation (EU GDPR)**,[31] which was introduced in 2018 to standardise data protection law across the EU, is sometimes described as the world's strongest set of data protection rules (or the 'gold standard' for data protection). It was introduced to give people in a growing digital economy greater control over how their personal information is used.

The EU GDPR applies to 'personal data' which is defined more broadly as including 'any information relating to an identified or identifiable natural person'.[32]

Adopting the definition of personal information in the Privacy Act would ensure consistency between the Queensland and Commonwealth regulatory frameworks. It is broader and more flexible than the current definition in the IP Act. However, it arguably does not address the uncertainty identified by the ACCC in relation to whether this definition captures a range of technical data.

Proposal for change: A new definition of 'personal information'

This Consultation Paper is seeking feedback on whether the definition of 'personal information in the IP Act should be amended to align with the definition of 'personal information' in the Privacy Act.

Personal information under the Privacy Act now means:

> information or an opinion about an identified individual, or an individual who is reasonably identifiable:
> (a) whether the information or opinion is true or not; and
> (b) whether the information or opinion is recorded in a material form or not.

QUESTION

1. *Should the **definition of personal information** in the IP Act be amended to reflect the definition which is currently in the Privacy Act?*

A single set of privacy principles for Queensland

The privacy principles in the IP Act regulate how agencies and their contracted service providers collect, store, use and disclose personal information. An individual can make a privacy complaint if an individual believes an agency has breached its obligations under the IP Act to comply with the principles.

The IP Act contains two sets of privacy principles – the **National Privacy Principles (NPPs)**, which apply to health agencies, and the **Information Privacy Principles (IPPs)**, which apply to all other agencies. The Privacy Act contains the APPs.

There are similarities between the IPPs and the NPPs in the IP Act. The IPPs and NPPs also share similarities with the APPs in the Privacy Act, with greater similarities between the APPs and the NPPs. There are also differences between all three sets of privacy principles which reflect, for example, that the APPs apply to both the public and private sector and the NPPs apply to health agencies.

[31] General Data Protection Regulation (EU) 2016/679 (EU GDPR).
[32] EU GDPR, article 4.

Issues

The existence of two similar but not identical sets of privacy principles in Queensland, which are not consistent with the APPs, has the potential to give rise to unjustified compliance costs, particularly for entities which may be subject to more than one set of privacy obligations.

Some agencies may have obligations under both the IP Act and the Privacy Act**.** The IP Act requires agencies to bind certain contracted service providers to privacy principles in the IP Act. This has the potential for contracted service providers to be subject to more than one set of privacy principles, for example if they provide services in more than one Australian jurisdiction, or contract with health agencies and non-health agencies in Queensland. The Privacy Act similarly requires Commonwealth agencies to bind contracted service providers to the APPs.

The different sets of privacy principles may also limit individuals' understanding of their privacy rights. There have been a number of calls for greater consistency in approaches to privacy regulation nationally, including by the Australian Law Reform Commission (ALRC).[33] To assist in achieving this consistency, a number of Queensland reports have considered whether a single set of privacy principles should be introduced.[34]

Potential benefits of adopting the Queensland Privacy Principles (QPPs)

Adopting a single set of privacy principles for Queensland would provide a uniform set of rules applying to all Queensland agencies and their contracted service providers. This would arguably reduce 'red tape' and compliance costs for contracted service providers and other entities which may be subject to more than one set of privacy principles. It may also give Queenslanders greater understanding of their privacy rights, and confidence that their personal information will be regulated in the same way, whether it is held by the Queensland Government, local government, Commonwealth Government or an organisation subject to the Privacy Act.

Adopting the QPPs would not only be an important step towards national consistency. There may also be potential additional privacy benefits, such as:

- sensitive information would be afforded a higher level of protection;
- there would be a requirement for the open and transparent handling of personal information. This principle promotes a 'privacy by design' approach, that is, it ensures that privacy and data protection compliance is included in the design of information systems from their inception; and
- individuals would be given the option of dealing anonymously or by pseudonym with an agency.

Potential impacts for agencies in adopting the QPPs

Despite the potential benefits of adopting the QPPs, as noted by the Review Report there would also likely be **administrative and resource implications for agencies.** Agencies will have to adapt their practices, procedures and systems to working with a new set of principles and become familiar with these new principles.

---

[33] ALRC report, *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108, 2008), (ALRC 2008 report) p 486.
[34] The Impala Report, recommendation 13 recommended that the IPPs and NPPs in the IP Act be amalgamated and strengthened, having regard to the APPs contained in the Privacy Act; Review Report, recommendation 13 referred to the potential benefits of a single set of privacy principles.

Proposal for change – the Proposed QPPs

The proposed QPPs are broadly consistent with the APPs but are modified for Queensland agencies. The APPs apply to both Commonwealth agencies and organisations. The QPPs only adopt the APPs to the extent they apply to agencies. For example, the QPPs do not contain principles similar to APP 7 (dealing with direct marketing) or APP 9 (dealing with government-related identifiers such as Medicare numbers or tax file numbers) as APP 7 and APP 9 do not apply to Commonwealth agencies.

The proposed QPPs and what they cover are listed below. The wording of the principles would be subject to further consultation as any new legislation is drafted.

QPP 1 Open and transparent management of personal information

An agency must:

- take reasonable steps to implement practices, procedures and systems that will ensure it complies with the QPPs, and is able to deal with related inquiries and complaints;
- have a clearly expressed and up to date QPP privacy policy; and
- take reasonable steps to make its QPP privacy policy available free of charge and in an appropriate form (e.g. on a website).

QPP 2 Anonymity and pseudonymity

An agency must give individuals the option of dealing with them anonymously[35] or by using a pseudonym[36] in relation to a particular matter, unless the agency is required or authorised to deal with identified individuals, or it is impracticable to deal with individuals who have not identified themselves.

QPP 3 Collection of solicited personal information

An agency must not collect *personal information* unless the information is reasonably necessary for, or directly related to, one or more of its functions or activities.
In addition, an agency must not collect *sensitive information*[37] unless the individual consents or an exception[38] applies.

An agency must only collect personal information by lawful and fair means.
Personal information must be collected only from the individual unless:

- the individual consents; or
- the collection is required or authorised by law or a court or tribunal order; or
- it is unreasonable or impracticable to do so.

---

[35] Anonymously is not defined in the Privacy Act. Its dictionary meaning is *in a way that prevents a person from being identified by name.*
[36] Pseudonym is not defined in the Privacy Act. The dictionary meaning of pseudonym is *a fictitious name.*
[37] Sensitive information in the Privacy Act means information or an opinion about an individual which includes, for example, their racial or ethnic origin, political opinions, religious beliefs or affiliations, sexual preferences or practices or criminal record. It also includes health information and genetic information about an individual and biometric information and biometric templates which may be used for the identification of a person.
[38] Exceptions would be similar to those in APP 3.4 and include items 1, 2, 3, 4 and 5 of the 'permitted general situations' as exceptions. QPP 3.4 includes exceptions in NPP 9(1)(e), (2) and (3) which permit health agencies to collect health information for existing purposes, including where necessary to provide a health service to an individual and where necessary for the purposes of: conducting research or the compilation or analysis of statistics relevant to public health or public safety and the management, funding or monitoring of a health service.

QPP 4 Dealing with unsolicited personal information

An agency must take the following steps if the agency receives personal information it did not solicit:[39]

- decide whether or not it could have collected the personal information under QPP 3 if it had solicited it; **and**
- if the agency could not have collected the personal information under QPP 3 and the information is not contained in a public record[40] — the agency must destroy or de-identify the information as soon as practicable, if it is lawful and reasonable to do so; **or**
- if the agency could have collected the personal information under QPP 3, or the information is contained in a public record, or the agency is not required to destroy or de-identify the information under QPP 4 – the agency may keep the information but must deal with it in accordance with QPPs 5 to 11.

QPP 5 Notification of the collection of personal information

An agency that collects personal information about an individual must take such steps as are reasonable in the circumstances to notify the individual of the following matters or to ensure the individual is aware of any such matters:

- the identity and contact details of the agency;
- the fact and circumstances of the collection;
- whether the collection is required or authorised by law;
- the purposes of collection;
- the main consequences (if any) for the individual if the personal information is not collected;
- the agency's usual disclosures of personal information of the kind collected by the agency;
- information about the agency's QPP privacy policy; and
- whether the agency is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located.

QPP 6 Use or disclosure of personal information

An agency that holds personal information about an individual which was collected for a particular purpose (the primary purpose) must not use or disclose the information for another purpose (secondary purpose) unless the individual consents or another exception applies.[41] The exceptions include:

- the individual would reasonably expect the agency to use or disclose the information for the secondary purpose, and the secondary purpose is related to the primary purpose of collection or, in the case of sensitive information, directly related to the primary purpose;
- the secondary purpose is required or authorised by or under an Australian law or court or tribunal order;

[39] Under section 6 of the Privacy Act, an entity ***solicits*** personal information if the entity requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included. ***Unsolicited information*** would include for example misdirected mail or a petition that includes names and addresses.
[40] A public record is defined in section 6 of the *Public Records Act 2002*.

- item 1, 2, 3, 4 or 5 of the permitted general situations in the Privacy Act[42] exists;
- the information is health information used or disclosed by a health agency in the circumstances currently permitted under NPP 2(3) or NPP 2(1)(c)[43];
- the agency reasonably believes that the secondary purpose is reasonably necessary for one or more enforcement-related activities of a law enforcement agency; or
- an agency discloses biometric information or biometric templates to a law enforcement agency in accordance with guidelines made by the Information Commissioner for this purpose.

QPP 7 Cross-border disclosure of personal information

Before the agency discloses personal information to an overseas recipient[44] the agency must take reasonable steps to ensure that the overseas recipient does not breach the QPPs in relation to the information (unless an exception applies).[45]

It is proposed that the IP Act would be amended to make an agency accountable for a breach of the QPPs by an overseas recipient unless an exception applies.[46]

QPP 8 Quality of personal information

An agency must take reasonable steps to ensure that the personal information the agency collects is accurate, up-to-date, and complete.

An agency must also take reasonable steps to ensure that the personal information it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete, and relevant.

---

[42] These permit the collection, use or disclosure of personal information where: (1) it is unreasonable or impracticable to obtain the individual's consent and the agency reasonably believes it is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety; or (2) the agency reasonably believes it is necessary to take appropriate action in relation to suspected unlawful activity or serious misconduct that is, or may be engaged in; or (3) the agency reasonably believes it is necessary to locate a missing person (in accordance with rules made by the Information Commissioner); or (4) it is reasonably necessary for a legal or equitable claim; or (5) a confidential alternative dispute resolution process. These are provided for as exceptions in QPP 3.4 and QPP 6.2, with items 1, 2 and 3 provided for as exceptions in QPP 7.2.

[43] These are, broadly, to permit disclosure to a person responsible for a person to whom the health agency provides a health service (in particular circumstances), and to permit use and disclosure for research and the compilation or analysis of statistics relevant to public health and safety.

[44] An overseas recipient would be described as 'a person who is not in Australia or an external Territory and who is not the agency or the individual'.

