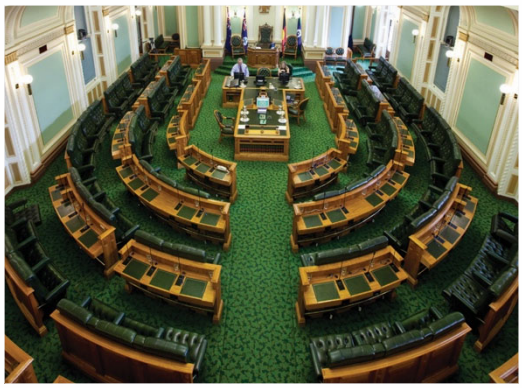
Parliamentary Committees


Inquiry into the Information Privacy and Other Legislation Amendment Bill 2023

Report No. 40, 57th Parliament
Education, Employment and Training Committee
November 2023

Education, Employment and Training Committee

Chair	Ms Kim Richards MP, Member for Redlands
Deputy Chair	Mr James Lister MP, Member for Southern Downs
Members	Mr Mark Boothman MP, Member for Theodore
	Mr Nick Dametto MP, Member for Hinchinbrook
	Mr Barry O'Rourke MP, Member for Rockhampton*
	Mr Jimmy Sullivan MP, Member for Stafford
	* Mr Don Brown MP, the Member for Capalaba, was appointed as a substitute member on behalf of Mr O'Rourke from 3-26 October 2023.

Committee Secretariat	
Telephone	+61 7 3553 6657
Email	eetc@parliament.qld.gov.au
Technical Scrutiny Secretariat	+61 7 3553 6601
Committee webpage	www.parliament.qld.gov.au/EETC

Acknowledgements

The committee acknowledges the assistance provided by the Department of Justice and Attorney-General and the Department of the Premier and Cabinet.

All web address references are current at the time of publishing.

Appendix F at the back of the report lists abbreviations and acronyms used in the report.

Contents

Chair's foreword

On behalf of the Education, Employment and Training Committee, I present this report on the committee's Inquiry into the Information Privacy and Other Legislation Amendment Bill 2023.

I commend this report to the House.

The committee's task was to consider the policy to be achieved by the legislation and the application of fundamental legislative principles – that is, to consider whether the Bill has sufficient regard to the rights and liberties of individuals, and to the institution of Parliament. The committee also examined the Bill for compatibility with human rights in accordance with the *Human Rights Act 2019*.

The primary objectives of the Bill are to: strengthen Queensland's information privacy framework to better protect personal information and improve responses and remedies for data breaches and data misuse; clarify and improve the operation of Queensland's information privacy and right to information frameworks; and provide for the proactive release of Cabinet documents.

To inform its examination of the Bill, the committee called for and received eight written submissions from stakeholders, was briefed by the Department of Justice and Attorney-General and the Department of the Premier and Cabinet, and heard evidence from key stakeholders at a public hearing on 13 November 2023.

On the basis of this evidence, the committee is satisfied that the Bill will achieve its policy objectives. The committee has made 3 recommendations, firstly that the Bill be passed, a recommendation to amend a provision in clause 33 of the Bill to impose a time limit on extended periods for assessments, and a further recommendation designed to clarify the impact of a proposed amendment to the definition of 'public authority' to exclude entities established by letters patent.

On behalf of the committee, I thank those individuals and organisations who made written submissions on the Bill. I also thank our Parliamentary Service staff as well as the officers from the two departments that assisted the committee during this inquiry.

Kim Richards MP

Chair

Recommendations

Executive Summary

This report presents a summary of the Education, Employment and Training Committee's examination of the Information Privacy and Other legislation Amendment Bill 2023.

The Bill aims to:

- strengthen Queensland's information privacy framework to better protect personal information and improve responses and remedies for data breaches and data misuse
- clarify and improve the operation of Queensland's information privacy and right to information frameworks
- provide for the proactive release of Cabinet documents.

The Bill proposes to implement or respond to recommendations for legislative change made in several recent reviews and reports. It does this primarily by amending two Acts:

- the *Information Privacy Act 2009* (IP Act)
- the *Right to Information Act 2009* (RTI Act)

The committee is satisfied that the Bill will meet these policy objectives, and therefore recommends that the Bill be passed.

The Bill raises several issues relating to human rights and the fundamental legislative principles set out in the *Legislative Standards Act 1992*, including:

- the impacts of proposed amendments to s 408E of the Criminal Code to strengthen offence provisions related to the misuse of a restricted computers on the right to liberty and security
- whether the adoption of Queensland Privacy Principles (QPPs) in lieu of most National Privacy Principles and Australian Privacy Principles would impact the right to privacy and reputation
- the impacts of enhanced entry powers for authorised officers of the Office of the Information Commissioner on the right to privacy and reputation
- whether the imposition of time limits for complainants to request referral of privacy complaints for adjudication impacts their right to a fair hearing
- impacts of proposed changes to internal and external review processes on the right to privacy and reputation
- whether the proposed amendments to the RTI Act that would allow agencies and Ministers to extend the time in which they must make internal review decisions are consistent with the principles of natural justice
- whether proposed amendments to the IP Act to impose timeframes for the Information Commissioner to give written notice that they do not believe the complaint can be resolved by mediation or an unsuccessful attempt at mediation, and for a complainant to refer a privacy complaint to the Queensland Civil and Administrative Tribunal are consistent with the principles of natural justice
- the impact of amendments to the IP Act to require a privacy complaint to a 'relevant entity' to be made within 12 months of the complainant becoming aware of the act or practice the subject of the complaint
- the impact of amendments to the IP Act to provide for the extension of the 'processing period' for an access or amendment application by 5 business days, if the application complies with all relevant application requirements and the applicant has only supplied a postal address for notices

- the impact of amendments to the IP Act to provide power for an 'authorised officer' to enter an agency's place of business, or another place occupied by the agency, in the specified circumstances
- whether new penalties under the IP Act for offences are relevant and proportionate
- whether proposed new transitional provisions for continuation of offences, that abrogate existing statutory rights, have sufficient regard to rights and liberties of individuals
- whether the delegation of legislative power for: the establishment of QPP codes, the extension of assessment periods for the mandatory data breach notification scheme; and the waiver of obligations, has sufficient regard to the Institution of Parliament
- whether the delegation of legislative power for the declaration of Corporations legislation displacement, by regulation, has sufficient regard to the Institution of Parliament.

Having considered these issues, the committee is satisfied the Bill is compatible with the *Human Rights Act 2019*, and has sufficient regard to fundamental legislative principles.

1 Introduction

On 12 October 2023, Hon Leanne Enoch MP, Minister for Treaty, Minister for Aboriginal and Torres Strait Islander Partnerships, Minister for Communities and Minister for the Arts introduced the Information Privacy and Other Legislation Bill 2023 on behalf of the Attorney-General. It was then referred to the Education, Employment and Training Committee, to report by 24 November 2023.

1.1 Policy objectives of the Bill

The Information Privacy and Other Legislation Amendment Bill 2023 (Bill) aims to:

- strengthen Queensland's information privacy framework to better protect personal information and improve responses and remedies for data breaches and data misuse
- clarify and improve the operation of Queensland's information privacy and right to information frameworks
- provide for the proactive release of Cabinet documents.

Most of the amendments proposed in the Bill relate to the *Information Privacy Act 2009* (IP Act) and the *Right to Information Act 2009* (RTI Act). The major changes it proposes include:

- aligning the definition of 'personal information' in the IP Act with the equivalent federal Act
- adopting a single set of privacy principles, the Queensland Privacy Principles (QPPs), based on the equivalent federal principles
- establishing a mandatory data breach notification (MDBN) scheme for government agencies
- enhancing the powers and functions of the Information Commissioner
- improving the process for making and dealing with RTI applications under the RTI Act, and the process for making privacy complaints, under the IP Act
- clarifying the definition of 'public authority' and thus the scope of the IP and RTI Acts
- facilitating the introduction of a proactive release scheme for Cabinet documents by:
    - ensuring that certain information and documents will remain exempt from the scheme and, therefore, public release
    - providing Ministers with protection from civil liability
    - protecting public interest immunity.[1]

The Bill also proposes amendments to section 408E (Computer hacking and misuse) of the Criminal Code to remove the reference to 'hacking' in the offence title to clarify the type of conduct captured by the offence. The Bill would also reclassify the offence as a misdemeanour, and increase the maximum penalty from two to three years imprisonment.

Schedules 1 and 2 make minor amendments to other Acts and regulations.

[1] Explanatory notes, pp 2-5.

1.2 The Bill responds to recent reviews and reports

The Bill proposes to implement or respond to recommendations for legislative change made in several recent reviews and reports:

- **the Review Report**[2]
  Department of Justice and Attorney-General, *Review of the Right to Information Act 2009 and Information Privacy Act 2009*, Report, October 2017
- **the Impala Report**[3]
  Crime and Corruption Commission, *Operation Impala, A report on misuse of confidential information in the Queensland public sector,* Report, February 2020
- **the Windage Report**[4]
  Crime and Corruption Commission, *Culture and Corruption Risks in Local Government: Lessons from an investigation into Ipswich City Council*, Report, August 2018
- **Strategic Review Report**[5]
  PWC, *Strategic Review of the Office of the Information Commissioner*, Report, 26 April 2017
- **Coaldrake Report**[6]
  Prof Peter Coaldrake, *Let the sunshine in: Review of culture and accountability in the Queensland public sector*, Final Report, 28 June 2022

Appendix D maps the relevant recommendations from each of these reviews and reports to the parts of the Bill that implement them.

1.3 Alignment of the IP Act with the *Privacy Act 1988* (Cth)

A number of provisions of the Bill seek to amend the IP Act to align with provisions of the *Privacy Act 1988* (Cth) (Commonwealth Privacy Act).

The amendments to the IP Act in the Bill do not pre-empt anticipated changes to the Commonwealth Privacy Act which is currently under review.

Key provisions of the Bill propose amendments to the IP Act to align provisions with the Commonwealth Privacy Act. These include:

- the amendment of the definition of 'personal information' to accord with the definition contained in the Commonwealth Privacy Act[7]
- the adoption of a single set of privacy principles (the QPPs) that are broadly based on the Australian Privacy Principles contained in the Commonwealth Privacy Act[8]

2 Available here: https://documents.parliament.qld.gov.au/tp/2017/5517T2014.pdf.

3 Available here: https://www.ccc.qld.gov.au/sites/default/files/Docs/Public-Hearings/Impala/Operation-Impala-report-on-misuse-of-confidential-information-in-the-Queensland-public-sector-v2.pdf.

4 Available here: https://www.ccc.qld.gov.au/sites/default/files/Docs/Publications/CCC/Culture-and-corruption-risks-in-local-government-Lessons-from-Ipswich-City-Council-Operation-Windage-Report-2018.pdf.

5 Available here: https://documents.parliament.qld.gov.au/tp/2017/5517T698.pdf.

6 Available here: https://www.coaldrakereview.qld.gov.au/assets/custom/docs/coaldrake-review-final-report-28-june-2022.pdf.

7 Department of Justice and Attorney-General, Briefing paper, 19 October 2023, p 3.

8 Department of Justice and Attorney-General, Briefing paper, 19 October 2023, p 4.

- the introduction of a mandatory data breach notification scheme. The features of the scheme draw upon the established scheme under the Commonwealth Privacy Act, as well as the *Privacy and Personal Information Protection Amendment Act 2022* (NSW)[9]

The federal government is reviewing the Commonwealth Privacy Act. The final review report released on 16 February 2023, contained 116 proposals for reform. In its response to the review report, released on 28 September 2023, the federal government agreed to 38 proposals, agreed in-principle to 68 proposals and noted 10 proposals.[10]

In its response to the review report, the federal government noted that the privacy reforms will complement other reforms being progressed, including Digital ID, the 2023-2030 Australian Cyber Security Strategy, the National Strategy for Identity Resilience, and Supporting Responsible AI in Australia, and will be progressed under the following focus areas:

- bringing the Commonwealth Privacy Act into the digital age
- uplift protections
- increased clarity and simplicity for entities and individuals
- improved control and transparency for individuals over their personal information
- strengthened enforcement powers for the Office of the Australian Information Commissioner.[11]

The next stage of the review will involve the development of legislative amendments informed by a detailed impact analysis and targeted consultation with stakeholders. The federal government will also engage with entities on proposals which are 'agreed in-principle' to explore whether and how they could be implemented so as to proportionately balance privacy safeguards with potential other consequences and any additional regulatory burden.

In its briefing paper prepared for the committee, the department clarified that the amendments to the IP Act proposed in the Bill do not pre-empt any anticipated changes to the Commonwealth Privacy Act.[12]

1.4 Legislative compliance

In accordance with s 93 of the *Parliament of Queensland Act 2001*, the committee's examination of the Bill included consideration of: the policy to be given effect by the legislation; the application of fundamental legislative principles (FLPs) contained in the *Legislative Standards Act 1992*; and the Bill's compatibility with the *Human Rights Act 2019* (HRA).

The Bill raises a number of issues relating to human rights and fundamental legislative principles.

Having considered these issues, the committee is satisfied the Bill is compatible with the *Human Rights Act 2019*, and has sufficient regard to fundamental legislative principles.

---

9 Department of Justice and Attorney-General, Briefing paper, 19 October 2023, p 9.

10 Australian Government, 2023, *Fact Sheet - Government Response: Privacy Act Review Report*, p 3. https://www.ag.gov.au/sites/default/files/2023-09/fact-sheet-government-response-privacy-act-review-report.PDF. 'Agreed in-principle' indicates that further engagement with entities and a comprehensive impact analysis is needed before the federal government makes a final decision on implementation of a proposal.

11 Australian Government, 2023, *Fact Sheet - Government Response: Privacy Act Review Report*, p 3. https://www.ag.gov.au/sites/default/files/2023-09/fact-sheet-government-response-privacy-act-review-report.PDF.

12 Department of Justice and Attorney-General, Briefing paper, 19 October 2023, p 3.

1.4.1 Human Rights Act 2019

According to the statement of compatibility, the Bill engages four human rights:

- the freedom of expression
- the right to privacy and reputation
- the rights to liberty and security of person
- the right to a fair hearing.[13]

There are nine aspects of the Bill that engage these rights in different ways:

- the amendments to s 408E of the Criminal Code (computer hacking and misuse) (cl 4)[14]
- the removal of review rights, as a result of the judicial and quasi-judicial functions of courts and tribunals being placed outside the scope of the RTI Act[15]
- the amendments to the definition of 'public authority', which will place entities established by letters patent outside the scope of the IP Act and RTI Act[16]
- the time limits placed on requests to refer complaints to the Queensland Civil and Administrative Tribunal (QCAT) under the IP Act[17]
- the power given to agencies to collect, use and disclose personal information where reasonably necessary to respond to data breaches [18]
- the creation of exceptions permitting the Information Commissioner and authorised staff to disclose personal information where necessary to lessen or prevent serious threats to life, health and safety[19]
- the creation of entry and inspection powers as part of the MDBN Scheme[20]
- the amendments to the RTI Act to maintain the 'status quo' regarding public interest immunity, despite the introduction of the proactive release of Cabinet documents[21]
- the creation of an immunity from civil liability for Ministers relating to information disclosure[22]

As such, one of the key issues considered by the committee was whether the safeguards included in the Bill are sufficient to protect human rights and, where rights would be limited, the extent to which those limitations are reasonable and justified.

This report discusses a number of provisions with the human rights implications as well as safeguards for limiting impacts on human rights.

1.4.1.1 Statement of compatibility

Section 38 of the HRA requires a statement of compatibility to be tabled for the Bill. The statement of compatibility did not always contain sufficient information to facilitate understanding of the Bill in

13 Statement of compatibility, p 3.
14 Statement of compatibility, p 4.
15 Statement of compatibility, p 6.
16 Statement of compatibility, p 8.
17 Statement of compatibility, p 10.
18 Statement of compatibility, p 12.
19 Statement of compatibility, p 14.
20 Statement of compatibility, p 16.
21 Statement of compatibility, p 19.
22 Statement of compatibility, p 20.

relation to its compatibility with human rights and the purpose of the limitation of certain rights, including on the following:

- consideration of less restrictive measures to achieve the purpose of the limitation on the right to liberty and security of person through the amendments to s 408 of the Criminal Code.
- sufficient connection between the proposed higher imprisonment term introduced through the amendments to s 408 of the Criminal Code (the means) and deterrence (the end it is seeking to achieve).

Generally, however the statement of compatibility provided sufficient information and detail as required under the HR Act.

The committee is satisfied that the safeguards included in the Bill to protect human rights are sufficient, and that the extent of any limitations on human rights are reasonable and justified in the circumstance.

The committee is also generally satisfied with the level of detail provided in the Statement of Compatibility tabled with the Bill.

1.4.2 Legislative Standards Act 1992

The committee assessed the Bill's compliance with the *Legislative Standards Act 1992* (LSA).

The Bill raises several issues relating to FLPs.[23] Many of these overlap with the human rights issues noted in the previous section, such as time limits placed on requests to refer complaints to QCAT under the IP Act.[24]

The most notable FLP issues raised by the Bill that do not overlap with the human rights issues already noted, include:

- the creation of new offences in the IP Act as part of the MDBN Scheme (cl 33)[25]
- a transitional provision which provides for the continuation of proceedings and convictions for offences against former ss 185 or 187 of the IP Act (cl 73)[26]
- the delegation of legislative power under provisions relating to:
    - the approval of Queensland Privacy Principles Codes of Practice by the Minister (cl 43)[27]
    - the preparation (by the Information Commissioner) and approval (by the Minister) of guidelines about the collection, use and disclosure of personal information about people reported as missing (cl 74)[28]
    - extensions of time to assess data breaches under the MDBN Scheme (cl 33)[29]

[23] Fundamental legislative principles are the principles relating to legislation that underlie a parliamentary democracy based on the rule of law. These principles include requiring that legislation has sufficient regard to rights and liberties of individuals and the institution of Parliament. See LSA, s 4.

[24] Explanatory notes, pp 7-8.

[25] Explanatory notes, p 9.

[26] Explanatory notes, p 12.

[27] Explanatory notes, p 13.

[28] Explanatory notes, p 13.

[29] Explanatory notes, p 14.

- the waiver or modification of privacy principle requirements by the Information Commissioner (cl 40)[30]
- the potential displacement of the *Corporations Act 2001* by regulation (cl 72).[31]

Most of these provisions are discussed in the report.

1.4.2.1 Explanatory notes

Explanatory notes were tabled with the introduction of the Bill. The explanatory notes contain the information required by Part 4 of the LSA and a sufficient level of background information and commentary to facilitate understanding of the Bill's aims and origins.

Having considered the provisions of the Bill, the committee is satisfied that its impact on fundamental legislative principles in regard to the rights and liberties of individuals and the Institution of Parliament is justified, and that the Bill is, therefore, compatible with fundamental legislative principles.

1.4.2.2 Consultation for the development of the Bill

The majority of the provisions of the Bill were subject to public and stakeholder consultation by the Department of Justice and Attorney-General. This included the department's release of a consultation paper for comment in June 2022.[32]

In August 2023, the department circulated a consultation draft of the Bill for targeted consultation. That draft contained amendments to give effect to information privacy and RTI reforms.[33]

No public consultation was conducted by the Government regarding the amendments in the Bill that support the proactive release of Cabinet documents.[34]

The majority of measures contained in the Bill seek to implement or address recommendations for legislative change from recent review reports noted above (the Review Report, Impala Report, Windage Report, Strategic Review Report, and Coaldrake Report). These reviews and reports had separate consultation processes.[35]

1.5 Bill should be passed

The committee is required to determine whether or not to recommend that the Bill be passed.

Recommendation 1

The committee recommends that the Information Privacy and Other Legislation Amendment Bill 2023 **be passed**.

30 Explanatory notes, p 14.

31 Explanatory notes, p 14.

32 Department of Justice and Attorney-General, 2022, *Proposed changes to Queensland's Information privacy and right to information framework*, https://www.publications.qld.gov.au/ckan-publications-attachments-prod/resources/7326cb08-a3da-451c-8c48-dc08ea9dcc6d/consultation-paper-proposed-changes-qld-ip-rti-framework.pdf?ETag=f9671bcc9b57d55cc316d1c803234761.

33 Explanatory notes, p 15.

34 Explanatory notes, p 15.

35 Department of Justice and Attorney-General, Briefing paper, 19 October 2023, p 2.

2 Examination of the Bill

This section discusses key issues raised during the committee's examination of the Bill. It does not discuss all consequential, minor or technical amendments. It discusses:

- defining 'personal information'
- the adoption of a single set of Queensland Privacy Principles
- QPP Codes
- the mandatory data breach notification (MDBN) Scheme
- misuse of restricted computers
- the proactive release of Cabinet documents
- waivers of obligations
- corporations legislation displacement
- the exclusion of letters patent entities from 'public authority' definition
- the time limit to request referral of privacy complaint to QCAT.

2.1 Defining 'personal information'

The Bill amends the IP Act to replace s 12 (Meaning of *personal information*), s 13 (Meaning of a *document* of an agency for ch 3) and s 14 (Meaning of a *document* of a Minister for ch 3) with new ss 12 and 13.

The new definition of personal information is consistent with the current definition in the Commonwealth Privacy Act, as recommended by the Impala Report (Recommendation 16).

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. The definition is also central to the effective operation of the IP Act as agencies' and bound contracted service providers' obligations arise in relation to personal information.

Recommendation 16 of the Impala Report recommended, in part, that the definition of 'personal information' in the IP Act be amended to accord with the definition contained the Commonwealth Privacy Act.

Clause 12 replaces ss 12 to 14 of the IP Act with a new meaning of *personal information* consistent with the current definition in s 6 of the Commonwealth Privacy Act. It provides:

> **12 Meaning of personal information**
>
> Personal information means information or an opinion about an identified individual or an individual who is reasonable identifiable from the information or opinion -
>
> (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.[36]

In its written brief, the department advised that 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.'[37]

[36] Bill, cl 12.

[37] Department of Justice and Attorney-General, Briefing paper, 19 October 2023, p 4.

Clause 12 of the Bill also inserts new s 13 of the IP Act which provides the personal information is 'held' by a relevant entity, or the entity 'holds' personal information, if the personal information is contained in a document in the possession, or under control, of the relevant entity. This definition is consistent with the definition of "holds" in s 6 (Interpretation) of the Commonwealth Privacy Act.[38]

2.1.1 Issues raised by stakeholders

Several submitters questioned whether the definition is fit for purpose in the digital age, or should be amended to align with changes to the definition in the Commonwealth Privacy Act mooted by the federal government for introduction in 2024.

Salinger Consulting Pty Ltd submitted that rapid advances in technologies, including artificial intelligence (AI) and facial recognition, mean that 'not identifiable by name' is no longer an effective proxy for 'who will suffer no privacy harm'.

They argued that the Bill should be 'amended, to explicitly incorporate into the threshold definition of 'personal information' the concept of *individuation*' which they describe as:

> …the 'singling out' of a person from a crown – a threat to privacy, autonomy and dignity.[39]

Salinger also commented that the federal government is working to amend the definition of 'personal information' in the Privacy Act following three court cases relevant to AI: the 7-Eleven case, the Clearview AI case and the Australian Federal Police case.[40] All 3 cases involved the storage of facial images in breach of Australian Privacy Principles.

In relation to the definition of personal information, the federal government's response to the Privacy Act review noted:

> Importantly, the Government considers that an individual may be reasonably identifiable where they are able to be distinguished from all others, even if their identity is not known.[41]

Salinger recommended specific changes to the definition to:

- refer to information or an opinion 'that relates to' (rather than 'about') an identified individual or an individual who is reasonably identifiable;
- refer to an individual being 'reasonably identifiable' if they are capable of being distinguished from all others, even if their identity is not known.[42]

The QLS noted that the Commonwealth Privacy Act Review has recommended changing the word 'about' in the definition to 'relates to' as part of proposals to seek to clarify that personal information includes technical information, inferred information and other information where that information relates to that individual and the connection is not too tenuous or remote'.[43]

The QLS recommended awaiting finalisation of the Privacy Act review process before amending the definition in the Information IP Act to ensure the stated aim of consistency is achieved.[44]

---

38 Explanatory notes, p 17.

39 Submission 2, p 4.

40 Salinger have published a summary of the three court cases on their website at: https://www.salingerprivacy.com.au/2022/04/11/oaic-determinations-blog/.

41 Attorney-General's Department, 2023, Government Response to the Privacy Act Review report, p 5. https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report.

42 Submission 2, p 2.

43 Submission 7, p 2.

44 Submission 7, p 2.

IIS Partners recommended that the definition of 'personal information be immediately updated if the definition in the Commonwealth Privacy Act is updated, and that this be prioritised ahead of other more complex updates.[45]

2.1.2 Advice from the department

The department told the committee:

- The federal government's response to the Privacy Act Review Report agreed in-principle that:
  - amendments to the Privacy Act are needed to clarify that personal information is an expansive concept that includes technical and inferred information (such as IP addresses and device identifiers) if this information can be used to identify individuals (see proposal 4.1);
  - the Commonwealth Privacy Act should include non-exhaustive lists to assist entities to determine when information will be personal information and when an individual will be reasonably identifiable (see proposals 4.2 and 4.4).
- It understands that the next stage of work in the Commonwealth Privacy Act Review will involve the development of legislative amendments informed by a detailed impact analysis and targeted consultation with stakeholders. The Commonwealth Government will also engage with entities on proposals which are 'agreed in-principle' to explore whether and how they could be implemented so as to proportionately balance privacy safeguards with potential other consequences and additional regulatory burden.
- The amendments to the definition of 'personal information' in the Bill do not pre-empt any anticipated changes to the Commonwealth Privacy Act but rather seek to achieve better alignment with the enacted legislation.
- It is a matter for Government whether further consideration should be given to amending the definition of personal information to align with any future changes to the definition.[46]

Committee comment

The committee notes the views expressed by stakeholders, and agrees with the proposed amendments relating to the meaning of 'personal information' in the IP Act to align the existing definition with the current definition in the Commonwealth Privacy Act.

The committee also notes the importance of maintaining consistency with subsequent changes to the Commonwealth Privacy Act that result from the federal government's ongoing review of that Act.

45 Submission 8, p 3.

46 Department of Justice and Attorney-General, Correspondence, 10 November 2023, pp 2-3.

2.2 Adoption of a single set of Queensland Privacy Principles

The Bill amends the IP Act to introduce a single set of privacy principles (the Queensland Privacy principles (QPPs)), to replace the two sets of privacy principles currently in the IP Act.