[45] See Appendix One for the details of the exceptions. The exceptions broadly relate to: a reasonable belief the overseas recipient is subject to a substantially similar law or binding scheme as the QPPs and where there are mechanisms that can be accessed by the individual to enforce the protection of the law or binding scheme; or the agency expressly informs the individual that if they consent, the principle will not apply and the individual consents; the disclosure is required or authorised by law; item 1, 2 or 3 of the permitted general situations in section 16A of the Privacy Act exists; the agency reasonably believes the disclosure is reasonably necessary for an enforcement related activity; or the disclosure is required or authorised under an international agreement relating to information sharing.

[46] Similar to section 16C of the *Privacy Act*.

QPP 9 Security of personal information

An agency must take reasonable steps to protect personal information they hold from misuse, interference, and loss, as well as unauthorised access, modification or disclosure.

Where an agency no longer needs personal information for any purpose for which the information may be used or disclosed under the QPPs, the agency must take reasonable steps to destroy the information or ensure it is de-identified, except where the personal information is part of a public record[47] or the agency is required by an Australian law or a court/tribunal order to retain the personal information.

QPP10 Access to personal information

An agency that holds personal information about an individual must, on request of the individual, give the individual access to the information.

An agency is not required to give access to personal information under QPP 10 if the agency is required or authorised to refuse to give the individual access to that information by or under chapter 3 of the IP Act, or any other Queensland Act that provides for access by persons to documents.

QPP 10 will also set out minimum access requirements, including the time period for responding to an access request, how access is to be given, and that a written notice, including the reasons for the refusal, must be given to the individual if access is refused.

QPP 11 Correction of personal information

An agency must take reasonable steps to correct personal information to ensure that information is accurate, up-to-date, complete, relevant and not misleading.

The requirement to take reasonable steps applies:

- where an agency is satisfied, independently of any request, that personal information it holds is incorrect; or
- where an individual requests an agency to correct their personal information.

QPP 11 sets out minimum procedural requirements in relation to correction of personal information, including taking reasonable steps to notify other agencies of a correction and giving notice to an individual which includes reasons and available complaint mechanisms if correction is refused; and taking reasonable steps to associate a statement with personal information an agency refuses to correct.

QUESTIONS

2. *Should the **proposed QPPs** be adopted in Queensland?*
3. *If not, in what ways should they be changed?*

[47] A 'public record' is defined in section 6 of the *Public Records Act 2002*.

‘Reasonable’ steps in the protection of personal information

Like the current requirements in IPP 4 and NPP 4, the proposed new QPP 9 would require agencies to take ‘reasonable steps’ to protect personal information they hold from unauthorised access, use, disclosure, modification and from any other misuse.

Issues

The Impala Report queried whether the requirement to take ‘reasonable steps’ in IPP 4 and NPP 4 was sufficient, including whether it was compatible with human rights.

The Impala Report recommended that the term ‘reasonable steps’ in IPP 4 and NPP 4 be further defined in accordance with the terms of Article 32 of the EU GDPR in relation to the security of data.[48]

In meeting their privacy obligations, agencies must act and make decisions in a way that is compatible with human rights, including the right to privacy. As stated by the Queensland Human Rights Commission (QHRC) in its submission to Operation Impala, based on international case law, the right to privacy may be interpreted as placing a positive responsibility on government to do what is necessary and reasonable to protect private information.[49] Based on these authorities the QHRC considered that the right to privacy under the HR Act may require public entities to have adequate procedural safeguards against unauthorised access and disclosure of stored personal information.[50]

As noted by the Queensland Human Rights Commissioner in giving evidence to Operation Impala:[51]

> *The level of protection necessary (for personal information) will depend upon the nature of the information collected, the purpose for which it is collected, and the harm that may be caused if privacy is breached. It will not be sufficient for public entities to only have policies in place; they must also take reasonable steps to ensure the policies are followed. Failure to provide adequate safeguards may amount to a disproportionate and therefore unlawful limitation of a person’s right to privacy.…the (Human Rights Act) will help inform the interpretation of what is ‘reasonable’, having regard to human rights and the factors described above.*

The terms ‘reasonable’, ‘reasonably’ and ‘reasonable steps’ are used throughout the IP Act and the Privacy Act. Although the OIC and Office of the Australian Information Commissioner (OAIC) provide some guidance on what may constitute ‘reasonable steps’, including in the context of APP 11 (which is similar to proposed QPP 9),[52] the term has not been defined in either Act.

[48] Impala report, recommendation 16.1.
[49] The QHRC submission to Operation Impala cited the following cases: *S and Marper v United Kingdom* [2008] ECHR 1581; *MM v United Kingdom* [2012] ECHR 1906.
[50] QHRC Public Submission 11, paragraph 6.
[51] Scott McDougall, Commissioner, QHRC, 22 November 2019.
[52] OAIC, Australian Privacy Principle Guidelines, (July 2019), Australian Privacy Principles guidelines - Home (oaic.gov.au).

There are some common factors that various guidelines[53] and human rights jurisprudence[54] suggest are relevant to the issue of what is 'reasonable' with respect to the steps that should be taken to secure personal information. This guidance suggests that what is 'reasonable' could depend on:

- the nature of the information collected including the amount and sensitivity of the personal information;
- the purpose for which the information is being collected;
- the nature of the agency holding the personal information including the agency's size, resources and its business model;
- the possible harm, or adverse consequences for an individual in the case of a breach; and
- the practicability, including time and cost involved in implementing the security measure considering all the circumstances.

On the other hand, Article 32 of the EU GDPR, which deals with security of information, provides for much more detailed guidance, specific to personal data requiring the 'controller' and the 'processor' to implement 'appropriate technical and organisational measures to ensure a level of security, appropriate to the risk', including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

While Article 32 of the EU GDPR is far more specific than the proposed factors above, adopting this would arguably not bring the QPPs into alignment with the APPs, particularly APP 11 (security of personal information) and all other State and Territory privacy principles.

The Privacy Act Review Discussion Paper proposed that APP 11 (which would be equivalent to QPP 9) be amended to state that 'reasonable steps' for APP 11 includes technical and organisational measures. It also proposed by the Privacy Act Review to include a list of factors that indicate what reasonable steps may be required.

[53] Guidelines discussing reasonable steps in the context of the IP Act produced by OIC include: https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/security,-accuracy-and-relevance/health-agencies-data-quality-and-data-security; https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/transferring-personal-information-out-of-australia/sending-personal-information-out-of-australia; and https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/collection/camera-surveillance-and-privacy.

[54] For example, the OIC's Policy on Mobile ICT devices states in relation to the security of government laptops, 'Staff are responsible for taking reasonable steps to maintain the security of the device. For example, using the provided tether in the office, ensuring the device is in their possession or securely stored when taken offsite, and by locking the computer when it is not in active use' (https://www.oic.qld.gov.au/publications/policies/mobile-ict-devices-policy). Also see *S and Marper v United Kingdom* [2008] ECHR 1581; *MM v United Kingdom* [2012] ECHR 1906.

Proposal for change: Guidance on 'reasonable steps'

The Consultation Paper is seeking feedback on whether the IP Act should prescribe a non-exhaustive list of matters that must be taken into account by an agency when determining what 'reasonable steps' would be in the context of QPP 9.

The factors to be considered could include:

- the nature of the information collected including the amount and sensitivity of the personal information;
- the purpose for which the information is being collected;
- the nature of the agency holding the personal information including the agency's size, resources and its business model;
- the possible harm, or adverse consequences for an individual in the case of a breach; and
- the practicability, including time and cost involved in implementing the security measure considering all the circumstances.

These factors would also not represent an exhaustive or definitive list.

Alternatively, the legislation could be amended to mandate that the OIC produce specific guidelines on what 'reasonable steps' would be in the context of QPP 9.

QUESTIONS

4. *What are the benefits and disadvantages of **defining the factors that must be considered in 'reasonable steps' for QPP 9** in the IP Act?*
5. *Could these factors be applied to other relevant parts of the IP Act?*
6. *Would **statutory guidelines**, produced by OIC be more flexible and useful?*

Enhanced powers and functions for the Information Commissioner to respond to privacy breaches

The OIC has an important role as part of Queensland Information Privacy framework. The OIC is an independent body established to promote access to government-held information and protect personal information held by the public sector.

The Information Commissioner is an officer of the Parliament and is not subject to direction from any person. The IP Act also provides for a Privacy Commissioner, whose role is that of a deputy to the Information Commissioner, with particular responsibility for matters relating to the Information Commissioner's functions under the IP Act.

In addition to its role in reviewing decisions of agencies and Ministers about access to, or amendment of personal information under Chapter 3 of the IP Act, OIC has other functions specific to privacy. The OIC promotes the principles and practices of information privacy through a range of training and communication activities; monitors agency compliance with the IP Act; and receives and mediates privacy complaints against relevant entities (agencies and contracted service providers).

To support these functions the Information Commissioner has a range of compliance and enforcement powers.

Issues

The **Information Commissioner's regulatory functions** are set out in Chapter 4, Part 1 of the IP Act. Relevant to the below discussion these functions include:

- **Decision-making functions:** including dealing with privacy complaints (the OIC can receive a complaint from an individual about an agency or contracted service provider that has failed to comply with the privacy principles);[55] and
- **Performance monitoring and support functions:** including conducting reviews into the personal information handling practices of relevant entities,[56] and conducing compliance audits[57] to assess entities' compliance with the privacy principles.

There are also certain investigative and compliance actions the Information Commissioner can take on their own initiative with respect to 'relevant entities'. For example, the Information Commissioner may issue a 'compliance notice' asking an agency or contracted service provider to take certain action within a certain timeframe.[58] The Information Commissioner may also require a person to provide documents or to attend and give evidence in relation to the Information Commissioner's decision to issue a compliance notice.[59] At the completion of a review, the Information Commission may report to Parliament (the Speaker) on the outcome of any review.[60]

A number of reports, in particular the Impala Report and the Review Report, have made recommendations to enhance the compliance and enforcement powers of the Information Commissioner and to extend their functions to better protect the privacy of individuals and respond to privacy breaches by agencies.

Own motion powers

The Impala Report and the Review Report both recommended that the IP Act be amended to provide the Information Commissioner with 'own motion' powers to investigate an agency or bound service provider engaged in conduct that may constitute an interference with the privacy of an individual.[61]

The IP Act does provide the Information Commissioner with the power, on the Commissioner's own initiative or otherwise, to conduct a review into the personal handling practices of relevant entities.[62]

However, as currently expressed this power is limited. The Information Commission may only conduct a review to identify:

- privacy related issues of a systemic nature generally; or
- particular grounds for the issue of a compliance notice.

The IP Act sets a high threshold for issuing a compliance notice, limiting the circumstances in which the Information Commissioner can investigate an act or practice. A compliance notice may only be issued if the Information Commissioner is satisfied on reasonable grounds that the conduct *constitutes*

[55] IP Act, s 136 and Chapter 5.
[56] IP Act, s 135(1)(a)(i).
[57] IP Act, s 135(b)(iii).
[58] IP Act, s 158.
[59] IP Act, s 197.
[60] IP Act, s 135(1)(a)(ii).
[61] Impala report, recommendation 14.1; Review Report, recommendation 19.
[62] IP Act, s 135(1)(a)(i).

a serious or flagrant contravention of the agency's obligation to comply with the privacy principles, or the contravention has occurred *on at least five occasions within the preceding two years*.[63]

Arguably this power does not expressly provide the Information Commissioner with power to:

- undertake reviews into personal information handling practices that do not identify broader systemic issues or particular grounds for issuing a compliance notice; or
- 'investigate' practices of agencies; or
- review 'acts' of agencies in addition to 'practices' of agencies.