This change is in response to Recommendation 16 of the Impala Report, and Recommendations 13 and 15 of the Review Report.

The proposed QPPs are intended to give Queenslanders a greater understanding of their privacy rights, and confidence that their personal information will be regulated in a consistent manner across Commonwealth, state and local governments.

The IP Act currently contains two sets of privacy principles:

- the National Privacy Principles (NPPs), which apply to health agencies
- the Information Privacy Principles (IPPs), which apply to all other agencies.

The Commonwealth Privacy Act contains the Australian Privacy Principles (APPs), which apply to Commonwealth agencies, and 'organisations' (i.e. private entities that include larger businesses with an annual turnover of more than $3 million per annum).

The Bill at cls 22 and 23 proposes to adopt, and require agencies to comply with, a single set of QPPs based on the APPs in the Commonwealth Privacy Act, in place of the NPPs applying to health agencies and the IPPs applying to all other agencies. The proposed QPPs are set out in proposed new Schedule 3 of the IP Act, contained in cl 74. **Appendix E** summarises the QPPs proposed in the Bill.

Clause 23 proposes amendments to s 27 of the IP Act to require that an agency (defined in s 18 of the IP Act to mean: a Minister, department, local government or public authority), other than an APP entity, must comply with QPPs.

Contracted service providers will continue to be bound by the new QPPs. Further, the Bill provides that the QPPs only apply to new contracts entered into after commencement, unless there is agreement to a variation.[47] The Bill does not extend the new privacy principle requirements to subcontractors.

The Bill also contains a range of exceptions to the QPPs, including in permitted general situations, and permitted health situations, some of which go beyond the exceptions in the Commonwealth Privacy Act.

2.2.1 QPPs give effect to review recommendations

The proposed changes give effect, in part, to a number of recommendations from the Impala report and the Review report.

From the Impala Report - Recommendation 16 recommended, in part, that the IPPs and NPPs in the IP Act be amalgamated and strengthened, having regard to the APPs contained in the Commonwealth Privacy Act.

From the Review Report - Recommendation 13, in part, states that the government should conduct further research and consultation to establish whether there is justification for moving towards a single set of privacy principles in Queensland. Recommendation 15 from that report recommended that the IP Act be amended to regulate 'disclosure' of information outside Australia rather than 'transfer'.

[47] Department of Justice and Attorney-General, Correspondence, 10 November 20923, p 7. See new s 216 to be inserted by cl 73.

2.2.2 APPs not reflected in QPPs proposed in the Bill

A number of APPs are not reflected, or are only partly reflected in, the QPPs proposed in the Bill, which would be a lessening of rights to privacy and reputation.

In further advice, the department explained that the QPPs in the Bill are broadly consistent with the APPs, with appropriate modifications to address the needs of Queensland agencies. Accordingly, the rights of access to, and correction of, personal information under QPP 12 and 13 respectively incorporate only those elements of APP 12 and 13 which are broadly consistent with existing privacy principles in the IP Act. The elements which have not been adopted from QPP 12 and 13 are the more detailed and prescriptive requirements of APP 12 and 13. They relate to issues such as timeframes, charges and notice provisions.

The department also advised that consultation was previously conducted with stakeholders on adopting the requirements of APP 12 and 13 in full. However, feedback from stakeholders was that to include all these elements in the QPPs would create duplicative provisions, add an additional and unnecessary process, could lead to appeals to QCAT, may negate the benefit of having a single right of access under the RTI Act, and would create timeframes inconsistent with those in the RTI Act.[48]

The Bill therefore adopts only some elements of APP 12 and 13, minimising overlap with the existing framework under the RTI Act and IP Act. As the formal and comprehensive rights of access and amendment under the RTI Act and IP Act continue, it is not considered there are any negative impacts on human rights.[49]

In its brief for the committee, the department noted that, while there are similarities between the new QPPs and the current IPPs and NPPs, the new QPPs impose higher standards than existing principles in some respects.[50]

2.2.3 Need for consistency between federal and state privacy frameworks

Stakeholders raised the following issues about ensuring consistency between APPs and QPPs:

- IIS Partners supported a goal of uniformity with the APPs to the extent possible, and do not support any additional amendments to the QPPs which undermine uniformity and introduce inconsistency or needless complexity.[51]
- IIS Partners also submitted that the committee should recommend immediate future review and update of the IP Act in the event of changes to the Commonwealth Privacy Act with the aim of ensuring ongoing legislative uniformity.[52]
- QLS noted its members' concerns about the timing of reforms before the review and reform of the Commonwealth Privacy Act has been finalised, and the risk this will create confusion and perpetuate inconsistencies between the State and Commonwealth privacy frameworks'[53]
- QLS recommended that the proposed QPPs be finalised after the Commonwealth Privacy Act reforms to ensure greater consistency and that any reforms adequately respond to current cyber security concerns.[54]

48 Department of Justice and Attorney-General, Correspondence, 20 November 2023, pp 3-4.

49 Department of Justice and Attorney-General, Correspondence, 20 November 2023, p 4.

50 Department of Justice and Attorney-General, Briefing paper, 19 October 2023, p 4.

51 Submission 8, p 2.

52 Submission 8, p 2.

53 Submission 7, p 2.

54 Submission 7, p 3.

In response, the department advised:

- It understands that the next stage of work in the Commonwealth Privacy Act Review will involve the development of legislative amendments informed by a detailed impact analysis and targeted consultation with stakeholders. The Commonwealth Government will also engage with entities on proposals which are 'agreed in-principle' to explore whether and how they could be implemented so as to proportionately balance privacy safeguards with potential other consequences and additional regulatory burden.
- The new single set of privacy principles do not pre-empt any anticipated changes to the Commonwealth Privacy Act but rather seek to achieve better alignment with the enacted legislation.
- It is a matter for Government whether further consideration should be given to amending the (QPPs) to align with future changes made to the APPs.[55]

2.2.4 Disclosure of personal information to overseas recipients and the failure to adopt APP 8 in proposed QPPs

Stakeholders raised a number of issues about the disclosure of personal information to overseas recipients, and the failure to adopt APP8 in proposed QPPs:

- QLS noted that the Commonwealth Privacy Act review includes consideration of whether APP 8 and the related accountability framework in s 16C of the Commonwealth Privacy Act requires clarification to protect consumers and support entities disclosing information overseas.[56]
- QLS recommended that consideration be given to revisiting the approach in s 33 of the IP Act following progress on the Commonwealth Privacy Act reforms, to avoid inconsistency and regulatory uncertainty for agencies.[57]
- OIC considered that QPP 8 would provide a better mechanism for regulating overseas disclosure of personal information than relying on s 33 alone, and that QPP 8 would confer greater flexibility on agencies and ensure Queensland's privacy framework is as closely aligned to the Commonwealth Privacy Act as possible.[58]
- OIC recommended that, should s 33 remain as the preferred method for regulating overseas disclosures of information (rather than adopting s 16C and APP 8 of the Commonwealth Privacy Act), the wording of the exceptions permitting overseas disclosures in certain circumstances are aligned with the wording of exceptions allowing disclosures in QPP 6:
    - section 33(a) should refer to 'consented' rather than 'agrees';
    - section 33(b) should refer to 'authorised or required under an Australian law or a court or tribunal order', rather than 'authorised or required under a law'; and
    - section 33(c) should not refer to 'welfare'.[59]

In response, the department advised:

- The Bill retains, with minor amendments (including replacing the term 'transfer' with 'disclosure'), s 33 of the IP Act regarding the transfer of personal information outside

55 Department of Justice and Attorney-General, Correspondence, 10 November 2023.

56 Submission 7, p 4.

57 Submission 7, p 5.

58 Submission 3, p 5.

59 Submission 3, p 5.

Australia. The Bill does not adopt APP 8 which concerns the disclosure of personal information to overseas recipients.

- The Commonwealth Government's response to the Commonwealth Privacy Act Review has agreed in-principle to various measures facilitating overseas data flows, including a mechanism to prescribe 'safe countries' to send information, with support provided by the Office of the Australian Information Commissioner (OAIC).
- It is a matter for Government whether any further changes will be made to the QPPs, including s 33 of the IP Act, once the Commonwealth Government response to the Privacy Act Review Report is legislated. [60]

2.2.5 Implications for local governments and agencies implementing new QPPs

The committee paid particular attention to points raised by the LGAQ about the impact the proposed MDBN scheme would have on the state's 77 local governments.

The LGAQ:

- noted that there would likely be administrative and resource implications for agencies and organisations in adopting a new single set of privacy principles which will need to be absorbed by those agencies and organisations.[61]
- noted that Queensland local governments will have to review and amend policies, procedures and systems and provide training to staff to appropriately embed these new principles which will involve ongoing costs on individual councils' budgets.[62]
- noted that implementation will be challenging for councils and without considerable financial support there will be a corresponding impost on ratepayers.[63]
- recommended that the State Government develop and adopt industry specific codes and guidelines developed specifically for the local government sector to directly inform their obligations and ensure guidance materials reflect their operating environment.[64]

In response, the department advised:

- Adopting a single set of privacy principles for Queensland government agencies and their bound contracted service providers is intended to: provide a uniform set of rules; give Queenslanders greater understanding of their privacy rights; and provide confidence that personal information will be regulated in the same way across all agencies, including where it is held by a local government.
- Clause 33 of the Bill provides that QPP codes may be initiated by the Information Commissioner or an agency. QPP codes are intended to allow a best practice approach to privacy across government and to help to build a consistently high standard for personal information management. Importantly, QPP codes are not intended to set a lower standard than the QPPs but rather provide more specific detail about how the QPPs are to be applied or complied with.
- Resourcing of the Office of the Information Commissioner (OIC) to undertake education and training will assist agencies and entities to implement the reforms. Phased commencement, including a 12-month delay to implement the MDBN scheme for local government, will

60 Department of Justice and Attorney-General, Correspondence, 10 November 2023.

61 Submission 4, p 5.

62 Submission 4, p 5.

63 Submission 4, p 6.

64 Submission 4, p 6.

provide a longer period for councils to transition to the new MDBN scheme and mitigate the immediate resourcing impact of needing to implement MDBN at the same time as other reforms, including new single set of privacy principles.

- It is currently anticipated that the reforms to the IP Act in the Bill will be commenced on proclamation by 1 July 2025. The MDBN Scheme for local government would then commence 1 July 2026. This delay will provide local governments with additional time to prepare for commencement, noting the significant work involved.[65]

2.3 QPP Codes

The Bill proposes amendments to the IP Act to facilitate the use of QPP codes as part of the information privacy framework.[66]

A QPP code is a written code of practice about information privacy, approved by regulation,[67] that states how one or more of the QPPs are to be applied or complied with, and the agencies that are bound by the code, or a way of determining the agencies that are bound by the code.[68] A QPP code may also impose additional requirements to those imposed by a QPP, to the extent the additional requirements are not inconsistent with a QPP.[69] The amendments would also require that an agency must not do an act, or engage in a practice, that contravenes a QPP code.[70]

Institution of Parliament

Delegation of legislative power, scrutiny by Legislative Assembly

A Bill should allow the delegation of legislative power only in appropriate cases and to appropriate persons.[71] Further, a Bill should sufficiently subject the exercise of a delegated legislative power to the scrutiny of the Legislative Assembly.[72] Legislation that incorporates into the law documents that are made by bodies outside of Parliament have the potential to adversely impact the institution of Parliament.[73]

The proposed use of QPP codes raises concerns about respect for the institution of Parliament, as these codes would be prepared by the Information Commissioner or an agency, and approved by the Minister, as opposed to being scrutinised by Parliament.

The explanatory notes justify the use of codes in these circumstances because the 'focus of the QPP codes is expected to be of a practical and operational nature which would not be appropriately suited to be dealt with in primary legislation'.[74]

A number of factors are relevant to the departure from fundamental legislative principles:

- Before the Information Commissioner or agency submits a draft code to the Minister, a draft must be published on an accessible agency website and the public must be invited to make submissions (and the submissions must be considered).[75]

65 Department of Justice and Attorney-General, Correspondence, 10 November 2023, pp 4-5.
66 Bill, cl 33 inserts new ss 40-43 IP Act.
67 Under new section 43 of the IP Act.
68 Bill, cl 33 inserts IP Act, s 40(1).
69 Bill, cl 33 inserts IP Act, s 40(2).
70 Bill, cl 33 inserts IP Act, s 41.
71 LSA, s 4(4)(a).
72 LSA, s 4(4)(b).
73 OQPC, Notebook, p 148.
74 Explanatory notes, p 13.
75 Under new s 42 of the IP Act.

- If the Minister endorses a draft code (or a draft amendment to a code), the QPP code (or amendment) will only take effect once it is approved by regulation.[76] The associated regulation will be subject to the usual tabling and disallowance provisions,[77] providing for a level of parliamentary scrutiny.

Committee comment

While the use of QPP codes is a delegation of legislative power, the committee notes that:

- the content of the codes is intended to be practical and operational in nature
- draft QPP codes will need to be open to public consultation
- final QPP codes and amendments must be approved by regulation, allowing for some level of parliamentary scrutiny.

Given these factors, the committee considers the breaches of fundamental legislative principles regarding the delegation of legislative power and scrutiny by the Legislative Assembly in relation to proposed amendments to the IP Act to provide for the use of QPP codes are reasonable and justified.

2.4 The Mandatory Data Breach Notification (MDBN) Scheme

The Bill proposes amending the IP Act to introduce a Mandatory Data Breach Notification (MDBN) scheme for public agencies. This change is a response to Recommendation 13 of the Review Report, Recommendation 12 of the Impala Report, and Recommendation 10 of the Coaldrake Report.

The introduction of the MDBN scheme would be a significant reform. It would likely strengthen the protection of personal information held by public agencies, including local governments.

2.4.1 Queensland needs an MDBN Scheme

According to the department's brief for the committee:

- A data breach[78] may be caused by malicious action, human error or a failure in information handling or security systems.
- 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.
- Queensland government agencies are currently not subject to any legislative requirements in the IP Act to notify data breaches concerning individuals' personal information, though, they are subject to a voluntary notification scheme under the OIC's Privacy Breach Management and Notification Guideline.
- 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).
- The introduction of a MDBN scheme is intended to ensure that there are clear, consistent requirements for Government agencies to notify individuals of data breaches, so that

[76] Under new s 43 of the IP Act.

[77] See SI Act, ss 49-50.

[78] Examples of a data breach 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.

individuals are able to take steps to reduce the risk of harm. This is expected to promote transparency, accountability and public confidence in Government agencies that handle personal information.[79]

2.4.2 The MDBN Scheme proposed in the Bill

All 29 substantive provisions required to establish the MDBN scheme are contained in a single clause of the Bill, cl 33.

The MDBN Scheme applies to agencies

The MDBN Scheme would apply to agencies. Under the IP Act, amended as proposed in the Bill, 'agency' would include:

- a Minister
- a department
- a local government
- a public authority (a term further defined by s 21 of the Act, subject to amendments in cl 19 of the Bill which clarify its scope).

However, 'agency' does not include entities mentioned in Schedule 2 of the IP Act, either in full, or in relation to the specific function listed in that schedule.[80] This means, for example, that the Legislative Assembly will not be subject to the MDBN Scheme, nor will courts in relation to their judicial function.[81] The MDBN scheme also does not apply to contracted service providers or subcontractors, consistent with the approach taken in the NSW MDBN scheme.[82]

Notably, the Bill clarifies that 'public authority' does not include an entity established by letters patent.[83] According to the statement of compatibility, such entities are generally charitable and religious organisations, for example churches, church trusts, bible societies, welfare associations, historical associations and kindergarten associations. They are excluded from the operation of the IP Act (and the RTI Act) because 'the information they hold is not properly characterised as *information in the government's possession or under the Government's control*' (emphasis original).[84]

General requirements under the MDBN Scheme

Under the MDBN Scheme, agencies would be required to:

- keep a register of eligible data breaches, which must include specified information[85]
- prepare and publish a data breach policy.[86]

The MDBN Scheme would require notification if a serious harm is likely

The MDBN Scheme is designed to protect personal information held by agencies. It would apply if there is an 'eligible data breach'. This means a data breach affecting an agency that:

- involves unauthorised access to, or disclosure of, personal information that is likely to result in serious harm to the individual to whom the information results, or

79 Department of Justice and Attorney-General, Briefing paper, 19 October 2023, pp 8-9.

80 IP Act, s 19; Bill, cl 16.

81 IP Act, Schedule 2.

82 Department of Justice and Attorney-General, Correspondence, 10 November 2023, p 7.

83 Bill, cl 19(5).

84 Statement of compatibility, p 9.

85 Bill, cl 33, proposed s 72 of the IP Act.

86 Bill, cl 33, proposed s 73 of the IP Act.

- involves personal information being lost in circumstances where unauthorised access to or disclosure of the information is likely, and this would be likely to result in serious harm to an individual.[87]

Whether a data breach falls into this category would be determined by reference to a number of factors, including the kind of personal information concerned and how sensitive it is.[88]

Obligations of agencies when a data breach occurs

Where an agency knows, or reasonably suspects, that a data breach has occurred, it would be required to:

- immediately take all reasonable steps to contain the data breach
- assess whether the data breach is an 'eligible data breach' within specified time limits (generally, within 30 days)
- take all reasonable steps to mitigate the harm caused by the data breach
- notify other agencies about data breaches that may affect them.[89]

Once an agency has determined that a data breach is an eligible data breach, it would be required to:

- notify, as soon as practicable, the Information Commissioner via a statement containing specified information (including a description of the kind of personal information affected, recommendations about how affected individuals should respond, and the number of people likely affected)[90]
- notify, as soon as practicable, individuals whose personal information has been affected about the data breach. This notification must:
    - be done on an individual basis, unless this is not reasonably practicable, in which case notification may be made by publishing information on an accessible agency website
    - include specific information, including: a description of the data breach and how it occurred, details about the personal information affected, information about the steps taken by the agency to mitigate harm, and information about how individuals can make a privacy complaint.[91]

Exemptions to the MDBN Scheme

Agencies would not have to comply with the notification requirements under the MDBN Scheme:

- to the extent that it would prejudice a criminal investigation or proceedings before a court or tribunal[92]
- if all of the affected information is the subject of a data breach at another agency, and that agency is taking the actions required under the MDBN Scheme[93]

87 Bill, cl 33, proposed s 47(1) of the IP Act.
88 Bill, cl 33, proposed s 47(2) of the IP Act.
89 Bill, cl 33, proposed s 48(2) of the IP Act.
90 Bill, cl 33, proposed s 51 of the IP Act.
91 Bill, cl 33, proposed s 53 of the IP Act.
92 Bill, cl 33, proposed s 55 of the IP Act.
93 Bill, cl 33, proposed s 56 of the IP Act.

- if the agency acts to mitigate a data breach with the result that serious harm is not likely or (for breaches relating to data loss) there is no unauthorised access to or disclosure of personal information[94]
- if doing so would be inconsistent with a confidentiality provision in other state of federal legislation[95]
- if doing so would create a serious risk of harm to health or safety[96]
- if doing so would compromise the agency's cybersecurity or lead to further data breaches (the agency is required to review the application of this exemption on a monthly basis and to comply with the MDBN Scheme once the exemption no longer applies).[97]

Information Commissioner responsible for supporting compliance, enforcement of MDBN Scheme

The Bill proposes amending the IP Act to give the Information Commissioner a range of powers and responsibilities in relation to the MDBN Scheme.

The Bill proposes that the Information Commissioner be given the power to give direction to agencies to provide information about data breaches, where they reasonably suspect that an eligible data breach has occurred.[98]

The Bill provides for the Information Commissioner to appoint authorised officers to monitor and investigate compliance with the MDBN Scheme.[99] The Information Commissioner must issue authorised officers with identity cards,[100] which they must produce or display when exercising powers under the IP Act.[101]

The Bill proposes that authorised officers have a range of powers, including:

- a general power to enter places occupied by an agency (excluding a part of the place where a person resides), subject to written notice being given by the Information Commissioner[102]
- general powers to require a demonstration of data handling systems, inspect relevant documents and remain at a place they have entered[103]
- the power to require reasonable help to exercise another power.[104] Failure to comply with a requirement to help would be made an offence, subject to a penalty of up to 100 penalty units (currently $15,480).[105]

2.4.3 Extension of assessment period under the MDBN scheme

Proposed new s 49 (Extension of period for assessment by agency), to be inserted by cl 33, would allow an agency, satisfied that an assessment of a known or suspected eligible data breach will take

94 Bill, cl 33, proposed s 57 of the IP Act.
95 Bill, cl 33, proposed s 58 of the IP Act.
96 Bill, cl 33, proposed s 59 of the IP Act.
97 Bill, cl 33, proposed s 60 of the IP Act.
98 Bill, cl 33, proposed s 61 of the IP Act.
99 Bill, cl 33, proposed ss 62 and 63 of the IP Act.
100 Bill, cl 33, proposed s 64 of the IP Act.
101 Bill, cl 33, proposed s 65 of the IP Act.
102 Bill, cl 33, proposed ss 67 and 68 of the IP Act.
103 Bill, cl 33, proposed s 69 of the IP Act.
104 Bill, cl 33, proposed s 70 of the IP Act.
105 Bill, cl 33, proposed s 71 of the IP Act.

longer than 30 days, to extend indefinitely the period within which the assessment must be completed.[106]

Institution of Parliament

Authorising the amendment of an Act only by another Act – extension of assessment period under the MDBN scheme

A Bill should only authorise the amendment of an Act by another Act.[107] Generally, a clause which enables an Act to be expressly or impliedly amended by subordinate legislation or executive action is inconsistent with the fundamental legislative principle that legislation should have sufficient regard for the institution of Parliament.[108]

Here, the Bill contains a clause that allows an agency to modify a statutory time period for completing an assessment.[109] Proposed s 48 of the IP Act contains the obligations on agencies in relation to data breaches. If an agency does not know whether a data breach is an eligible data breach of the agency, it must conduct an assessment as to whether there are reasonable grounds to believe the data breach is an eligible data breach of the agency.[110]

Proposed s 48(3) of the IP Act would require that such assessments be completed within 30 days.[111] However, proposed s 49 would allow an agency to extend the 30 day time period unilaterally, for an indefinite period of time. The agency must be 'satisfied the assessment cannot reasonably be completed within the 30 day period'[112] and must provide notice to the Information Commissioner of the extension period[113] (though an agency is not required to apply to the Information Commissioner for the extension).

Whilst the Information Commissioner may ask the agency to provide further information,[114] there does not appear to be any limit on the length of an extension period.

Regarding the justification for the provision, the explanatory notes state:

> The amendment is justified on the basis that it is needed to provide sufficient flexibility to allow agencies to undertake a fulsome assessment of a data breach, and acknowledging that there may be significantly complex matters involved leading to an agency being best placed to determine how long an assessment may take if not possible to achieve within 30 days taking into consideration factors including resourcing.[115]

Whilst it is not generally acceptable for an agency or department to moderate the application of a particular provision of an Act, the committee notes that proposed s 49 relates specifically to an extension of time in particular circumstances.[116] The committee also notes that an agency must be satisfied that an assessment cannot be 'reasonably completed' within the 30 days, providing some threshold before an extension can be made. Presumably, the Information Commissioner can also make inquiries in this regard.

106 Bill, cl 33 inserts IP Act, ss 48, 49.
107 LSA, s 4(4)(c).
108 OQPC, Notebook, p 159.
109 Bill, cl 33, inserts IP Act, s 49.
110 Under new s 48(2)(b) of the IP Act.
111 Under new s 48(3) of the IP Act.
112 Under new s 49(1) of the IP Act.
113 Under new s 49(3) of the IP Act.
114 Under new s 49(4) of the IP Act.
115 Explanatory notes, p 14.
116 OQPC, Notebook, p 160.

Concerns raised by the OIC

The OIC in its submission raised concerns about proposed s 49, noting that 'undue delay in assessment and notification can impact the effectiveness of a data breach reporting scheme.[117]

The OIC recommend that this provision incorporate a limitation that any extension only be for an amount of time reasonably required for the assessment to be conducted, as is the case in the NSW MDBN scheme.[118]

Committee comment

Whilst proposed section 49 of the IP Act is inconsistent with the fundamental legislative principle that legislation has sufficient regard for the institution of Parliament, the committee considers the inconsistency to be justified in the circumstances, given the limited scope of the provision and the ability of the Information Commissioner to have some oversight of the extension process.

The committee agrees, however, with the OIC that proposed s 49 in cl 33 should be amended to require that any extension of time must be only for an amount of time reasonably required for the assessment to be conducted, as is required in the equivalent provision of the NSW MDBN scheme.

Recommendation 2

The committee unanimously recommends that the proposed new section 49 in clause 33 be amended to require that any extension of time must be only for an amount of time reasonably required for the assessment to be conducted.

2.4.4 Resourcing impacts of the MDBN Scheme

The Bill's provisions for the establishment of a MDBN scheme would likely have substantial resourcing impacts on the OIC, which would have oversight of the scheme.

The explanatory note state that the OIC 'has been allocated $11.465 million over four years, and $2.563 million ongoing, through the State Budget 2023-24 for operational implementation, development of an ICT solution and training and awareness activities.'[119]

The Bill would also have resourcing impacts on agencies that would be subject to the scheme, including local councils and universities. According to the explanatory notes, these costs will be absorbed by those agencies.[120]

Concerns raised by the LGAQ

In its submission, the LGAQ noted that Queensland councils are currently subject to a voluntary notification scheme which it describes as 'workable for local Government due to the decentralised nature of the State and the financial and workforce challenges that most of the State's councils face'.[121] LGAQ also noted that the vast majority of councils do not have budget nor the workforce experience to implement and maintain requirements for the MDBN scheme, and that a mandatory MDBN scheme in local government would likely struggle to be successful if it resulted in undue burdens on the operations of councils.[122]

117 Submission 3, p 2.

118 See s 59K of the *Privacy Information Protection Act 1998* (NSW).

119 Explanatory notes, p 6.

120 Explanatory notes, p 6.

121 Submission 4, p 7.

122 Submission 4, p 7.

The LGAQ recommended:

- the introduction of a MDBN scheme be carefully considered in the local government context, including the limited resources available to councils, and steps taken to ensure that establishment would include facilitation funding for councils[123]
- that State and federal governments develop and resource an expert Security Operations Centre for local government authorities as a shared service concept[124]
- financial assistance and training support be provided, and the introduction of such a scheme be phased in with a grace period[125]
- realistic reporting timeframes should also be set, and review period built in, to ascertain whether a MDBN scheme is workable in the local government context[126]
- councils should continue to be subject to a voluntary notification scheme, as is currently the case, or that local government be given an exemption under the new MDBN scheme (which could be achieved through a waiver or modification).[127]

In response, the department advised:

- Consistent with its statutory role, it is anticipated the OIC will provide training (locally and regionally, online and in person) about the new obligations and requirements. OIC will similarly prepare guidelines and templates for agencies to draw from. Resourcing has been provided to the OIC for this purpose to ameliorate the impact.
- It is currently anticipated that the MDBN scheme would commence for agencies on 1 July 2025, by proclamation. The Bill provides a 12-month delay to commence the MDBN scheme for local government. This would provide a longer period for local governments to transition to the new MDBN scheme and mitigate the immediate resourcing impact of needing to implement the new single set of privacy principles and the MDBN scheme at the same time. [128]

Further issues raised by the OIC

The OIC submission raised a number of further issues and recommendations regarding the provisions of the Bill for the proposed MDBN scheme. These issues, and the department's advice are discussed below.