An own motion power would allow the Information Commissioner to investigate a matter, whether or not a complaint has been made, or whether or not the issue identified broader systemic issues or the grounds for issuing a compliance notice.

If an own motion investigation conducted by the Information Commissioner was to reveal grounds for a compliance notice, the Information Commissioner could use existing powers to issue a compliance notice under the IP Act, or report to the Speaker as provided for under section 135, on the findings of any investigation. The existing powers to give a person written notice requiring information to be given to the Commissioner and/or to appear before the Commissioner to answer questions[64] could also be extended to an own motion investigation function.

The Australian Information Commissioner (AIC) has an own motion power under section 40(2) of the Privacy Act. The AIC may, on the Commissioner's own initiative, investigate an act or practice if: the act or practice may be an interference with the privacy of an individual, or a breach of APP 1[65]; and the Commissioner thinks it desirable that the act or practice be investigated.

Declaration powers

In Queensland, under the IP Act, if an agency or contracted service provider does not comply with privacy principles, then an individual can make a privacy complaint to the Information Commissioner. Currently, the Information Commissioner's role is not to make determinations or a decision in relation to the complaint, but to attempt to mediate privacy complaints that cannot be resolved with the agency.

Complaints which cannot be mediated by the Information Commissioner are referred to QCAT. After hearing the matter, QCAT may order that the complaint, or a part of the complaint, has been substantiated. If QCAT makes such an order, it may also make other orders, including that:

- an act or practice of the agency is an interference with the privacy of the complainant and that the agency must not repeat or continue the act or practice; and/or
- that the agency apologise to the complainant for the interference with the complainant's privacy; and/or
- that the complainant is entitled to a stated amount, of not more than $100,000, to compensate the complainant for loss or damage suffered by the complainant because of the act or practice complained of, including for any injury to the complainant's feelings or humiliation suffered by the complainant.[66]

[63] IP Act, s 158.
[64] IP Act, s 197.
[65] APP 1 provides for open and transparent management of personal information.
[66] IP Act, s 178.

In contrast, following a privacy complaint or an own-motion investigation,[67] the AIC may make a 'determination' which may include a number of declarations such as:

- that the act or practice is an interference with the privacy of one or more individuals; and the person or entity must not repeat or continue the act or practice; or
- that the person or entity must take specified steps within a specified period to ensure that the act or practice is not repeated or continued; or
- that a complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice.[68]

Once the AIC has investigated a complaint and made an appropriate declaration, the government agency or organisation which the declaration applies to must comply with it.[69] However, the Federal Court or Federal Circuit Court can issue orders to enforce determinations.[70]

The Impala Report recommended a similar power be given to the Information Commissioner, considering that this would, following referral to a court for enforcement, give aggrieved persons official recognition that that their privacy was breached, and avoid lengthy and costly court proceedings.[71]

Given the respective roles of the Information Commissioner and QCAT under the IP Act in relation to resolving individuals' privacy complaints in Queensland's current information privacy framework (i.e. independent conciliator and determinative tribunal respectively) providing the Information Commissioner with a declaratory function following an investigation, in response to an individual complaint could be seen as duplicative of the determinative role of QCAT.

However, the question remains as to whether the Information Commissioner should be given a determinative power to make declarations following the exercise of the proposed new own motion investigation. A power to make such declarations (similar to those that QCAT can currently make) would be a significant departure from the current role of the Information Commissioner.

An intervener role for OIC

The IP Act gives the Information Commissioner and Privacy Commissioner an entitlement to appear and be heard in a proceeding arising out of the performance of the Commissioner's functions under the IP Act.[72] It does not appear that this provision gives any right for the Information Commissioner or Privacy Commissioner to appear in QCAT in relation to a privacy complaint mediated by the OIC and referred to QCAT. Rather, it gives them a right to appear in tribunal and court proceedings in respect of proceedings such as appeals of external review decisions made by the Information Commissioner.[73] The Impala Report recommended that the OIC be able to appear as a friend of the court (*amicus curiae*), and have the power to intervene in QCAT proceedings, where appropriate and with leave of the court.

[67] Privacy Act, s 52.
[68] IP Act, s 178
[69] Privacy Act, ss 55 and 58.
[70] Privacy Act, s 55A.
[71] Impala report, p 118.
[72] IP Act, s 155.
[73] *Commissioner of the Police Service v Shelton & Anor* [2020] QCA 96; *SJN v Office of the Information Commissioner & Anor* [2019] QCATA 115; *Powell v Queensland University of Technology* [2017] QCA 200.

A number of **other statutory officers** in Queensland have the power to intervene in court and tribunal proceedings with respect to particular rights and interests related to their functions. For example:

- the **Public Advocate** may intervene in a proceeding before a court or tribunal, or in an official inquiry, involving protection of the rights or interests of adults with impaired capacity for a matter, with the leave of the court, tribunal or person in charge of the inquiry and subject to the terms imposed by the court, tribunal or person in charge of the inquiry;[74] and
- the **Human Rights Commissioner** may intervene in and be joined as a party to a proceeding before a court or tribunal in which: (a) a question of law arises that relates to the application of this Act; or (b) a question arises in relation to the interpretation of a statutory provision in accordance the HR Act.[75]

Like certain other statutory officers who have the power to intervene in court and tribunal proceedings with respect to particular rights and interests related to their functions, it may be beneficial to allow the OIC to play a similar role with respect to the protection of information privacy under the IP Act. The OIC is well placed to assist the court in understanding the IP Act and the obligations on agencies, including those imposed by the privacy principles.

Proposal for change: Enhanced powers for the Information Commissioner

This Consultation Paper is seeking feedback on whether the powers of the OIC should be enhanced to:

- **Provide the Information Commissioner with own motion powers**

  The IP Act could be amended to provide the Information Commissioner with power to investigate, on the Information Commissioner's own initiative, an act or practice of an agency which may be a breach of the privacy principles. These powers would:

  - allow the Information Commissioner, on the Information Commissioner's own initiative, to investigate an act or practice if:
    - the Information Commissioner considers on reasonable grounds that the act or practice may be a breach of the privacy principles; and
    - the Information Commissioner considers it is in the public interest that the act or practice be investigated;
  - enable the Information Commissioner to exercise all the powers under current section 197 of the IP Act including: by written notice, requiring a person to give information to the commissioner; and requiring a person to attend before the commissioner to answer questions relevant to the investigation;
  - allow the Information Commissioner to make a report to the Speaker and the Parliamentary Committee on the outcome of the investigation – which must be tabled in Parliament; and
  - should the own motion investigation reveal the grounds for a compliance notice to be issued under current section 158 of the IP Act, enable the Information Commissioner to issue this notice.

[74] *Guardianship and Administration Act 2000*, s 210.
[75] HR Act, s 51.

- **Provide the OIC with the power to intervene in tribunal or court proceedings involving the IP Act**, with the leave of the court or tribunal and on terms or conditions provided by the court or tribunal.

QUESTIONS

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

Mandatory DBN scheme

What is a notifiable data breach?

Under a mandatory DBN scheme there is a legal requirement to notify individuals (and the Regulator) when a breach of security leads to the disclosure of personal information. A data breach may be caused by malicious action, human error or a failure in information handling or security systems.

Examples of data breaches include:

- a USB or mobile phone that holds an individual's personal information being stolen;
- a database containing personal information being hacked; and
- someone's personal information inadvertently sent to the wrong person.[76]

Data breaches have the potential to cause serious harms to individuals, depending on the type and sensitivity of the personal information involved in the data breach and the circumstances. Examples of serious harms could include identity theft or identity fraud, physical harm, emotional harm and discrimination.

The **main purpose of notification** is to mitigate the risk of a data breach by giving affected individuals an opportunity to take steps (where appropriate) to reduce the likely harm(s) of the data breach (for example, to change passwords or open a new account).

Issues

The IP Act does not contain mandatory data breach notification obligations, however, the OIC has a Privacy Breach Management and Notification Guideline, which includes considerations around notifying persons whose privacy may be affected by a privacy breach.

While no other State or Territory has implemented a mandatory DBN scheme, the Commonwealth Notifiable Data Breaches scheme (Commonwealth NDB scheme) under the Privacy Act was introduced in 2018.[77] The Commonwealth NDB scheme applies to entities which are covered by the Privacy Act. This includes most Australian Government agencies, business entities with an annual turnover of more

[76] OAIC, https://www.oaic.gov.au/privacy/data-breaches/what-is-a-data-breach/.
[77] The *Privacy Amendment (Notifiable Data Breaches) Act 2017* established the scheme on 22 February 2018.

than $3M and other organisations.[78] The Commonwealth NDB scheme also applies to additional entities, including Queensland agencies, in relation to Tax File Number information.

The NSW Government also released a discussion paper about the issue in 2019 and consulted on a draft Bill to introduce a scheme based on the Commonwealth NDB scheme.[79] The proposed scheme would also include augmented regulatory powers for the NSW Privacy Commissioner (PC) to empower the PC to:

- make directions and recommendations to agencies where there are reasonable grounds to believe there has been an eligible data breach;
- enter premises and inspect anything that may relate to compliance by an agency with the scheme;
- conduct audits and investigations in relation to the scheme; and
- provide a report to the head of the agency and responsible minister.[80]

The Impala Report recommended that a mandatory DBN scheme be implemented in Queensland. The report considered such a mandatory scheme was necessary due to the serious impacts of data breaches, not only on individuals whose privacy is breached, but also Government, reducing public confidence in the integrity of government operations.

A mandatory DBN scheme would not only be good privacy practice but would enhance and protect the privacy rights of individuals and provide many benefits for Queensland including improved transparency and accountability for government agencies. Consistency with the Commonwealth scheme would give individuals who deal with Queensland agencies the same protections as those individuals have when dealing with Federal Government agencies.

Proposal for change: A mandatory DBN scheme for Queensland

This Consultation Paper is seeking feedback on whether a mandatory DBN scheme, based on the Commonwealth NDB scheme should be introduced in Queensland.

This scheme would require agencies to notify the OIC and an affected individual of an 'eligible data breach'.

Eligible data breach

This would occur where there is unauthorised access to, unauthorised disclosure of, or loss of personal information where a reasonable person would conclude the unauthorised access or disclosure would be likely to result in serious harm to any of the affected individuals. Serious harm may include serious physical, psychological, emotional, financial or reputational harm.[81]

[78] Other organisations include health service providers; businesses that sell or purchase personal information and credit reporting bodies. State government agencies are covered to the extent they hold Tax File Number (TFN) information, but only with respect to the TFN information.
[79] NSW Department of Communities and Justice, *Mandatory Notification of Data Breaches by NSW Public Sector Agencies: Discussion Paper*, July 2019: Mandatory data breach notification (nsw.gov.au).
[80] NSW Privacy and Personal Information Protection Amendment Bill 2021 (Exposure draft Bill): Proposed changes to NSW privacy laws.
[81] 'Serious harm' is not defined in the Privacy Act but the AIC provides guidance on what constitutes 'serious harm' and the meaning of the term is also guided by judicial consideration.