2.4.5 Obligations of agencies in relation to data breaches

The OIC noted that the obligation in new s 48(2)(a) of the IP Act may overlap with the obligations in new s 48(4)(a).[129]

The OIC recommended that the requirements in new s 48(4) be moved into new section 48(2)(a), noting that the obligations to contain and mitigate a data breach are important requirements in the scheme, both where an agency is aware a breach is an eligible data breach, and where an agency suspects a data breach to be an eligible data breach.[130]

The department advised it is considering the issues raised relating to moving proposed new s 48(4).

123 Submission 4, p 7.
124 Submission 4, p 7.
125 Submission 4, p 8.
126 Submission 4, p 8.
127 Submission 4, p 8.
128 Department of Justice and Attorney-General, Correspondence, 10 November 2023, p 11.
129 Submission 3, p 2.
130 Submission 3, p 2.

2.4.6 Agencies must notify particular individuals

The OIC noted that new s 53 of the IP Act provides that an agency must, as soon as practicable, notify each individual whose personal information has been accessed, disclosed or lost if it is reasonably practicable to do so, and if this does not apply, to notify each affected individual, and that these subsections appear to relate to the same individuals.[131]

The OIC recommended that new s 53(1)(b) instead refer to individuals likely to be affected by the data breach, aligning with the distinction made in new s 51(2)(e)(i), and with other similar breach reporting schemes which extend to individuals '*at risk from the eligible data breach*'.[132]

The department advised that it is considering a clarification of the issue identified with new s 53, including clarification of the terminology in s 51(2)(e) and s 53(1)(a).

2.4.7 Power to access/inspect systems via electronic means

The OIC queried whether a power to access/inspect systems via electronic means should also be contemplated to permit 'remote access' by OIC to a system, without first requiring physical entry.[133]

The department advised that it is considering the need for OIC to have remote access to systems as part of proposed entry and inspection powers to assess an agency's data handling procedures and systems.

2.4.8 Power to make a record/or take copies of information

The OIC recommended that a power to make a record and/or take copies of information the subject of the inspection would assist investigations.[134]

The department advised that:

- The *Privacy and Personal Information Protection Amendment Act 2022* (NSW) includes an entry and inspection power similar to the power included in the Bill and does not include a power to take copies or make records.
- The proposed entry and inspection powers are intended to be consistent with FLPs as far as possible. To ensure consistency with FLPs, powers that may be exercised on entry of premises, must be specified as far as practical and justifiable in proportion to the interference in rights and liberties involved.
- The entry and inspection powers in the Bill have been limited in scope to ensure the FLP departures are justified on the basis that, in viewing the systems and practices, the OIC would gain practical insights and understanding that they would not otherwise be able to obtain through the use of other existing powers.
- The policy intent of the Bill, in not providing the ability for the OIC to record or take copies of documents, is to ensure that documents are not inappropriately provided to the OIC, for example, if they contain personal information, confidential or privileged information.
- The power under s 197 of the IP Act, as amended by the Bill, will allow the Information Commissioner to require that a person to give information in written form, if the Information Commissioner is satisfied on reasonable grounds that the person has information relevant to a stated review, investigation, audits, preliminary inquiries of a respondent for a privacy

131 Submission 3, p 3.

132 Submission 3, p 3.

133 Submission 3, p 2.

134 Submission 3, p 2.

complaint, or a decision of the Information Commissioner whether to give a compliance notice or a mediation of a privacy complaint.

2.5 Powers of the Information Commissioner

The OIC submission raised a number of issues about the powers of the Information Commissioner, and opportunities to clarify or strengthen them.

2.5.1 Functions of the Information Commissioner

The OIC recommended that the statement of the Commissioner's functions in s 135(b)(i) of the IP Act include a reference to chapter 3A, as it currently only references compliance with the privacy principles, as this would assist the OIC to exchange information relating to data breaches with other entities under s 199.[135]

The department advised it is considering whether the functions of the Information Commissioner in s 135(1)(a)(i) could be made clearer to encapsulate the MDBN related functions.

2.5.2 Compliance notices

The OIC recommended extending the Information Commissioner's new power under new s 158(3) to issue compliance notices to the entirety of Chapter 3A, which will enable the Information Commissioner to rectify serious, flagrant or repeated failures by an agency under the MDBN scheme as a whole (including to require compliance with a direction to give a statement under new s 61 of the IP Act).[136]

In response, the department advised that cl 41 amends s 158 of the IP Act to allow the Information Commissioner to give a relevant entity a compliance notice if the Commissioner is satisfied on reasonable grounds that the entity has done an act or engaged in a practice in contravention of a relevant obligation. New s 158(3) defines a relevant obligation to include not only chapter 3A, part 2 or 3, but a direction given to the agency under s 61(2) and ss 72 and 73.

2.5.3 Preliminary inquiries related to an investigation

The OIC recommended that the Information Commissioner be enabled to make inquiries of any person in the course of overseeing the administration of the scheme generally, and not only where the Information Commissioner may be contemplating investigation.

In response, the department advised that the provision is a non-coercive enabling provision and there would be nothing to prevent the OIC from making inquiries of agencies related to its administration of the scheme generally as part of performing its functions under s 135.

The provision is included specifically in relation to investigation powers to make it clear that the threshold specified in s 135(a)(ii) does not need to be satisfied in advance of such preliminary inquiries relevant to a potential investigation being made.

The OIC also recommended that consideration be given to replicating s 106 of the RTI Act to make it clear that no legal impediments constrain persons from disclosing information to the Information Commissioner for the purposes of the Commissioner's functions under the IP Act.

2.5.4 Power of Information Commissioner to require information or attendance

The OIC recommends that the power to require information or attendance also be extended to compliance with the obligations in new Chapter 3A generally, to enable information gathering in the

[135] Submission 3, p 3.

[136] Submission 3, p 3.

context of the administration of the MDBN scheme as a whole, and not only in the context of investigations.

In response, the department advised that cl 71 of the Bill amends s 197 of the IP Act to allow the Information Commissioner to compel information or attendance of any person where the Information Commissioner is satisfied on reasonable grounds that the person has information relevant to:

- a review into personal information handling practices under s 135(1)(a)(i);
- an investigation of an act done or practice engaged in by a relevant entity in relation to personal information under s 135(1)(a)(ii) - this a contravention of the entity's obligations under chapter 3A;
- an audit under s 135(1)(b)(iii) – this relates to compliance with the Act generally including Chapter 3A;
- preliminary inquiries the commissioner is making of the respondent for a privacy complaint – this may be about an act or practice that may be breach of an agency's obligations to comply with chapter 3A, part 2 or 3;
- a decision of the commissioner whether to give an agency a compliance notice under chapter 4 – this may relate to an obligation to comply with chapter 3A, part 2 or 3, a direction under s 61(2) or ss 72 or 73.
- the mediation of a privacy complaint under chapter 5 – this may be about an act or practice that may be breach of an agency's obligations to comply with chapter 3A, part 2 or 3.

This provides a broad and reasonable basis for compelling information and attendance. As indicated above, the department will give further consideration to this issue.[137]

In regard to the OIC's recommendation that s 106 of the RTU be replicated in the IP Act, the department advised that s 106 of the RTI provides that:

- no obligation to maintain secrecy or other restriction on the disclosure of information, whether imposed under an Act or a rule of law, applies to the disclosure of information to the Information Commissioner;
- legal professional privilege does not apply to the production of documents or the giving of evidence.
- such provisions are only appropriate in the context of external reviews to ensure that the external review body is able to stand in the shoes of the original decision maker and make the decision afresh. The approach in the RTI Act is consistent with the approach in s 21(6) of the *Queensland Civil and Administrative Tribunal Act 2009* (QCAT Act) in relation to external reviews generally conducted by QCAT.
- the OIC has very different functions under the IP Act compared to the RTI Act. For example, under the IP Act the OIC can undertake investigations and inquiries, they can mediate privacy complaints and can oversee and manage the MDBN scheme and issue compliance notices. It is important that secrecy, confidentiality, and privilege are maintained. Displacing these important rules are not commensurate with the nature of the Information Commissioner's functions and powers under the IP Act.138

[137] Department of Justice and Attorney-General, Correspondence, 10 November 2023, pp 17-19.

[138] Department of Justice and Attorney-General, Correspondence, 10 November 2023, pp 19-20.

2.6 Misuse of restricted computers

Misuse of confidential information has been a longstanding issue in the Queensland public sector.

Clause 4 proposes to amend s 408E of the Criminal Code to clarify the type of conduct captured by the offence, reclassify the offence as a misdemeanour, and increase the maximum penalty from 2 to 3 years imprisonment.

Public servants have access to a range of information and have obligations to manage confidential information in accordance with ethical obligations, security standards and relevant legislation. These responsibilities protect the rights of the people whose information is held and promote community trust, and inappropriate access to information can lead to harm for both individuals and the agency.[139]

According to the Crime and Corruption Commission (CCC), the misuse of confidential information – either through unauthorised access and/or unauthorised disclosure – has been a 'longstanding issue in the Queensland public sector', and 'can be a key enabler of other types of corrupt conduct'.[140]

In its report, *Operation Impala, A report on misuse of confidential information in the Queensland public sector* (Impala Report), the CCC reported 1,060 allegations made in 2018-19 relating to misuse of confidential information across the public sector, an increase of almost 50 per cent over a three-year period. These 1,060 allegations of misuse of confidential information in 2018-19 represented 13 per cent of all allegations of corrupt conduct received by the CCC that year.[141]

According to the explanatory notes, the proposed amendments are designed to address concerns raised by the CCC in its Impala Report that the current penalties 'do not adequately reflect the serious nature of deliberate breaches of the public's privacy by public officers'.[142]

The Bill proposes at cl 4 to amend the Criminal Code to increase the maximum penalty for the simpliciter offence[143] of misuse of a restricted computer from 2 years imprisonment to 3 years imprisonment, and reclassify the offence as a misdemeanour (which is an indictable offence[144]).[145] The proposed amendments to the offence of 'computer hacking and misuse' (Criminal Code, s 408E) incorporate some aspects of the relevant recommendation.[146] However it does not introduce a new offence of 'misuse of confidential information by public officers' as proposed in Recommendation 10 of the Impala Report.

The department's written brief explained, 'consultation on the new offence proposed by the Impala Report in the Public Consultation Paper was divided, with no clear support for the proposed new

139 Explanatory notes, p 5.

140 Impala Report, p 26.

141 Impala Report, p 26.

142 Explanatory notes, p 4.

143 'Simpliciter' refers to the basic version of an offence, with no circumstance of aggravation.

144 An 'indictable offence' (as distinct from a simple offence) is a criminal offence which must generally be prosecuted on an indictment (a written charge by a person authorised to prosecute criminal offences) before a judge and jury in the District or Supreme Court. Crimes and misdemeanours are indictable offences.

145 Bill, cl 4 amends Criminal Code, s 408E. The existing offence provides that a person who uses a 'restricted computer' without the consent of the computer's 'controller' commits an offence (s 408E(1)). The existing offence includes circumstances of aggravation, providing that: if the person causes or intends to cause 'detriment' or 'damage', or gains or intends to gain a 'benefit', they commit a crime and are liable to imprisonment for 5 years (s 408E(2)); and if the person 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, the person commits a crime and is liable to imprisonment for 10 years (s 408E(3)). It is a defence to a charge under this section to prove that the use of the restricted computer was authorised, justified or excused by law (s 408E(4)).

146 Bill, cls 3-5.

offence.'[147] As a result, the Bill proposes amending s 408E of the Criminal Code 'to improve its operation and clarity having regard to the underlying issues forming the basis of the recommendation in the Impala Report.' [148]

Clause 4 engages s 29 of the HRA which provides for the right to liberty and security of person.[149] The Bill limits the right to liberty and security of person in s 29 of the HRA by changing the offence in s 408E of the Criminal Code from a simple offence to a misdemeanour and increasing the maximum penalty from 2 to 3 years imprisonment. This exposes perpetrators of this offence to lengthier imprisonment terms.

The statement of compatibility states that the maximum sentence for an offence is a reflection of its seriousness, and that increasing penalties for an offence is a suitable way of showing that the offence is considered to be more serious.[150] Therefore, it argued, limiting the right to liberty and security of person by increasing the maximum penalty will more appropriately reflect the seriousness of the offence and the harm caused by this type of offending and will send a message to offenders and the community that this conduct is viewed seriously and is not acceptable.[151]

Rights and liberties of individuals

General Rights and liberties – penalties

Clause 4 also raises a potential FLP issue.

Consequences imposed by legislation should be relevant and proportionate. In line with this, a penalty should be proportionate to the offence, and penalties within legislation should be consistent with each other.[45]

The explanatory notes seek to justify the increased maximum penalty on 'the demonstrated need for deterrence and to meet community expectations'.[48] As regards the Bill's reclassification of the offence, the explanatory notes contend that 'there will no longer be a time limit on commencing a prosecution'.[49] In that regard, the explanatory notes observe that the Impala Report highlighted that one of the challenges in applying s 408E of the Criminal Code is that, in some cases, charging under the offence becomes statute barred:

> Examination of the manner in which the subject agencies dealt with instances of staff misusing information has led the CCC to conclude that there are delays, often lengthy, in agencies taking action, and further delay when the matter is referred to the QPS. Moreover, the QPS may hold off on charging if there is a concurrent investigation in relation to the public officer for a more serious offence, noting that this type of corruption is often paired with more serious corruption.[152]

The explanatory notes advise that the classification of this offence as a misdemeanour is consistent with the approach taken for other similar Criminal Code offences used to prosecute corruption and abuse of office (see Chapter 13 of the Criminal Code).[51]

In advice to the committee, the department further explained that the Impala Report referred to the importance of general deterrence when sentencing for an offence under s 408E by reference to the commentary contained in Carter's Criminal Law of Queensland.[153] This commentary refers to the case of *R v Stevens* [1999] as an appeal against sentence under a similar provision of the *Crimes Act 1914* (Cth) and the remarks of Studdert J that:

147 Department of Justice and Attorney-General, Briefing paper, 19 October 2023, p 12.

148 Department of Justice and Attorney-General, Briefing paper, 19 October 2023, p 12.

149 HRA, s 29.

150 Statement of compatibility, p 5.

151 Statement of compatibility, p 5.

152 Impala Report, p 105.

153 Impala Report, p 108.

> Computer technology plays an important role in modern society. The potential for harm by computer abuse of the type that occurred in this case, in a society that is becoming increasingly dependent upon computers, requires that considerations of deterrence, not only of the offender but of others who might be tempted to offend in a similar way, should be adequately reflected when it comes to sentence.[154]

The department also explained that the overarching purpose for the amendments is to address concerns about the inadequacy of the current penalty as highlighted in the Impala Report.[155] The increase in penalty sends a clear message to the community about the seriousness with which Parliament views this kind of offending.[156]

Noting the CCC's views, as expressed in the Impala Report, and that the Criminal Code includes a considerable range of offences, including those with maximum penalties attracting periods of imprisonment (many greater than the penalty proposed by the Bill), it appears that, in increasing the maximum penalty for the simpliciter offence (the circumstances of aggravation remain unaffected), the proposed provision is generally proportionate to the offence and the seriousness of the relevant conduct, and that the proposed consequences are relevant to the offending conduct.

Additionally, as per the advice in the explanatory notes, reclassifying the offence appears consistent with the approach taken for comparable existing offences.

Despite the points made in the explanatory notes, the proposed amendments will have a direct impact on the rights and liberties of offenders, with the increased penalty potentially increasing a term of imprisonment, and the reclassification of the offence meaning it is treated more seriously and that commencement of a prosecution is no longer limited by time.

Committee comment

The committee notes the important work of the Crime and Corruption Commission (CCC) in its Impala Report to highlight the growing incidences of misuse of confidential information in the Queensland public sector, and that these incidents can be a key enabler of other types of corrupt conduct.

The committee also notes the intent of the provisions proposed in cl 4 to amend the Criminal Code to increase the seriousness of the offence of misuse of a restricted computer, as well as increase the maximum penalty that applies. The committee considers the impact on the right to liberty and security of those who would commit such crimes is reasonable given the significance risks posed by misuse of confidential information, and the growing incidence of such matters being brought to the attention of the CCC. The committee also accepts that the proposed changes to the offence will help to deter would-be offenders.

The committee also considers the proposed amendments to be appropriate and reasonable in the circumstances, and have sufficient regard to fundamental legislative principles.

154 *R v Stevens* [1999] NSWCCA 69, [54].

155 Impala Report, pp 105, 107-9.

156 Department of Justice and Attorney-General, Correspondence, 20 November 2023, p 6.

2.7 Proactive release of Cabinet documents

The Bill proposes three changes to the RTI Act to facilitate the introduction of the proactive release scheme. The Queensland scheme proposed in the Bill would be the first of its kind in Australia.

2.7.1 How the proactive release scheme would work

The Coaldrake Report recommended that Cabinet submissions (and their attachments), agendas, and decisions papers be proactively released and published online within 30 business days of such decisions.[157] This is known as the 'proactive release scheme'.

The explanatory notes state that this administrative scheme, modelled on the equivalent New Zealand scheme, will be implemented via an amendment to the Cabinet Handbook. As such, legislation is not required to enable the scheme.[158] This mirrors the approach taken in New Zealand, where the scheme was implemented via a Cabinet circular.[159]

The department advised the committee that the intention of the proactive release policy is to publicly release cabinet submissions, attachments to submissions and cabinet decisions within 30 business days of a cabinet decision being made.[160]

Changes proposed to facilitate the proactive release scheme

The Bill proposes three changes the RTI Act to facilitate the introduction of the proactive release scheme. These amendments:

- provide clarity for applicants and decision makers under the RTI Act concerning the exempt status of information in Cabinet submissions and Cabinet decisions, and other Cabinet related documents, in view of the official publishing of information by decision of Cabinet under the proactive release scheme;
- provide protection from civil liability for Ministers disclosing information under a publication scheme or other administrative scheme in good faith; and
- ensure that the public interest immunity in proceedings and processes is not altered by the publication of information by Cabinet, or decisions by Cabinet to officially publish Cabinet information.[161]

Proactive release to be disregarded when assessing whether disclosures are in the public interest

The Bill proposes that courts and investigatory bodies be required to disregard the proactive release scheme when deciding whether or not a common law of statutory provision prevents the production or disclosure of information connected to Cabinet because it would be contrary to the public interest.[162] In other words, the Bill proposes to maintain the 'status quo' in relation to public interest immunity, despite the introduction of the proactive release of cabinet documents.[163]

The Statement of Compatibility explains that this amendment 'arises from observations on the operation of New Zealand's proactive release scheme, where the existence of a proactive release

157 This was Recommendation 2 of the Coaldrake Report.

158 Explanatory note, p 2.

159 Department of Justice and Attorney-General, Briefing paper, 19 October 2023, p 23.

160 Department of Justice and Attorney-General, Briefing paper, 19 October 2023, p 23.

161 Department of Justice and Attorney-General, Briefing paper, 19 October 2023, p 24.

162 Bill, cl 87.

163 Statement of compatibility, p 19.

scheme has led courts to place less weight on Cabinet confidentiality in considering public interest immunity'.[164]

Ministers granted immunity from civil liability

As part of the proposed proactive release scheme, Ministers would be granted immunity from civil liability arising from the disclosure of information under publication schemes[165] or other administrative schemes where they have acted in good faith. Any civil liability would, instead, attach to the State.[166] The Bill give as examples of disclosing information:

- publishing information on a department's website
- official publication by decision of Cabinet of information contained in a Cabinet document.[167]

The explanatory notes state that the granting of immunity is required to protect Ministers from the risk of civil liability that arises as a result of the proactive release of Cabinet documents. They assert that the approach taken in the Bill is consistent with the protection given to employees of public sector entities under the *Public* Sector *Act 2022.*

The immunity from civil liability proposed in the Act appears to be very broad – it will apply in relation to all publication schemes and administrative schemes, not just the proactive release of Cabinet documents. The explanatory notes do not explain why such a broad immunity is necessary. However, the department advised the committee in a briefing paper, that:

> The RTI Act already contains certain protections from civil liability for 'relevant entities'. In addition, such protections are afforded to 'prescribed persons' within the *Public Sector Act 2002* in relation to the civil liability of engaging in conduct in an official capacity.
>
> The proposed amendments are not dissimilar to these existing protections and afford the same reasonable and appropriate protection from civil liability to Ministers who disclose information under the proactive release scheme in good faith.[168]

Redacted information to remain exempt

The Bill proposes that Schedule 3 (Exempt Information) of the RTI Act be amended to 'ensure that the publication of documents under a proactive release scheme does not alter the exempt status of redacted information and of other Cabinet-related documents currently taken to be comprised exclusively of exempt information under the RTI Act.'[169]

2.7.2 Implementation of the proactive release scheme

The explanatory notes advise that:

> to the extent that cost implications can be ascertained, an initial $10.137 million over four years was allocated through the State Budget 2023-24 for whole-of-government implementation of the proactive release scheme. This funding includes $6.073 million for the Department of the Premier and Cabinet to manage and coordinate the scheme across government, to manage implementation of ICT systems to support proactive release and for seven additional FTE [positions] to support the proactive release scheme. It also includes $4.064 million over four years for the Department of Justice and Attorney-General to implement the proactive release scheme within its agency.[170]

---

164 Statement of compatibility, p 19.

165 Section 21 of the RTI Act requires agencies to publish a scheme setting out the classes of information they have available and the terms in which they will make the information available, including any charges.

166 Bill, cl 89.

167 Bill, cl 89.

168 Department of Justice and Attorney-General, Briefing paper, 19 October 2023, p 24.

169 Bill, cl 136; Explanatory notes, p 2.

170 Explanatory notes, p 6.

The explanatory notes also advise that the proactive release scheme would be kept under review, and any additional costs identified would be brought to the Cabinet Budget Review Committee for further consideration.[171]

Committee comment

The committee welcomes the provisions of the Bill to support the introduction of the proposed proactive release scheme for Cabinet documents.

2.8 Waivers of obligations

Clause 40 of the Bill expands on a provision in the IP Act[172] to allow a relevant entity to apply to the Information Commissioner for an approval that waives or modifies an obligation of the entity to comply with:

- the privacy principle requirements, or
- for an agency, provisions relating to the assessment of suspected eligible data breaches,[173] notifying eligible data breaches,[174] keeping a register[175] and publishing a data breach policy.[176]

Institution of Parliament

Delegation of legislative power – waiver of obligations

A Bill should allow the delegation of legislative power only in appropriate cases and to appropriate persons[177] and should be subject to parliamentary scrutiny.[178]

Here, the Information Commissioner may waive or modify the requirements of legislation as it applies to a relevant entity which is a delegation of legislative power.

The Information Commissioner may only grant an approval if the commissioner is satisfied that the public interest in the relevant entity's compliance with the obligation is outweighed by the public interest in waiving or modifying the entity's compliance with the obligation.[179]

The explanatory notes justify this provision on the basis that 'it is necessary to provide flexibility in balancing the interests of protection of individual personal information against other emerging public interests',[180] though it is not clear what would constitute an emerging public interest in this regard.

However, the current requirements in s 157 of the IP Act will apply to any approval, meaning that approvals must be made by gazette notice and will be subject to the tabling and disallowance provisions of the *Statutory Instruments Act 1992* (SI Act) providing a safeguard in this respect.

Committee comment

Whilst the provision providing for a modification or waiver of statutory requirements does involve a delegation of legislative power, the committee considers it appropriate in light of the safeguards

171 Explanatory notes, p 6.
172 Bill, cl 40 amends IP Act, s 157.
173 Under proposed chapter 3A, part 2 of the IP Act.
174 Under proposed chapter 3A, part 3 of the IP Act.
175 Under proposed s 72 of the IP Act.
176 Under proposed s 73 of the IP Act.
177 LSA, s 4(4)(a).
178 LSA, s 4(4)(b).
179 IP Act, proposed s 157(4).
180 Explanatory notes, p 14.

provided for in s 157 of the IP Act, such that the provision has sufficient regard for the institution of Parliament.

2.9 Corporations legislation displacement

The Bill includes provisions[181] which allow for regulations to declare a provision of the IP Act or RTI Act that apply in relation to a prescribed corporation[182] to be a 'Corporations legislation displacement provision' for the purposes of the *Corporations Act 2001* (Cth) (Corporations Act).[183]

The effect of declaring a Corporations legislation displacement provision is that the whole of the Corporations legislation or a particular provision of the Corporations legislation does not apply to the extent that there would otherwise be an inconsistency between the Corporations legislation and the state law.[184]

Institution of Parliament

Delegation of legislative power

A Bill should allow the delegation of legislative power only in appropriate cases and to appropriate persons[185] and should be subject to parliamentary scrutiny.[186]

Issues of fundamental legislative principle arise here because it is a regulation, rather than an Act of Parliament, that may declare certain provisions of the IP Act or RTI Act to be Corporations legislation displacement provisions. Regulations may also declare to whom (eg all prescribed corporations or a particular prescribed corporations) a displacement provision would apply.[187]

The explanatory notes argue that the amendments are justified on the basis that they are necessary to provide flexibility to ensure that if a corporation is prescribed in the future to be a public authority under the RTI Act or IP Act, consideration can be given at that time to provisions of the Corporations legislation which should be displaced to give effect to provisions in the Act.[188]

Aside from the need for flexibility in dealing with future public authorities, it is not clear from the explanatory notes in what circumstances these provisions will be used.