An agency must have regard to certain matters in determining whether access to, or disclosure of, information would be likely to result in serious harm, including:

- the kind of information and the sensitivity of the information;
- the nature of the harm;
- the persons, or kinds of persons who have obtained, or could obtain the information;
- whether the information is protected by one or more security measures; and
- the likelihood of those security measures being overcome.

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).

Assessment of suspected eligible data breaches

Agencies would need to conduct reasonable and expeditious assessments of *suspected* eligible data breaches and take reasonable steps to complete assessments within 30 days.

When notification is required

If an agency had reasonable grounds to *believe* that there has been an eligible data breach, it must (as soon as practicable) give a copy of a statement about the data breach to the OIC which includes details about:

- the identity and contact details of the agency;
- a description of the eligible data breach;
- the kind or kinds of information concerned;
- recommendations about the steps that individuals should take; and
- if the agency wishes, the identity and contact details of other entities involved in the data breach.

The agency must notify affected individuals and give them the above statement. If practicable, the entity must take reasonable steps to:

- notify the contents of the statement to individuals whose personal information was involved; or
- notify the contents of the statement to individuals who are at risk of serious harm; or
- publish the statement as soon as practicable, if it is not practicable to notify the individuals.

Exceptions to requirement to comply with the mandatory DBN scheme

Exceptions would include enforcement-related activities, where compliance would be inconsistent with secrecy provisions and where the Commissioner declares that notification is not required.

Role and function of the OIC

The OIC would have an oversight role for the mandatory DBN scheme with functions and powers to monitor and ensure compliance with the scheme.

Actions that the OIC may take

The existing regulatory powers of the OIC could be extended to facilitate the OIC's oversight role. This would include:

- conducting reviews, audits and own motion investigations in relation to agencies' compliance with the mandatory DBN scheme;
- providing a report to the Parliament (the Speaker) on the findings of an audit, review or investigation;
- issuing a compliance notice (under current section 158 of the IP Act) where an agency has failed to comply with their obligations under the mandatory DBN scheme (and the act or practice is a serious or flagrant contravention of the obligation or has been repeated contravention); and
- powers (under current section 197 of the IP Act) to require a person to give information to the Commissioner or that a person attend before the Commissioner to answer questions relevant to an eligible data breach under the mandatory DBN scheme.

Proposed new regulatory powers

Proposed new regulatory powers for the OIC could include The power to make directions and recommendations to an agency about the handling of a data breach under the mandatory DBN scheme including:

- giving a written notice to an agency directing the agency to prepare a statement about a data breach; and
- recommending that an agency notify individuals in relation to a data breach as provided for under the mandatory DBN scheme.

QUESTIONS

11. *Is the mandatory DBN scheme as outlined above suitable for adoption in Queensland?*

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

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

Criminal sanctions for misuse of personal information by public officers

As recognised by the Impala Report, **public sector employees are in a particular position of trust by virtue of their office**. When public sector employees misuse confidential information there is a loss of public confidence in the agencies concerned. The Impala Report also recognises that the misuse of confidential information by employees can have significant consequences for the individual affected.

The Impala Report **recommended the creation of a new offence in the Criminal Code** that would be more useful in prosecuting offending related to misuse of confidential information.

Section 408E (Computer hacking and misuse) of the Criminal Code currently captures the use of a restricted computer without the consent of the computer's controller. Section 408E contains three offences. Firstly, section 408E(1) contains a simple offence: a person who uses a restricted computer without the consent of the computer's controller commits a simple offence and is liable to a maximum penalty of imprisonment for 2 years. Subsections (3) and (4) specify two circumstances of aggravation for the offence which apply where the offender:

- causes or intends to cause detriment or damage, or gains or intends to gain a benefit (Maximum penalty of five years imprisonment); or
- causes a detriment or damage or obtains a benefit for any person to the value of more than $5,000 or intends to commit an indictable offence (Maximum penalty of 10 years imprisonment).

Provisions comparable to section 408E of the Criminal Code exist in each Australian jurisdiction. While a comprehensive jurisdictional scan has not been undertaken, some jurisdictions also appear to have offences specifically directed to misuse of information by public officers. For example, section 122.4 of the *Criminal Code Act 1995* (Cth) contains an offence relating to unauthorised disclosure of information by current and former Commonwealth officers.

In recommending a new criminal offence to deal with misuse of confidential information by public officers, the Impala Report noted the following challenges with the ability to prosecute an employee within a public sector agency for inappropriately accessing or generally misusing confidential information under section 408E (Computer hacking and misuse) of the Criminal Code:

- use of the term 'computer hacking' does not make it clear to public officers that their conduct in accessing confidential information to which they have access in the performance of their duties can be a criminal offence if they do so for an improper purpose;
- the definition of the word 'benefit' is limited, particularly where knowledge is the only thing gained from accessing the confidential information;
- the current maximum penalties do not adequately reflect the serious nature of deliberate breaches of the public's privacy by public officers; and
- in some cases, charging under the offence becomes statute-barred.

The ability to prosecute offenders, including public sector officers, forms an important part of Queensland's justice system. Having effective criminal laws is essential to provide a clear statement to the community about which conduct is unacceptable, to ensure offending is properly punished as well as to provide a deterrent to potential offenders.

Issues

Is there a need for a new criminal offence and if so, what should it be?

The Consultation Paper is seeking feedback on the proposed new additional criminal offence of misuse of confidential information by public officers.

The Impala Report recommended a new offence provision of *misuse of confidential information by public officers*. In contrast to section 408E of the Criminal Code, the offence would apply to the misuse of confidential information on a computer and any confidential information regardless of its source (e.g. a paper file). The **key characteristics of the proposed new offence** are as follows:

- a simpliciter offence with a maximum penalty of five years providing that it is a crime to access confidential information not in furtherance of the performance of a function of the agency;
- three circumstances of aggravation which would increase the maximum penalty to ten years imprisonment, namely:
    - where the public officer or another person obtains a benefit (which includes obtaining

knowledge by itself); or
    - when disclosure is made to a third party; or
    - where access could facilitate the commission of a crime.
- for the purposes of the provision, all information that is held on a restricted database, even if publicly available elsewhere, will be considered confidential information;
- the offence is to contain a definition of 'benefit' that includes:
    - obtaining knowledge of information from a database; or
    - finding that there is no record in the database; or
    - obtaining knowledge of information that is available from another public source; and
- the offence will be an indictable offence that may be heard and decided summarily at the election of the prosecution under section 552A.

In addition to section 403E of the Criminal Code, **there are other existing provisions on the Queensland statute** which may be relevant to this type of conduct by public officers, including for example:

- section 85 (Disclosure of official secrets) of the Criminal Code, which carries a maximum penalty of 2 years imprisonment;
- section 87 (Official corruption) of the Criminal Code, which carries a maximum penalty of 7 years imprisonment;
- section 88 (Extortion by public officers) of the Criminal Code, which carries a maximum penalty of 3 years imprisonment; and
- section 92A (Misconduct in relation to public office) of the Criminal Code, which carries a maximum penalty of 7 years imprisonment.

Some specific legislation also includes offence provisions relevant to the unauthorised use or disclosure of confidential information. Examples include section 10.1 (Improper disclosure of information) of the *Police Service Administration Act 1990* and section 217B (Confidentiality of information) of the *Fisheries Act 1994*.

QUESTIONS

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

15. *Do you have any other comments about this issue?*

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

This part seeks feedback on proposed changes to Queensland's **information privacy and right to information framework** to **clarify and improve the operation of that framework.**

Background

While the proposals for significant changes to Queensland's information privacy framework were discussed in Part A, this Part discusses proposals for implementing those recommendations that would clarify and improve the operation of the framework. A number of reports (outlined below) have made recommendations for changes to Queensland information privacy and right to information framework.

Review Report

In accordance with the RTI Act and the IP Act,[82] a statutory review was undertaken with public consultation processes in 2013 and 2016. While the Review Report, tabled in October 2017, noted that in general the Acts were achieving their objects, it made 23 recommendations for legislative amendments.

The Strategic Review Report

In accordance with the RTI Act[83] a strategic review of the OIC was undertaken by PricewaterhouseCoopers and finalised and tabled in 2017, making two recommendations for legislative change, both of which are consistent with Review Report recommendations.

Windage Report

Operation Windage was an investigation by the CCC into allegations of corruption related to Ipswich City Council. The Windage Report concluded that private companies established by local governments can create corruption risks through a lack of oversight and transparency. Recommendation 3(b) of the Windage Report was that *councils' controlled entities should be deemed to be units of public administration, bringing these entities within the oversight of the CCC and also subjecting them to the Right to Information Act 2009*. Operation Impala was a CCC corruption investigation into agencies' unauthorised access and disclosure of confidential information (specifically individuals' personal information). The Impala Report recommended a number of legislative changes (including to the IP Act and the Criminal Code) to respond to unauthorised access and disclosure of individuals' personal information by agencies and their officers.

Developments in case law about courts and tribunals

A series of appeals brought by Justice Carmody and the Department of Justice and Attorney-General (DJAG) against Information Commissioner decisions (Carmody decisions)[84] and *Q20 v Department of*

[82] RTI Act, s 183; IP Act, s 192.
[83] RTI Act, s 186.
[84] *Carmody v Information Commissioner & Others* [2018] QCATA 14; *Carmody v Information Commissioner & Others* (No 2) [2018] QCATA 15; *Carmody v Information Commissioner & Others* (No 3) [2018] QCATA 16; *Carmody v Information Commissioner & Others* (No 4) [2018] QCATA 17; *Carmody v Information Commissioner & Others* (No 5) [2018] QCATA 18; *Carmody v Information Commissioner & Others* (No 6) [2018] QCATA 19.

Justice and Attorney-General (Q20),[85] have emphasised judicial independence and provided guidance about the operation of the RTI and IP Acts in relation to the judicial and quasi-judicial functions of courts and tribunals.

The proposals set out below relate to:

- Making applications
- Processing applications
- Exemptions
- Internal and External reviews
- Application of the RTI and IP Acts
- Privacy issues
- Other issues

Making applications

A single right of access (Review Report, recommendation 2)

The RTI Act provides a right of access to documents of an agency or a Minister.[86] The IP Act provides a right of access to documents of an agency or a Minister to the extent the documents contain the individual's *personal information*.[87] The grounds for refusing access to information, timeframes, and all other processes are the same under both Acts. The IP Act also allows individuals to apply to agencies or Ministers to amend their *personal information*.

This framework was implemented following the Solomon Report recommendation that access and amendment rights for *personal information* be in a separate Privacy Act, to make the application process simpler and quicker for applicants and to permit greater specialisation in complex access matters.

However, these benefits have not eventuated, and the Review Report found that having a right of access in both Acts has resulted in:

- legislative duplication, as the grounds for refusing access to information, the timeframes, and all other processes are the same under both Acts;
- complicated reasons for decisions, as extensive cross-referencing between Acts is required (where some documents contain an individual's *personal information* and some do not); and
- possible delays in processing applications and giving access to documents if applications are made under the wrong Act.

The Review Report concluded that the separation between the Acts is confusing to applicants and agencies expend a great deal of time determining under which Act an application should be processed.