There will, however, be parliamentary scrutiny through the tabling and disallowance provisions of the SI Act that will apply to regulations making these declarations.[189] Further, it is recognised that the intent of any declarations is to give effect to the state law over the Corporations legislation, to the extent of any inconsistency.

Committee comment

The committee is satisfied that the delegation of legislative power to allow for regulations to declare Corporations legislation displacement provisions, and the public authorities they apply to, is reasonable in the circumstances which have been described above.

181 Bill, cl 72 inserts IP Act, s 199A; Bill, cl 134, inserts RTI Act, s 191A.

182 Prescribed corporation means a corporation within the meaning of the Corporations Act that is declared under s 21(1)(c) of the IP Act or s 16A of the RTI Act to be a public authority for those Acts.

183 See Corporations Act, s 5G.

184 See explanatory notes, p 15; Corporations Act, s 5G.

185 LSA, s 4(4)(a).

186 LSA, s 4(4)(b).

187 Bill, cl 72 inserts IP Act, s 199A; Bill, cl 134 inserts RTI Act, s 191A.

188 Explanatory notes, p 15.

189 SI Act, ss 49-50.

The committee also notes that the tabling and disallowance provisions for regulations making these declarations would provide opportunities for their parliamentary scrutiny.

2.10 Exclusion of letters patent entities from 'public authority' definition

Clauses 19 and 84 of the Bill would amend the definition of 'public authority' under the IP Act and the RTI Act to exclude an entity established by letters patent. The effect of this amendment would be that entities established by letters patent would not be subject to obligations under either Act.

The proposed amendments would limit freedom of expression (s 21 of the HRA), by precluding access and amendment applications being made to such entities under the RTI Act, and would mean that the privacy protections under the IP Act would not apply to personal information held by such entities, limiting the right to privacy and reputation (s 25 of the HRA).

Entities established by letters patent are generally charitable and religious organisations such as Bible Societies, Churches, Church Trusts, Kindergarten Associations, Welfare Associations and Historical Associations.[190] However, the QHRC submits that an orphanage may also be established by letters patent, and notes a 2017 finding by QCAT that an orphanage, established by letters patent in 1929 issued by the Governor, was a 'public authority' under the existing definition of the RTI Act (the Stanway case).[191]

According to the statement of compatibility, the purpose of the limitation on the right to freedom of expression is to provide consistency with the purposes of the RTI Act (which is for a right of access to information in the government's possession or under the government's control), and to alleviate the administrative burden on entities established by letters patent in complying with RTI Act obligations. These obligations include dealing with access applications, publishing disclosure logs and maintaining publication schemes.[192]

The purpose of the limitation to the right to privacy and reputation is to provide consistency with the purposes of the IP Act (which is to provide for the fair collection and handling in the public sector environment of personal information) and to alleviate the administrative burden on entities established by letters patent in complying with the IP Act. These obligations include complying with the privacy principles under the IP Act and, will, subject to passage of the Bill, include requirements to comply with the MDBN scheme.[193] The statement of compatibility also advised:

- The limitation imposed by the Bill supports the purpose of ensuring the consistency with the purposes of the RTI Act and IP Act by ensuring that rights of access and information privacy protections are limited to government information rather than extending to entities established by letters patent (generally having religious or charitable purposes). The limitation also supports the purpose of alleviating the administrative burden of such entities by excluding them from the scope of requirements in the Acts
- There are no less restrictive reasonably available ways to achieve the purpose of the Bill. Options such as providing that organisations established by letters patent are subject to the RTI Act in relation to specified functions only, would not achieve the purpose of the limitation.
- The proposed amendments strike the right balance between the rights to freedom of expression and privacy and the need for reasonable limitations on the operation of RTI and IP legislation. Clarifying the operation of the RTI Act and IP Act is consistent with a free and democratic society.

190 Statement of Compatibility, p 9.

191 *Stanway v Information Commissioner & Anor* [2017] QCATA 30.

192 Statement of compatibility, p 9.

193 Statement of compatibility, p 9.

- It appears that, other than in the Stanway case referred to above, applications under the RTI Act and IP Act have not been made to organisations established by letters patent. These rights have therefore rarely been exercised.

Concerns raised by the QHRC

The QHRC submission further notes that missions and dormitories were often established by religious organisations that may be Queensland entities established by letters patent, and that these entities may hold significant personal and cultural information about First Nations peoples.[194] In fact, the committee noted at its public hearing these entities may hold significant personal and cultural information about all Queenslanders.

The QHRC argued that proposed amendments in the Bill (cls 19 and 84) would have the potential to impact how information relating to Aboriginal people and Torres Strait Islander people is protected, managed and disclosed, which engages rights to freedom of expression (s 21), rights to privacy and reputation (s 25), and the cultural rights of Aboriginal peoples and Torres Strait islander peoples (s 28) protected by the HRA.

The QHRC argues that consideration should be given to any impact the proposed amendment to the definitions in the IP Act and RTI Act might have on the rights and entitlements of First Nations People in respect of their data, and on truth-telling and treaty processes.[195]

The QHRC further submits that this issue 'should be investigated to ensure respect and protection of the cultural rights of Aboriginal peoples and Torres Strait Islander peoples'. [196]

In response, the department advised:

- It notes the issues raised and will give further consideration to the issue.
- The purpose of the RTI Act is to provide a right of access to information in the government's possession or the government's control. While letters patent organisations are established by the Governor in Council, it understands that those entities were not intended to be captured by the RTI framework. The Bill excludes letters patent organisations as public authorities under the RTI Act and IP Act, consistent with a recommendation made by the Information Commissioner in response to matters raised in the Stanway case. It would be open to those entities to provide voluntary access to any records they may hold to assist with the Path to Treaty and truth telling inquiry.[197]
- The *Path to Treaty Act 2023* provides that the Truth Telling and Healing Inquiry has limited compulsion powers directed towards the participation of and production of information or documents from government agencies only. This model intends to encourage voluntary participation and sharing of histories, stories, experiences and truths from Aboriginal and Torres Strait Islander peoples and non-Indigenous Queenslanders alike.[198]

Committee comment

The committee notes the worthy intentions of the proposed amendments to exclude entities established by letters patent from the definition of 'public authority', though, remains concerned that the amendments could have wider, and as yet unknown, implications than the department has envisaged in its development of the Bill. The committee would like confirmation that:

194 Submission 6, p 2.

195 Submission 6, p 2.

196 Submission 6, p 4

197 Department of Justice and Attorney-General, Correspondence, 10 November 2023, p 28.

198 Department of Justice and Attorney-General, Correspondence, 10 November 2023, p 28.

- the proposed amendment to the definitions in the IP Act and RTI Act would not impact on the rights and entitlements of First Nations People and other Queenslanders in respect of their ability to access personal and family data that may be held by institutions owned by Queensland entities established by letters patent, and on truth-telling and treaty processes; and
- there are no alternative, less restrictive and reasonably available ways to achieve the same purpose as the proposed amendments at clauses 19 and 84.

Recommendation 3

That the Attorney-General **clarify** whether:

- the proposed amendment to the definitions in the IP Act and RTI Act would impact on the rights and entitlements of First Nations People and other Queenslanders in respect of their ability to access personal and family data that may be held by institutions owned by Queensland entities established by letters patent, and on truth-telling and treaty processes; and
- there are alternative, less restrictive and reasonably available ways to achieve the same purpose as the proposed amendments at clauses 19 and 84.

2.11 Time limit to request referral of privacy complaint to QCAT

The Bill at cl 53 proposes a 20 day time period for people to write to the Information Commissioner to request that their privacy complaints be referred to QCAT. [199] A 'privacy complaint' is a complaint by an individual about an act or practice of a relevant entity (as defined) in relation to the individual's personal information, that may be a breach of the 'privacy principle requirements' (as defined), or (for an agency) chapter 3A, part 2 or 3 of the IP Act.

The 20 day limit proposed in the Bill is significantly shorter than the 60 days proposed in Recommendation 18 of Review Report, though extensions are possible. The Information Commissioner may, if asked by the complainant, extend the period to request referral of the complaint if the Commissioner is satisfied that doing so is reasonable in the circumstances. If the period is extended, the Information Commissioner must give a written notice to the complainant and the respondent for the privacy complaint stating the new period.[200]

This difference between the recommended time limit to request referral of a privacy complaint, and the time limit proposed in the Bill, is notable because both the statement of compatibility and the explanatory notes identify the time limit as limiting human rights.[201] The amendments made by proposed new s 175A that introduces time limits for the referral of privacy complaints to QCAT engage the right to a fair hearing.

A fair hearing includes a reasonable opportunity to each party to present its case. This includes the opportunity to be informed of the opposing party's case and to respond.[202] The right to a fair hearing also relates to the right to 'commence, defend and settle proceedings as civil rights under the common law'.[203] The right to a fair hearing is also concerned with the procedural fairness of a decision. What fairness requires will depend on all the circumstances of the case. Broadly, it ensures a party has a reasonable opportunity to put their case in conditions that do not place them at a substantial

199 Bill, cl 53.

200 Explanatory notes, p 27.

201 Explanatory notes, p 8; Statement of compatibility, p 10.

202 *Roberts v Harkness* [2018] VSCA 215 [48].

203 *Goddard Elliott (a firm) v Fritsch* [2012] VSC 87 [553].

disadvantage compared to their opponent. This principle is commonly known as the principle of equality of arms.[204]

Rights and liberties of individuals

Consistency with the principles of natural justice

Legislation should be consistent with the principles of natural justice. The proposed amendment abrogates existing statutory rights of a complainant by providing that they have only 20 business days to ask for a privacy complaint to be referred to QCAT.

According to the explanatory notes, the amendments are justified on the basis that they are needed to provide more certainty for respondents and applicants about the status of complaints, and ensure that referrals to QCAT are made within a timely manner. For referrals to QCAT, the Information Commissioner would have discretion to extend the timeframe if reasonable in the circumstances.[205]

For privacy complaints to an agency or bound contracted service provider, the respondent may agree to a longer period if satisfied that the extension is reasonable. The explanatory argues that the amendments, therefore, provide sufficient flexibility to ensure fairness to an applicant.

The statement of compatibility states that the purpose of the 20 day limitation is to prevent an unreasonable delay on the part of a complainant in seeking a referral to QCAT and provide increased certainty for the complainant and respondent for the complaint.[206] It also states that the proposed amendments implement Recommendation 18 of the Review Report.

The Review Report considered whether there should be a time limit on when privacy complaints can be referred to QCAT. Most submissions to the review supported imposing a time limit to ensure certainty around the management of complaints.[207] Queensland Urban Utilities commented as follows:

> Without a time limit as to when a complaint can be made to QCAT, there is a possibility that a complaint may be referred to QCAT some years later, by which time relevant documents or information may no longer be available, or relevant officers within the agency may be unable to recall the full particulars of the original complaint or may have left the position/organisation.
>
> In this event, it may unduly prejudice an agency's ability to respond or defend itself or reduce the agency's ability to take corrective action in order to reduce the potential damage associated with a privacy complaint or breach. [208]

The OIC, in its submission to the review, also commented:

> The imposition of a time limit will provide for timely resolution of privacy complaints and prevent a situation from arising where a complainant requests OIC refer a privacy complaint to QCAT several years later.[209]

The statement of compatibility states that there are no less restrictive and reasonably available alternatives that would meet the purpose intended, and that providing a longer initial time period than 20 business days would result in the increased certainty for the complainant not being realised, and allow more scope for delay on the part of the complainant.[210] The statement also adds that, on

204 *Knight v Wise* [2014] VSC 76 [36].

205 Explanatory notes, p 8.

206 Statement of compatibility, p 11.

207 Review Report, p 42.

208 Review Report, p 42.

209 Review report, p 42.

210 Statement of compatibility, p 11.

balance, the importance of the amendments in providing reasonable limitations outweighs any limitations imposed on the right to a fair hearing.[211]

Submissions to the committee's inquiry did not address this aspect of the Bill.

Committee comment

The committee acknowledges the purposes of the proposed amendments: to prevent unreasonable delays in complainants seeking a referral to QCAT; to provide certainty for the complainant, the respondent and QCAT; and to achieve greater efficiency in addressing complaints about government action.

The committee agrees that the importance of the amendments in providing reasonable limitations outweighs any limitations imposed on the right to a fair hearing.

The committee is satisfied the provisions are consistent with fundamental legislative principles, noting that the Information Commissioner would have discretion to extend the timeframe if considered by the Information Commissioner to be reasonable in the circumstances.

2.12 Continuation of offences

The Bill at cl 73 includes a transitional provision[212] which applies in relation to an offence against former ss 185 or 187[213] committed in relation to a chapter 3 document by a person before the commencement.

- Section 185 states that a person must not, in order to gain access to a document containing another person's personal information, knowingly deceive or mislead a person exercising powers under the IP Act. The maximum penalty for the offence is 100 penalty units, being $15,480.
- Section 187 states that a person given notice to give information, or produce a document,[214] or attend before the Information Commissioner, must not, without reasonable excuse, fail to do so. The maximum penalty for the offence is 100 penalty units, being $15,480.

The Bill provides that a proceeding for the offence may be continued or started and the person may be convicted of and punished for the offence, despite s 11 of the Criminal Code. Section 11 of the Criminal Code states:

> (1) A person can not be punished for doing or omitting to do an act unless the act or omission constituted an offence under the law in force when it occurred; nor unless doing or omitting to do the act under the same circumstances would constitute an offence under the law in force at the time when the person is charged with the offence.
>
> (2) If the law in force when the act or omission occurred differs from that in force at the time of the conviction, the offender can not be punished to any greater extent than was authorised by the former law, or to any greater extent than is authorised by the latter law.