[85] [2020] QICmr 40.
[86] RTI Act, s 23.
[87] IP Act, s 40. Individuals can also apply under the IP Act to amend their personal information IP Act, s 41.

Proposal for change – A single right of access

Amendments are proposed to the RTI and IP Acts to provide a single right of access under the RTI Act, regardless of whether the information requested is the applicant's *personal information*. In addition, individuals should apply under the RTI Act, rather than the IP Act, to amend their own *personal information*.

The current position in relation to fees would not change – there would be no application fee where applications are for only the applicant's *personal information* whereas all other applications would require an application fee.

Access applications and amendment applications – Forms (Review Report, appendix 3)

A valid application under the RTI Act must be in the approved form, provide sufficient information concerning the document sought to enable the agency to identify it, and state an address to which notices may be sent.[88]

The Review Report found that the requirement to apply on a form (rather than in writing, as in other jurisdictions) imposes an additional step for applicants who need to locate, download and submit an approved form. This has been criticised as unnecessarily bureaucratic. No other Australian jurisdiction requires an approved form to make an access application.

[88] RTI Act, s 24(2)(a).

Proposal for change – Remove the requirement for applications to be in the approved form

It is proposed 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.

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.

Evidence of identity – Agents (Review Report, recommendation 23, appendix 3)

Where someone applies for personal information on behalf of another person (as an agent), the agent must provide both evidence of their authority to act on the applicant's behalf and evidence of their own identity.[89]

This requirement extends to all agents and may be seen as burdensome, particularly for legal practitioners, who may make frequent applications to the same agency.

Proposal for change – Remove the requirements for agents to provide evidence of identity in all cases

It is proposed 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.

[89] RTI Act, s 24(3)(b).

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

A person who applies for access to, or amendment of, personal information must provide evidence of their identity.[90] Copies of identification documents must be certified by a qualified witness.[91] A qualified witness means a lawyer or notary public, or a commissioner for declarations, or a justice of the peace.[92]

The Review Report found that it can be difficult for applicants seeking access to documents to access qualified witnesses, particularly in rural or remote areas.

Proposal for change – Expanding the list of qualified witnesses

Amendments are proposed to 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.

Processing applications

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

If an applicant is not given written notice of the decision by the end of the *processing period* for an access application for a document, the agency or Minister is taken to have made a decision refusing access to the document.[93]

The *processing period* is a period of 25 business days from the day the application is received by the agency or Minister.[94] At any time before the end of the processing period, an agency or Minister may ask the applicant for more time to process the application (a *further specified period*).[95] The agency or Minister can continue to process the application only if:

- they have asked the applicant for a *further specified period* before the *processing period* has expired;
- the applicant has not refused the request; and
- the agency or Minister has not received notice that the applicant has applied for internal or external review under the Act.[96]

The Review Report found that the existing timeframes are arguably unnecessarily complex. For example, it is not clear whether a *further specified period* should be added to the end of the *processing period*, or whether it starts as soon as the agency makes the request. If an agency asks for a longer *processing period* and the applicant initially does not respond but later refuses after the *processing period*, it is not clear whether the agency has the additional *processing time* for the period it is waiting for the applicant's response, or whether it has no extra time at all.

[90] RTI Act, s 24(3)(a); IP Act, s 43(3)(a).
[91] RTI Regulation, s 3(2); IP Regulation, s 3(2).
[92] RTI Regulation, s 3(3); IP Regulation, s 3(3).
[93] RTI Act, s 46.
[94] RTI Act, s 18.
[95] RTI Act, s 35(1).
[96] RTI Act, s 35(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 (ie. 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*.

Application outside scope of Act – Timeframes (Review Report, recommendation 23, appendix 3)

If the recipient of an access application decides the application is outside the scope of the Act (for example, because the requested document is a document to which the Act does not apply), the agency or Minister has 10 business days to give the applicant written notice of the decision.[97]

The Review Report found that 10 business days is a very short timeframe for what can be a complex decision. A processing period of at least 25 business days applies in relation to access applications that are not outside the scope of the Act. If the application is for documents that are both inside and outside the scope of the Act, the application will be subject to different timeframes. These differing timeframes can create complex jurisdictional issues for review rights.

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.

Schedule of relevant documents (Review Report, recommendation 3)

Under the RTI Act, applicants must be provided with a schedule of relevant documents before the end of the processing period.[98] The schedule of documents is intended to provide a basis for applicants to consider and narrow the scope of documents sought. The schedule was intended to cut processing times and the costs of providing material.

Agencies have reported that the schedule of documents is not achieving its intended objective, is often not a useful tool for applicants, and applicants rarely reduce the scope of their application on the basis of the schedule. The Review Report found that a more effective way of refining the terms of an application to deliver the best result for the applicant may be for an agency or Minister to consult with the applicant directly.

[97] RTI Act, s 32.
[98] RTI Act, s 36(1)(b)(i).

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.

Charges estimate notices (CENs) – Not required when no charges apply (Review Report, recommendation 23, appendix 3)

Agencies must provide applicants with an estimate of the charges likely to be payable for an application (a charges estimate notice, or CEN) and a schedule of relevant documents before the end of the processing period.[99]

An applicant can agree to waive the requirement for a schedule of relevant documents, but the requirement to provide a CEN cannot be waived, even if an agency decides that charges are not payable, for example, where it spends less than five hours processing the application. The Review Report found that there is arguably no benefit to providing a CEN where no charges apply.

Proposal for change – No requirement for a CEN where no charges

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

CENs – Applicants limited to two (Review Report, recommendation 23, appendix 3)

After receiving a CEN, an applicant can then consult with the agency to either:[100]

- confirm they wish to proceed with their application in its original terms and agree to pay the estimated fees; or
- narrow their application with a view to reducing the amount of charges; or
- withdraw their application.

This must be done within 20 business days of receiving the CEN or the application is taken to have been withdrawn.[101]

The Review Report found that a minor inconsistency currently exists in the RTI Act. Although only two CENs may be issued, if an applicant narrows their applicant after receiving the second CEN, agencies are required to advise that an additional CEN may be issued.

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.

[99] RTI Act, s 36.
[100] RTI Act, s 36(2).
[101] RTI Act, s 36(3).

Additional time for documents sent by post (responding to Review Report, recommendation 11, appendix 3)

Where an applicant has not been given written notice of a *considered decision* by the last day of the processing period, the agency or Minister is taken to have refused the application.[102] This is known as a *deemed decision*. The processing period is 25 business days. Certain periods do not count as part of the processing period, including for example any *further specified period* requested by the agency or Minister.

Section 39A of the *Acts Interpretation Act 1954* provides that where an Act allows a document to be served by post, service is carried out by properly addressing, prepaying and posting the document as a letter. Notice is taken to be 'given' at the time in which the letter would be delivered in the ordinary course of business, unless the contrary is proved. The section applies whether the expression 'deliver', 'give', 'notify', 'send' or another expression is used.

Agencies have reported that changes to Australia Post's delivery times in early 2016 (which added two extra days delivery time to most services) have significantly impacted on processing times where decision notices are delivered by post (rather than email or fax). In practice, an agency must now post written notice by day 20 of the processing period to ensure that the applicant receives the notice by day 25.

Because of the longer delivery times, there is a risk the applicant may not receive the *considered decision* within the 25-day timeframe, whereupon a *deemed decision* refusing access will be taken to have been made.

To address these concerns, the Review Report (recommendation 23, appendix 3) recommended that section 46 of the RTI Act be amended so that written notice is required to be 'sent' (rather than 'given') by the end of the processing period. However, the proposal presents a more practical solution to this issue and avoids difficulties in defining when a notice is 'sent'.

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.

Public interest balancing test (Review Report, recommendation 7)

When deciding an application for access to information under the RTI Act, decision-makers must apply the public interest balancing test.[103] If information is not exempt, agencies must apply the test by balancing relevant public interest factors favouring disclosure and non-disclosure. Agencies must allow access to the information unless, on balance, disclosure would be contrary to the public interest.

[102] RTI Act, s 46.
[103] RTI Act, schedule 4.

The test is a central aspect of the RTI Act and reflects other right to information legislation across Australia.

Schedule 4 of the RTI Act contains four parts, each listing different types of public interest factors:

- Part 1 lists factors *irrelevant* to deciding the public interest – for example, that disclosure of the information could cause embarrassment to the Government;
- Part 2 lists factors *favouring disclosure* in the public interest – for example, that disclosure of the information could reasonably be expected to promote open discussion of public affairs and enhance the Government's accountability;
- Part 3 lists factors *favouring non-disclosure* in the public interest – for example, that disclosure of the information could reasonably be expected to prejudice the collective responsibility of Cabinet; and
- Part 4 lists factors *favouring non-disclosure in the public interest because of the public interest harm in disclosure* – for example, that disclosure of the information could prejudice the conduct of an investigation by the Ombudsman.

The steps in applying the public interest are:[104]

- Identify and disregard any irrelevant factors (part 1 factors);
- Identify any relevant factors favouring disclosure (part 2 factors);
- Identify any relevant factors favouring non-disclosure (part 3 and part 4 factors);
- Balance the factors favouring disclosure against any factors favouring non-disclosure; and
- Decide whether, on balance, disclosure of the information would be contrary to the public interest.

The RTI Act allows decision-makers to consider additional factors in addition to those listed in the four parts of schedule 4 – it provides that the factors to be considered *include* those listed in schedule 4.

The Review Report found that the ability to consider additional factors when applying the public interest test could be made clearer by having an express statement to this effect in the RTI Act.

Proposal for change – Clarify that other matters can be considered

A clarifying amendment to the RTI Act is proposed to include an express statement that factors other than those listed in schedule 4 may be considered as part of the public interest balancing test.

Exemptions

New exemption for information affecting relations with other governments

An agency or Minister must decide to give access to a document unless disclosure would be contrary to the public interest.[105] Schedule 3 of the RTI Act contains exemptions – types of information the disclosure of which the Parliament has considered would, on balance, be contrary to the public interest. Schedule 4 then sets out factors Parliament considers appropriate for deciding whether

[104] RTI Act, s 49.
[105] RTI Act, s 48, s 49.

disclosure of information would be contrary to the public interest – irrelevant factors, relevant factors favouring disclosure, and relevant factors favouring nondisclosure.

If information falls within an exemption in schedule 3, a decision-maker is not required to then apply the public interest balancing test. The Solomon Report recommended that the Act contain only one public interest test.

The RTI Act does not contain a specific exemption for information affecting relations with other governments. Instead, damage to relations with other governments is a factor favouring non-disclosure for decision-makers to consider when applying the public interest test.[106]

Factors favouring nondisclosure in the public interest include where disclosure of the information could reasonably be expected to:

- prejudice intergovernmental relations;[107] or
- cause damage to relations between the State and another government or divulge information of a confidential nature that was communicated in confidence by or for another government.[108]

The COVID-19 pandemic has highlighted the need for intergovernmental decision-making, and requirements for increased co-operation between leaders in Australia and internationally.

All jurisdictions in Australia operate to protect information of this nature. In the Commonwealth, Victoria, Western Australia, South Australia, Tasmania and the Northern Territory, there are exemptions which are subject to a public interest test.[109]

In New South Wales and the Australian Capital Territory, like Queensland, when applying the public interest test a relevant factor favouring nondisclosure exists if disclosure of the information could reasonably be expected to prejudice relations with another government.[110]

Proposal for change – A new exemption for matters affecting relations with government

There is a proposal to create a new exemption for matters affecting relations with other governments.

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. 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

[106] If an access application is made to an agency or Minister for a document, the agency or Minister must decide to give access to the document unless disclosure would, on balance, be contrary to the public interest: s 49.
[107] RTI Act, item 14 of part 3 of schedule 4.
[108] RTI Act, item 1 of part 4 of schedule 4.
[109] *Freedom of Information Act 1982* (Cth), s 47B; *Freedom of Information Act 1982* (Vic), s 29; *Freedom of Information Act 1991* (SA), schedule 1, part 2, item 5; *Freedom of Information Act 1992* (WA), schedule 1, item 2; *Right to Information Act 2009* (Tas), s 34; *Information Act 2002* (NT), s 51.
[110] *Government Information (Public Access) Act 2009* (NSW), s 14; *Freedom of Information Act 1989* (ACT), schedule 2, s 2.2.

- 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.

Internal and external reviews

Review rights – courts and tribunals

The RTI Act does not apply to courts and tribunals (and other judicial and quasi-judicial entities) in relation to their judicial or quasi-judicial functions.[111] This exclusion reflects the fundamental principles of judicial independence – the separation of judicial power from the legislative and executive arms of government. When a person makes an application to a judicial or quasi-judicial entity requesting access to documents relating to the entity's judicial or quasi-judicial functions, that entity may decide that the application is outside the scope of the Act, on the basis that the Act does not apply to the entity.[112]

However, that decision is a reviewable decision, and therefore the person affected can apply for internal review by the entity or external review by the Information Commissioner.[113]

An external review decision by the Information Commissioner can be appealed to the QCAT Appeal Tribunal.[114] An appeal may only be on a question of law and must be heard and decided by a judicial member.[115]

The existence of an external review right to the Information Commissioner of this decision by a judicial or quasi-judicial entity (such as a court) contravenes the principle of judicial independence. This is because on an external review, the judicial or quasi-judicial entity would be subject to the scrutiny of the Information Commissioner. In practical terms, during an external review these entities can refuse to provide the documents in question to the Information Commissioner, to preserve judicial independence, effectively nullifying the Information Commissioner's external review jurisdiction.

Since the tabling of the Review Report, a series of appeals in the QCAT Appeal Tribunal[116] has clarified the application of the RTI and IP Acts to courts and tribunals, highlighting the central importance of judicial independence.

[111] RTI Act, ss 14, 17 and items 1 to 8 of schedule 2, part 2.
[112] RTI Act, s 32.
[113] RTI Act, s 80(1), 85, schedule 5.
[114] RTI Act, s 119(1).
[115] RTI Act, s 119(2), (4)(b).
[116] *Carmody v Information Commissioner & Ors* [2018] QCATA 14; *Carmody v Information Commissioner & Ors (No 2)* [2018] QCATA 15; *Carmody v Information Commissioner & Ors (No 3)* [2018] QCATA 16; *Carmody v Information Commissioner & Ors (No 4)* [2018] QCATA 17; *Carmody v Information Commissioner & Ors (No 5)* [2018] QCATA 18; *Carmody v Information Commissioner & Ors (No 6)* [2018] QCATA 19; *Q20 v Department of Justice and Attorney-General* [2020] QICmr 40.

Proposal for change – Removal of the right to internal review and external review in relation to courts and tribunals exercise of judicial functions

It is proposed to remove the right of internal review and external review to the Information Commissioner of a decision by a judicial or quasi-judicial entity that an application is outside the scope of the Act, because the Act does not apply to the entity in relation to its judicial or quasi-judicial functions.

The right to appeal to the QCAT Appeal Tribunal on a question of law would be retained. This would ensure oversight of the original decision but will be more consistent with the principles of judicial independence. Any rights of judicial review under parts 3 and 5 of the *Judicial Review Act 1991* would be unaffected.

The proposed amendment would reflect the current reality, which is that external review by the Information Commissioner of these decisions is effectively not available, preserve judicial independence with respect to the operation of the RTI Act, and clarify the position for users of the RTI Act. Although there will be no administrative review by the executive, there will still be a right to a 'safeguard' appeal which can only be conducted by the judiciary.

Timeframes for internal review (Review Report, recommendation 11)

A person affected by a reviewable decision may apply to have the decision internally reviewed by the agency or Minister dealing with the application.[117] A decision on an internal review application must be made as soon as possible, but not later than 20 business days after the internal review application is made.[118] If the applicant is not notified of a decision within 20 business days of their internal review application being made, the agency is deemed to have affirmed the original decision.[119]

Although internal reviews are conducted quickly in many cases, in some situations it would benefit the applicant for agencies to have additional time to process an internal review application. For example, where additional documents that were not processed as part of the original application have been located and need to be considered and where consultation needs to be undertaken with a third party. The Review Report found that allowing agencies to extend the time in which the agency must make an internal review decision may also help to reduce the number of matters proceeding to external review.

Proposal for change – Allow extension of time for internal review decisions

It is proposed 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.

[117] RTI Act, s 80(1).
[118] RTI Act, s 83.
[119] RTI Act, s 83(2).

Disclosure of documents to other parties at external review (Review Report, recommendation 11, appendix 3)

A person affected by a reviewable decision may apply to have the decision externally reviewed by the Information Commissioner.[120] The Commissioner, after conducting an external review of a decision, must make a written decision either affirming the decision, varying the decision, or setting aside the decision and substituting the Commissioner's decision.[121]

The Information Commissioner has broad powers on external review. The procedure to be followed is, subject to the RTI Act, within the discretion of the Commissioner[122] and the Commissioner is not bound by the rules of evidence and may inform himself or herself on any matter in any way the Commissioner considers appropriate.[123] The Information Commissioner has power to do all things that are necessary or convenient to be done for, or in connection with, the performance of the Commissioner's functions under an Act,[124] which include investigating and reviewing decisions of agencies and Ministers.

While conducting an external review, the Commissioner may identify a third party to whom the disclosure of the documents may be of concern but who was not identified when the agency was making its decision at first instance.[125] However, despite the broad powers outlined above, the Information Commissioner must not disclose documents the subject of the review to anyone, other than:

- a member of the staff of the OIC in the course of performing duties as a member of the staff; or
- a person who created the document or who gave the document or information in the document to the agency or Minister (or that person's representative when participating in a review).[126]

Because of this restriction, current practice is for the Commissioner to prepare correspondence asking the third party to advise the Commissioner of their views about disclosure of the documents, and to request that the agency send this correspondence on the Commissioner's behalf.

Proposal for change – Allow Commissioner to disclose documents during an external review to third parties

To assist the Commissioner in performing his or her function of investigating and reviewing an agency's decision, and to reduce the resource burden for agencies required to consult third parties on behalf of the Commissioner, it is proposed that the RTI Act be amended to allow the Commissioner to disclose documents during an external review to third parties, to facilitate the resolution of an external review.

It is proposed that the basis for such disclosure by the Commissioner should correspond to that in section 37(1) and (2) for an agency at first instance. So, on external review, where a document

[120] RTI Act, s 85.
[121] RTI Act, s 110.
[122] RTI Act, s 95(1)(a).
[123] RTI Act, 95(1)(c).
[124] RTI Act, s 125.
[125] See RTI Act, s 37.
[126] RTI Act, s 107.

contains information the disclosure of which may be reasonably expected to be of concern to a third party, despite section 107, the Commissioner may give access to the document to the third party to:

- obtain the views of the third party about whether:
  - the document is a document to which the Act does not apply; or
  - the information is exempt information or contrary to public interest information; and
- to inform the third party that if access is given to the document because of an access application, access may also be given to the document under a disclosure log.

If the Commissioner discloses a document to a third party, the Commissioner would be required to notify the agency that it has done so.

Release of documents following informal resolution settlement (Review Report, recommendation 11, appendix 3)

The Information Commissioner is required to identify opportunities and processes for early resolution of external review applications, including mediation, and promote settlement of external review applications.[127] The term *informal resolution* is used to describe the methods used by the Information Commissioner to resolve applications, or particular issues raised in applications, on an informal basis.

If an external review is resolved informally, the Commissioner must give each participant in the external review notice that the external review is complete, with the external review taken to be complete at the date of that notice.[128]

Agencies may be reluctant to release documents, or parts of documents, during the informal resolution process, due to the application of confidentiality provisions in other legislation to the information to be released as part of the informal resolution. The Review Report found that agencies may not consider section 6 of the RTI Act (Relationship with other Acts prohibiting disclosure of information) adequate to protect them in the context of informal resolution, particularly where there is no written decision from the Information Commissioner.

Proposal for change – Clarify an agency may release documents following informal resolution

It is proposed to amend the RTI Act to clarify that an agency may release documents following an informal resolution of a review.

While one view is that the Act already allows for the release of documents by an agency as a result of an informal resolution settlement, it is arguably preferable to expressly provide that documents may be released by an agency as a result of an informal resolution settlement to give agencies comfort and confidence. This would also assist agencies who have legislative provisions prohibiting disclosure as the release of documents will be in accordance with legal authority.

[127] RTI Act, s 90(1).
[128] RTI Act, s 90(4).

Application of the RTI Act and IP Act

Prescribing entities under the RTI Act

An entity may be declared by regulation to be a public authority,[129] and thus subject to the RTI Act,[130] if the entity meets any of the following criteria:[131]

- the entity is supported directly or indirectly by government funds or other assistance; or
- the government is in a position to exercise control over the entity; or
- the entity is established under an Act; or
- the entity is given public functions under an Act.

On 14 August 2018, the CCC tabled the Windage Report, following an investigation by the CCC into allegations of corruption related to Ipswich City Council. The Windage Report concluded that private companies established by local governments can create corruption risks through a lack of oversight and transparency. Recommendation 3(b) of the Windage Report was that entities controlled by councils should come within the oversight of the CCC and the RTI Act.

In Queensland, State and local Governments perform their functions using a wide range of structures, including for example companies, trusts, funds and other entities, with a broad range of commercial and charitable purposes. Many entities are automatically subject to the RTI Act, as they come under the definition of 'agency'.[132] However, many entities are not, even though they may be funded or provided assistance by government or subject to government control. For example, companies incorporated under the *Corporations Act 2001* (Corporations Act) are not covered by the RTI Act. Currently only the Bar Association of Queensland has been declared by regulation as a public authority.

Proposal for change – Clearer criteria for prescribing entities under the RTI Act

Amendments are proposed to the RTI Act to provide clearer criteria for prescribing entities as public authorities, to clarify that entities can be prescribed for only part of their functions, and to clarify that companies under the Corporations Act can be prescribed.

An amendment is also proposed to introduce non-binding factors in the RTI Act to provide guidance as to whether to prescribe an entity. These would include (but not be limited to) the following:

- if the entity is a company, whether it is a company limited by shares;
- the size of the entity, based on number of employees or level of turnover;
- the purpose of the entity, including whether it is performing functions that are generally identified with the functions of government; and
- the extent to which functions of the entity have previously been undertaken by government.

The proposed amendment recognises the broad range of entities controlled by councils and the State, providing a targeted mechanism by which entities can be subject to additional transparency and oversight, on a case-by case basis, without instituting a blanket and inflexible approach.

[129] RTI Act, s 16(1)(c).
[130] RTI Act, s 14.
[131] RTI Act, s 16(1)(c).
[132] RTI Act, s 14.

Contracted service providers (Review Report, recommendation 1)

Privacy obligations under the IP Act apply to contracted service providers, in that contracting agencies are required to take all reasonable steps to ensure that the contracted service provider is required to comply with the privacy principles.[133] Once bound, the contracted service provider is responsible for any breach of the privacy obligations in the IP Act and an individual can make a privacy complaint against the contracted service provider.

Subcontractors are not subject to the IP Act. The Review Report found that failure to contractually bind a subcontracted service provider to comply with the privacy principles means that an individual whose personal information is dealt with by that subcontracted provider will not be afforded any privacy protection.

An OIC Guideline (issued under section 132 of the RTI Act) recommends agencies consider either prohibiting the use of a subcontractor or requiring any subcontractor to comply with the privacy principles.

Proposal for change – Extend privacy obligations to subcontractors

An amendment is proposed to extend privacy 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 privacy 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 the privacy principles, the contracted service provider would be liable for any privacy breaches committed by the subcontractor.

This may not represent a significant change in practice where agencies already impose contractual obligations on contracted service providers to require any subcontractors to comply with the privacy principles under the IP Act, as recommended in the Guidelines published by the OIC.

Organisations established by letters patent

In *Stanway v Information Commissioner & Anor*,[134] Judge Horneman-Wren decided that the Frederick Marsden Youth Centre Inc – an entity initially established as an orphanage in 1929 by letters patent issued by the Governor – was a public authority (and therefore an agency) under the RTI Act.

The implications of the Stanway decision are that other organisations established by letters patent (generally for a religious or charitable purpose) could be subject to the RTI and IP Acts. This is inconsistent with the purpose of the RTI Act, which is essentially to give a right of access to information in the government's possession or under the government's control. It would also be inconsistent with the purpose of the IP Act, which is to ensure government entities handle personal information appropriately.

[133] IP Act, chapter 2, part 4.
[134] [2017] QCATA 030.

Further, should these entities fall within the scope of the RTI and IP Acts, dealing with information access applications and complying with the privacy principles is likely to impose an unsustainable administrative burden.

Proposal for change – Entities established by letters patent not subject to RTI Act and IP Act

To overcome the effect of the Stanway decision, and to maintain consistency with the purpose of the RIT and IP Acts, it is proposed to amend the RTI Act and the IP Act to ensure that they do not apply to entities established by letters patent.

Privacy issues

Note: Part A of the Consultation Paper discusses various proposals for significant changes to Queensland's framework for information privacy. If some of these reforms were implemented (for example a single set of privacy principles) some of the below proposals may no longer be relevant. Nevertheless, feedback is welcome on all proposals.

Privacy complaints – Requirements (Review Report, recommendation 17)

Under the IP Act, an individual must not make a complaint to the Information Commissioner unless:

- the individual has first complained to the agency;
- at least 45 business days have elapsed since the complaint was made; and
- the individual has either not received a response to the complaint, or the individual has received a response but considers it inadequate.[135]

However, the Review Report found that the IP Act does not specify how a privacy complaint must be made to an agency. The IP Act also does not contain any requirements in relation to an agency's complaints management process.

Proposal for change – Requirements for lodgement of a privacy complaint

It is proposed to introduce certain requirements for lodgement of a privacy complaint with an agency to ensure some degree of consistency and certainty in the way privacy complaints are received and handled across agencies. It is proposed to amend the IP Act to specify that privacy complaints 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 complaint.

Agencies would be able to accept a complaint older than 12 months if it is reasonable in the circumstances. Agencies may develop their own internal policies to determine when the discretion will be exercised. The OIC may also issue guidelines[136] as to when such powers ought to be exercised.

[135] IP Act, s 166(3).
[136] IP Act, s 132.

Agencies would also be required to give reasonable help to an individual making a privacy complaint. This could include, for example, providing details about how to lodge the complaint and who the complaint should be addressed.

Privacy complaints – Timeframes (Review Report, recommendation 18; Strategic Review Report, recommendation c)

A person may not make a privacy complaint to the Information Commissioner unless certain conditions have been met, including that at least 45 business days have elapsed since making the complaint to the agency and the person has either not received a response from the agency or considers the response to be inadequate.[137]

The Review Report found that specifying a 45-day timeframe raises two issues. Firstly, it may be difficult for relevant entities to resolve privacy complaints in this relatively short period, for example, where a privacy complaint is complex to resolve or is part of another grievance process (like a workplace dispute). Secondly, an applicant may receive a response to their complaint quickly, but if they are dissatisfied with the agency's response, they cannot take their complaint to the Information Commissioner until the 45 business days have passed.

Both scenarios may cause frustration for a complainant. In a jurisdiction that heavily emphasises the informal resolution of complaints, the capacity for the process to be a source of frustration can prevent the resolution of complaints.

Proposal for change – Allow agencies to request extensions of time for resolution of privacy complaints

To allow for greater flexibility and the more efficient resolution of privacy complaints, it is proposed to amend the provisions in the IP Act affecting timeframes for privacy complaints to allow agencies to request extensions of time if required. Extensions of time would be by agreement with the complainant.

It is also proposed to amend the IP Act to allow a complainant to refer their complaint to the 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.

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

Under the IP Act, if a privacy complaint is made to the Information Commissioner and either the Information Commissioner does not believe the complaint can be resolved by mediation, or mediation is attempted but is not successful, the Information Commissioner must, within 20 business days of being asked to do so, refer the privacy complaint to QCAT.[138] QCAT must then exercise its original jurisdiction under the *Queensland Civil and Administrative Tribunal Act 2009* to hear and decide the referred privacy complaint.

[137] IP Act, s 166(3).
[138] IP Act, s 175.

No provision limits the time within which an applicant may ask the Information Commissioner to refer the complaint to QCAT if the Information Commissioner is unable to resolve a complaint. In comparison, in Victoria, applicants must tell Office of the Victorian Privacy Commissioner in writing within 60 days of receiving the Commissioner's decision if they want their complaint referred to the Victorian Civil and Administrative Tribunal.

Proposal for change – Time limit for applicant to ask Information Commissioner to refer complaint to QCAT

To ensure certainty, it is proposed to amend the IP Act to provide that an applicant has 60 days 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, or mediation is attempted but is not successful. The Information Commissioner would have discretion to extend the timeframe if reasonable in the circumstances.

NPPs and health agencies (Review Report, recommendation 22)

A law enforcement agency is not subject to the following IPPs if the law enforcement agency is satisfied on reasonable grounds that noncompliance is necessary for specified law enforcement activities:[139]

- IPP 2 (Collection of personal information (requested from individual));
- IPP 3 (Collection of personal information (relevance etc.));
- IPP 9 (Use of personal information only for relevant purpose);
- IPP 10 (Limits on use of personal information);
- IPP 11 (Limits on disclosure).

This recognises that an agency's use of personal information for investigation and enforcement purposes may not be compatible with the IPPs in all circumstances. For example, it would defeat the purpose of covert surveillance if agencies were to inform an individual that their personal information was being collected.

The Review Report found that there is no equivalent exemption for health agencies with law enforcement functions in relation to the NPPs. Health agencies with law enforcement functions should be exempt from the requirement to comply with some NPPs in the same manner that law enforcement agencies are currently exempt from compliance with the IPPs.

[139] IP Act, s 29.

Proposal for change – Exempt health agencies with law enforcement functions from compliance with corresponding NPPs

It is proposed to ensure health agencies with law enforcement functions are exempt from the requirement to comply with corresponding NPPs, subject to the health agency being satisfied on reasonable grounds that noncompliance with the NPP is necessary for:

- 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
- the management of property seized or restrained under a law relating to the confiscation of the proceeds of crime; or
- the enforcement of a law, or of an order made under a law, relating to the confiscation of the proceeds of crime; or
- the execution or implementation of an order or decision made by a court or tribunal, or
- the conduct of proceedings started or about to be started in a court or tribunal in relation to the responsibility.

IPP 4 – Element of reasonableness (Review Report, recommendation 21)

Information Privacy Principle 4 (IPP 4) provides that an agency having control of a document containing personal information must ensure that the information is protected against loss, unauthorised access, use, modification or disclosure and any other misuse.

The Review Report found that the strict requirement in IPP 4 means that there is no element of reasonableness or a requirement to take reasonable steps as is the case in other IPPs (for example, IPP 2, which only requires an agency to 'take all reasonable steps' to ensure certain consequences occur). IPP 4 could result in an agency being responsible for a breach of IPP 4 even when it had taken all reasonable measures to keep information secure. There may be instances of loss or misuse outside the reasonable control of an agency, for example loss of a data centre during a natural disaster event. This obligation is also not consistent with the obligation on health agencies in National Privacy Principle 4 (NPP 4), which requires a health agency to take reasonable steps to protection information.

Proposal for change – Amendment to IPP 4

It is proposed to amend IPP 4 to provide, in line with other IPPs, that an agency must take *reasonable steps* to protect information.

Transferring personal information outside Australia (Review Report, recommendation 15)

The IP Act restricts the circumstances in which agencies may transfer an individual's personal information outside of Australia to where one of the exceptions in that section apply, for example, where the individual agrees to the transfer, where the transfer is authorised or required under a law or where the transfer is necessary to lessen or prevent a serious threat to an individual or to the public. Agencies are increasingly using a range of technology, such as smartphones, drones, and tablets as part of their day-to-day business and cloud computing solutions are becoming more popular. The use of such technology may result in the transfer of personal information outside Australia in situations in breach of the IP Act, for example, if the information is stored on an overseas server.

The Review Report found that the restrictions on overseas transfer are burdensome, particularly where the transfer of information is low risk. The broad meaning of the word *transfer* creates unnecessary complexity for agencies and leads to outcomes potentially not considered at the time the laws were passed. For example, sending someone their own personal information when they are overseas would be a transfer. Transfer is simply the movement of personal information and does not take into account the content of the information or whether or not the agency retains control of it.

Proposal for change – Regulate *disclosure* of personal information outside Australia

It is proposed to amend the IP Act to regulate *disclosure of personal information* outside Australia rather than *transfer* of information. *Disclosure of personal information* is defined under the IP Act,[140] such that an entity (the first entity) discloses personal information to another entity (the second entity) if:

- the second entity does not know the personal information, and is not in a position to be able to find it out; and
- the first entity gives the second entity the personal information, or places it in a position to be able to find it out; and
- the first entity ceases to have control over the second entity in relation to who will know the personal information in the future.

The amendment would utilise the existing definition of *disclosure of personal information* and would therefore provide clarity to agencies as to when the restriction regarding transferring information overseas applied. The definition is also less broad than the concept of a *transfer*, which is beneficial for agencies.

Definition of generally available information (Review Report, recommendation 20)

Under the IP Act, the privacy principles do not apply to a document that is a generally available publication.[141] A generally available publication is defined to be '… a publication that is, or is to be made, generally available to the public, however it is published'.[142]

The Review Report found that the definition does not provide clear guidance about what constitutes a generally available publication. In particular, it is not clear that a generally available publication includes a publication which is available for a fee. By contrast, the definition of generally available publication in section 6 of the *Privacy Act* is more specific and technology neutral:

> *a magazine, book, article, newspaper or other publication that is, or will be, generally available to members of the public:*
> *(a) whether or not it is published in print, electronically or in any other form; and*
> *(b) whether or not it is available on the payment of a fee.*

[140] IP Act, s 23.
[141] IP Act, schedule 1.
[142] IP Act, schedule 5.

Proposal for change – Amend the definition of *generally available publication* in the IP Act

It is proposed to amend the definition of *generally available publication* in 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.

Other issues

Disclosure logs – which documents to publish (Review Report, recommendation 8)

The RTI Act requires agencies to maintain disclosure logs – online details of applications made to the agency under the RTI Act, and online documents already released under that Act.[143] The rationale for disclosure logs is that if one person has expressed an interest in accessing particular documents, then the same documents might be of interest to the wider community. Disclosure logs also provide an opportunity for the agency to publish documents with associated supporting information, explaining issues of public interest in greater depth. Disclosure logs are part of proactive disclosure of information under the RTI Act.

Prior to commencement of amendments made in 2012, all agencies were subject to the same disclosure log requirements. However, the 2012 amendments made some significant changes, including making it compulsory for departments and Ministers (not other agencies) to publish on a disclosure log documents which have been released to an applicant (unless the documents fall within certain exceptions, including being defamatory). Previously, departments and Ministers had discretion whether to include the documents on a disclosure log (for example, in the interests of space and readability, documents which were heavily redacted may not have been published). In addition, even if the documents were to be made available, departments and Ministers would only include information identifying the document and information about how the document could be accessed rather than publishing the material in full.

The Review Report found that questions have arisen as to the effectiveness of disclosure logs and whether the criteria for what should and should not be in disclosure logs results in useful information being published. Questions have also arisen around whether the increased burden on departments and Ministers has resulted in relevant and useful information being proactively published.

Proposal for change – Disclosure log requirements

Amendments are proposed to the RTI Act so that departments and Ministers are subject to the requirements that applied before the 2012 amendments. All agencies would therefore be subject to the same requirements, where copies of a document may be included on a disclosure log if reasonably practicable, but otherwise, details identifying the document and information about how to access may be included on the disclosure log.

[143] RTI Act, chapter 3, part 7, division 2.

The purpose of the proposed amendment is to ensure disclosure logs are accessible and relevant. These changes would also reduce the administrative burden imposed by current disclosure log requirements on departments and Ministers. It is also proposed that disclosure log requirements be supported by Information Commissioner Guidelines, rather than Ministerial Guidelines (see section 78B of the RTI Act), providing further assistance and guidance to agencies about what to include in a disclosure log.

Disclosure logs – Information about applicants (Review Report, recommendation 9)

Following the 2012 amendments, departments and Ministers must also publish on a disclosure log the applicant's name and the name of any entity for whose benefit access to the document was sought (if relevant).

The Review Report found that there is arguably little substantive benefit in disclosure logs having information about applicants. In addition, applicants may be concerned about their personal information being published on websites.

Proposal for change – Disclosure logs – Information about applicants

It is proposed 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; and
- remove the requirement for applicants to state whether they have applied for access on behalf of another entity as part of their application.

Publication schemes (responding to Review Report, recommendation 10)

Agencies, other than excluded agencies, must publish a scheme (a *publication scheme*) setting out the classes of information that the agency has available, and the terms on which it will make the information available, including any charges that apply.[144]

Publication schemes must be compliant with any Ministerial Guidelines.[145] The current Guidelines[146] specify the classes of information which must be published, and require information published to be significant, appropriate, accurate, current and up to date. They also specify that where possible, the information must be easily accessible through an agency's website and a direct link to the document should be provided.

Publication schemes are intended to assist in 'pushing' government information into the public domain, as access applications for information are intended as a last resort.

Publication scheme requirements under the RTI Act have been criticised as overly prescriptive and redundant, resulting in duplication of information and administrative inefficiency. Stakeholders have suggested that there is little benefit to having the relevant content published under the publication

[144] RTI Act, s 21(1).
[145] RTI Act, s 21(3).
[146] Ministerial Guidelines, Operation of Publication Schemes and Disclosure Logs at www.rti.qld.gov.au.

scheme where agency websites have become more easily navigable and user-friendly and where the information is already published elsewhere on the website. Arguably, members of the public are more likely to search a website for information by subject, rather than via a publication scheme. Agencies have also reported that publication schemes are often seen as a compliance exercise, rather than an easily locatable and searchable source of information.

Since 2009, other government initiatives aimed at pushing government information out have been developed, including the Open Data portal, the Government Publication portal, the Queensland Government website and franchise based websites which deal with particular themes, such as 'Your Rights, Crime and the Law' or 'Environment, land and water'.

Other jurisdictions have less onerous requirements, instead generally requiring agencies to maintain an 'information statement', outlining the functions of the agency, the information the agency holds, and the procedures for accessing that information. Certain documents are required to be published, however not via the 'information statement' itself.

However, such a scheme should be consistent with 'information statement' requirements in other Australian jurisdictions, outlining the functions of the agency, the information the agency holds, and the procedures for accessing that information.

Recommendation 10 of the Review Report was that current publication scheme requirements should be removed and agencies should instead be required to routinely publish significant, accurate and appropriate information about the agency on whichever website is most relevant.

However, this may not have provided sufficient guidance to agencies and may not have resulted in publication of appropriate information. Accordingly, the proposal requires further information to be published.

Proposal for change – Publication scheme requirements

Agencies should continue to be required to publish a publication scheme. However, it is proposed that publication scheme requirements more closely reflect the requirements in other jurisdictions. Agencies would still be required to publish certain documents, however this information would not be required to be published within an agency's publication scheme or under specific 'classes' of information. Agencies would therefore be able to integrate the required information into more relevant parts of their websites and/or other websites where appropriate, rather than via their publication schemes. This would prevent duplication of the publication of information and ensure accessibility by the public.

It is proposed to amend the RTI Act to require agencies to maintain a publication scheme which outlines:

- the structure and functions of the agency;
- how the functions of the agency affect members of the public;
- any arrangements to enable members of the public to engage with the agency's functions;
- the kinds of information held by the agency;
- the kinds of information that the agency makes publicly available and how that information is made available; and

- procedures for requesting information including any fees which may be payable.

It is proposed that agencies would be required to publish information prescribed by regulation, to the extent that the information is held by the agency, and where that information is significant, appropriate and accurate. The RTI Regulation could be amended to prescribe, for example, the following information:

- the agency's policy documents (as currently defined in section 20 of the RTI Act);
- the agency's reports, lists and registers as required by legislation;
- the agency's budgetary papers;
- information about government grants made or administered by the agency;
- information about the agency or the work of the agency contained in any document tabled in the Legislative Assembly by or for the agency; and
- information about all boards, councils, committees, panels and other bodies that have been established by the agency and any report or recommendation prepared by these bodies.

To reduce restrictions on the format in which agencies publish information, it is proposed that requirements to comply with Ministerial guidelines be removed. The publication scheme regime can continue to be supported by Information Commissioner guidelines under section 132 of the Act (section 132 of the RTI Act allows the Information Commissioner to publicly issue guidelines, including for publication schemes and disclosure logs).

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

The RTI and IP Acts provide that the Minister administering the Act must prepare an annual report on the operation of the Act and arrange for it to be tabled in Parliament.[147] The RTI and IP Regulations set out the details of what must be included in the annual report, including for example numbers of access and amendment applications, refusals to deal with applications, refusals of access under each relevant provision of the RTI Act, documents included in a disclosure log, and internal and external review applications received.[148]

The Review Report found that preparing the annual report imposes a significant burden on reporting agencies, particularly where agencies do not have efficient systems in place to collect and report on data, and on the agency which collates the information.

There are clear interests in having meaningful data available that will provide scrutiny of the effectiveness of the legislation and whether it is achieving its objectives, but the usefulness of the information agencies currently report on is unclear. Stakeholders have reported that the current data collected is not a meaningful representation of their activities under the Acts.[149] In addition, the metrics reported on, and the distance in time from recording to publication, limit the value this information provides to effective planning and management of activity.

[147] RTI Act, s 185; IP Act, s 194.
[148] RTI Regulation, s 8; IP Regulation, s 6.
[149] Strategic Review Report, p 14.

In several Australian jurisdictions (the Commonwealth, Victoria, Western Australia and the Northern Territory) the Information Commissioner, rather than the Minister, is responsible for preparing the annual report.

Proposal for change – Annual reporting requirements

It is proposed to amend the annual reporting requirements to minimise administrative burden for agencies, improve utility of data, and facilitate timeliness of reporting by:

- transferring legislative responsibility for preparing the annual reports from the responsible Minister to the Information Commissioner;
- requiring agencies to provide the information to the Information Commissioner as soon as practicable after the end of a financial year; and
- requiring the Information Commissioner to give any annual reports to the Speaker and parliamentary committee, who must then cause the report to be tabled in the Assembly on the next sitting day after it is given.

It is proposed that the information which must be included in the annual report continue to be prescribed under the RTI and IP Regulation.

Currently, s 8(c) of the RTI Regulation and s 6(c) of the IP Regulation effectively require agencies to count every time a refusal provision is relied on. It is proposed instead that reporting on the total refusal provisions used for an application as a whole would be preferable. Other prescribed data could include:

- the number of access applications received by each agency and Minister, as well as the outcomes of these complaints, including for example which applications were granted in full or in part, which refused in full or in part, which refused to be dealt with;
- the number of privacy complaints received by each agency and Minister, as well as the outcomes of these privacy complaints;
- applicant type (for example, member of the public, lawyer/agent, private business, media, community organisation, Member of Parliament); and
- data relating to push model initiatives and proactive release of information.

It is proposed to remove the requirement for agencies to report on details of external review applications made from their decisions as the OIC is already required to report on external review matters.

The proposal to include data relating to push model initiatives and proactive release of information is in addition to information included in recommendation 12 of the Review Report.

Reports to the Speaker
(Review Report, recommendation 11, appendix 3)

The RTI Act provides a general power for the Information Commissioner to do all things necessary or convenient for the performance of the Commissioner's functions.[150] The Information Commissioner's support functions include monitoring the way the public interest test is applied by agencies.[151]

There is no specific ability for the Commissioner to report to the Speaker on systemic issues (including the way in which the public interest test is applied by agencies). This is contrast with the IP Act. Under that Act, after conducting a review into personal information handling practices of relevant entities to identity privacy related issues of a systemic issue generally, the Commissioner may report to the Speaker on the findings of any review.[152]

Proposal for change – Reports to the Speaker

For consistency between the two Acts, it is recommended that the RTI Act be amended to clarify that the Information Commissioner can report to the Speaker on systemic issues.

The purpose of the amendment would be to provide a power to the Commissioner to report to the Speaker on a broad range of matters which relate to the Commissioner's functions, including external review. The amendment would not displace the existing requirement that the Commissioner report on the outcome of a review to the parliamentary committee (section 131(2)).

[150] RTI Act, s 125.
[151] RTI Act, s 128(1)(d).
[152] IP Act, s 135.