[211] Statement of compatibility, p 12.

[212] Bill cl 73 inserts IP Act, s 225.

[213] Meaning what is now the current sections 185 and 187 of the IP Act, which will become the 'former' sections if the Bill is passed.

[214] Meaning a chapter 3 document under the current IP Act.

Rights and liberties of individuals

Abrogation of existing statutory right – continuation of offences

Whether legislation has sufficient regard to rights and liberties of individuals depends on whether, for example, an abrogation of established statute law rights and liberties has been sufficiently justified.[215]

Issues of fundamental legislative principle arise here as the Bill may, in providing for the continuation of these offences, abrogate the rights of an individual under s 11 of the Criminal Code.

The transitional provision itself states that it will only apply to an offence committed *before* the commencement,[216] which means that the act or omission would have constituted an offence under the law in force when the conduct occurred. However, the second limb of s 11(1) relates to when an individual is *charged* with an offence. It is this part of s 11 that raises issues of fundamental legislative principle as it appears that, under this provision, an individual could potentially be charged with an offence against former ss 185 or 187 despite those laws (as relates to chapter 3 documents) not being in effect at the time the person is charged (and following from that, when proceedings are started and the person is potentially convicted and punished).

The explanatory notes provide the following justification for the provision:

> The continuation of proceedings and convictions and punishments for these offences is justified on the basis that the offences are in effect for the same conduct under provisions with continued effect under the RTI Act, and the amendment merely ensures that any conduct that occurred under the former IP Act continues to be subject to these offences.[217]

No further elaboration is provided. However, it can be seen that there are similar offences contained in the RTI Act relating to the conduct[59] and that whilst the Bill is amending ss 185 and 187 of the IP Act,[218] it does not remove these offences entirely. For the most part, the amendments relate to the removal of reference to 'chapter 3 documents' that are also removed by other parts of the Bill. In other words, it appears that the conduct being referred to would still be an offence if the Bill is passed, and the potential abrogation of statutory rights would relate to circumstances where a person has committed conduct in relation to a chapter 3 document and has not yet been charged.

Committee comment

The committee considers that any potential abrogation of statutory law rights in relation to the continuation of offences under s 185 and s 187 of the IP Act would be justified, given the limited scope of the transitional provision.

2.13 Agencies and Ministers to extend the time in which they must make internal review decisions

The Bill proposes to amend the RTI Act to allow agencies and Ministers to extend the time in which they must make internal review decisions: where the applicant has only supplied a postal address for notices; where third-party consultation is required;[219] or by agreement with the applicant.

215 OQPC Notebook, p 106.

216 Bill, cl 73 inserts IP Act, s 225(1).

217 Explanatory notes, p 12.

218 Bill, cls 61 and 63.

219 The Bill provides for the internal review processing period to be 30 business days from the valid application day, if the application relates to an access application and involves consultation with a relevant third party under s 37 of the RTI Act (that section authorises an agency or Minister to give access to a document that contains information, the disclosure of which may reasonably be expected to be of concern to a relevant third party, only if the agency or Minister has taken the steps that are reasonably practicable to discharge the specified requirements).

Rights and liberties of individuals

Under the RTI Act (s 80), a person affected by a 'reviewable decision' (Bill, cl 140 amends existing definition RTI Act, sch 5 and cl 139 inserts sch 4A) may apply to have the decision reviewed by the agency or Minister dealing with the application. Section 83 requires an agency or Minister to decide an internal review application as soon as practicable, however if the applicant isn't notified of a decision earlier, the agency's principal officer or the Minister is taken to have made a decision at the end of the 20 business days affirming the original decision.

Clauses 111 and 112 of the Bill inserts proposed new s 82A and amends s 83, of the RTI Act respectively.

Legislation should be consistent with the principles of natural justice, which include that procedural fairness should be afforded to a person, meaning fair procedures that are appropriate and adapted to the circumstances of the particular case.[220]

According to the explanatory notes, the proposed amendments allow a longer period for agencies and Ministers to make internal review decisions, potentially to the detriment of an applicant seeking such a decision, and abrogates existing statutory rights as, currently, internal review decisions do not accommodate extensions.[221]

Committee comment

The committee is satisfied with the justifications provided by the explanatory notes, including that there be sufficient time to conduct third-party consultation (intended to protect the rights of third parties), and that the proposed amendments may benefit the applicant where additional documents (not processed as part of the original application) have been located at the internal review, and need to be considered.

In that regard, on balance, the committee is satisfied that the proposed amendments have sufficient regard to the rights and liberties of individuals.

[220] LSA, s 4(3)(b).

[221] Explanatory notes, p 7.

Appendix A – Submitters

Sub #	Submitter
001	The Public Advocate
002	Salinger Consulting Pty Ltd
003	Office of the Information Commissioner Queensland
004	Local Government Association of Queensland
005	Crime and Corruption Commission
006	Queensland Human Rights Commission
007	Queensland Law Society
008	Information Integrity Solutions (IIS Partners)

Appendix B – Officials at public briefings

The committee held public briefings in Brisbane on 23 October and 13 November 2023.

The same officers provided both briefings.

Department of Justice and Attorney-General

- Mrs Leanne Robertson, Assistant Director-General
- Ms Melinda Tubolec, Acting Director
- Ms Joanna Eisemann, Principal Legal Officer
- Ms Alexis Hailstones, Principal Legal Officer
- Ms Kathryn Allan, Principal Legal Officer

Department of the Premier and Cabinet

- Ms Rachel Welch, Executive Director
- Mr Rob Lloyd-Jones, Director

Appendix C – Witnesses at public hearing

The committee held a public hearing in Brisbane on 13 November 2023.

Local Government Association of Queensland

- Ms Alison Smith, Chief Executive Officer
- Mr Angus Sutherland, Lead – Intergovernmental Relations

Office of the Information Commissioner

- Ms Stephanie Winson, Acting Information Commissioner
- Mr Paxton Booth, Privacy Commissioner
- Ms Anna Rickard, Acting Right to Information Commissioner

ISS Partners

- Ms Nicole Stephensen, Partner

Queensland Human Rights Commission

- Ms Neroli Holmes, Deputy Commissioner
- Ms Rebekah Leong, Principal Lawyer

Appendix D – Mapping recommendations to relevant parts of the Bill

Recommendation		How the Bill responds	Relevant clauses
Review Report Department of Justice and Attorney-General, *Review of the Right to Information Act 2009 and Information Privacy Act 2009*, Report, October 2017			
2	Amend the RTI Act and IP Act to provide for a single right of access under the RTI Act.	Amends the IP Act and RTI Act to provide for a single right of access to documents, including for personal information, to be applied for under the RTI Act, with the RTI Act also to cover applications to amend personal information	10, 80, 82
3	Remove the mandatory nature of the requirement under the RTI Act for applicants to be provided with a schedule of relevant documents, giving agencies a discretion whether to provide one.	Amends the RTI to remove the mandatory requirement for agencies and Ministers to give an applicant a schedule of relevant documents	96
7	Amend the RTI Act to include an express statement that factors other than those listed in Schedule 4 may be considered.	Amends Sch 4 of the RTI Act to clarify that factors for deciding the public interest may include factors other than those mentioned in the schedule	138
8	Amend the RTI Act so that departments and Ministers are subject to the disclosure log requirements that applied before the 2012 amendments.	Amends the RTI to require departments and Ministers to be subject to the same requirements as other agencies for disclosure logs under the RTI Act	102, 103
9	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.	Amends the RTI 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	102
10	Amend the RTI Act to remove current publication scheme requirements and instead require agencies to routinely publish significant, accurate and appropriate information about the agency on whichever website is most relevant.	Amends the RTI to require agencies to publish publication schemes on accessible agency websites, and requires them to include specified details, including the types of information held by the agency, how that information is made available, and procedures for asking for information.	88

Recommendation		How the Bill responds	Relevant clauses
11	Amend the RTI Act to allow agencies to extend the time in which agencies must make internal review decisions by agreement with the applicant or where third party consultation is required.	Amends 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.	111
12	Amend the annual reporting requirements under the Right to Information Regulation 2009 and the Information Privacy Regulation 2009 to: • transfer responsibility for preparing the annual reports from the responsible Minister to the Office of the Information Commissioner.	Amends the IP Act and RTI Act to transfer responsibility for preparing annual reports on the operation of the Acts from the responsible Minister to the Information Commissioner.	67, 133
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.	Amends to IP Act to adopt a single set of privacy principles in, based on the Australian Privacy Principles (APPs) in the Commonwealth Privacy Act and referred to as the Queensland Privacy Principles (QPPs), in place of the National Privacy Principles (NPPs) applying to health agencies and the Information Privacy Principles (IPPs) applying to all other agencies. Amends the IP Act to establish a mandatory data breach notification scheme applicable to agencies.	22-26 33 (proposed Ch 3) 74 33 (proposed Ch 3A)
14	Amend the definition of 'personal information' in the IP Act to be consistent with the Commonwealth definition.	Amends the IP Act to align the definition of 'personal information' in the IP Act with the definition in the *Privacy Act 1988* (Cth).	12
15	Amend the IP Act to regulate 'disclosure' of information outside Australia rather than 'transfer'.	Amends the IP Act to replace reference to 'transfer' of information outside Australia with 'disclosure'	27
16	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 to the relevant agency within 12 months of the complainant becoming	Amends the IP Act so that privacy complaints to an agency or bound contracted service provider are required to meet stated requirements, including being made in writing and	49

Recommendation		How the Bill responds	Relevant clauses
	aware of the act or practice the subject of the complaint. Agencies should also be required to give reasonable help to an individual making a privacy complaint to put the complaint in written form.	within 12 months of the complainant becoming aware of the act, failure to act or practice the subject of the complaint. Amends the IP Acts so that relevant agencies must give reasonable help to individuals to put complaints in writing.	
17	Amend the IP Act to allow agencies to request extensions of time for complaints to be resolved if required and 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 45 business days to expire.	Amends the IP act so that agencies can request extensions of timeframes for privacy complaints by agreement with the complainant. Amends the IP to remove the requirement for complainants to wait 45 business days from initial complaint to refer their complaint to the Information Commissioner.	47 (proposed s 164A) 48(3)
18	Amend the IP Act to provide that a complainant has 60 days to ask the Information Commissioner to refer a privacy complaint to QCAT for hearing. The 60 days should run from the day the Commissioner gives written notice under section 175 of the IP Act that the Information Commissioner does not believe the complaint can be resolved by mediation, or mediation is attempted but is not successful.	Amends the IP so that a complainant has 20 business days to ask the Information Commissioner to refer a privacy complaint to QCAT, with extensions possible where the commissioner is satisfied it would be reasonable in the circumstances.	53
19	Amend the IP Act to expressly provide the Information Commissioner with an 'own motion power' to investigate an act or practice which may be a breach of the privacy principles, whether or not a complaint has been made.	Amends the IP Act to provide a power to investigate, on the Information Commissioner's own motion, an act, failure to act or practice of an agency which may be a breach of the privacy principles or other stated obligations under the IP Act	35
20	Amend the definition of 'generally available publication' in the IP Act to be consistent with the Commonwealth definition. The amended definition should also ensure that purely digital communications are captured as appropriate.	Amends the definition of 'generally available publication' to mirror the definition in the *Privacy Act 1989* (Cth) including by capturing electronic publications	75

Recommendation		How the Bill responds	Relevant clauses
23	Amend the RTI Act and IP Act to make the operational changes listed in Appendix 3. The relevant recommended changes[222] are to:		
	(i) clarify the definition of 'processing period'	Amends the RTI Act to amend the definition of 'processing period'	86, 95
	(ii) extend the timeframe for making decisions about applications outside the scope of the Act	Amends the RTI Act to extend the timeframe for making decisions about applications outside the scope of the Act to 25 days	92
	(iii) require access applications to be in writing (with the approved form optional)	Amends the RTI Act to remove the requirement for applications to be in the approved form	90
	(iv) require amendment applications to be in writing (with the use of approved forms optional)	Amends the RTI Act to remove the requirement for amendment applications to be in the approved form	105 (proposed s 78E)
	(vi) remove the requirement for agents to provide evidence of identity in all cases	Amends the RTI Act to remove the requirement for agents to provide evidence of identity in all cases	90, 105 (proposed s 78E)
	(vii) limit the requirement to provide charge estimates notices (CENs) to two charge estimates per applicant and clarify that any narrowing of a second CEN would not require a third CEN to be issued	Amends the RTI Act to clarify that applicants are limited to two charge estimates notices (CENs) and that any narrowing of a second CEN would not require a third CEN to be issued	96
	(viii) provide that written notices of decisions must be sent (not given) by the end of the processing period to allow for postal delivery timeframes	Amends the RTI Act to extend the 'processing period' by five business days if the only address the applicant has given the agency or Minister to be sent notices is a postal address	86
	(ix) permit the disclosure of documents during an external review where necessary to facilitate that review	Amends the RTI Act to allow the Information Commissioner to disclose documents during an external review to third parties, to facilitate the resolution of an external review	121

[222] According to the explanatory notes, the Bill only addresses changes (i)-(iv) and (vi)-(xi).

Recommendation		How the Bill responds	Relevant clauses
	(x) permit the release of documents following an informal resolution settlement	Amends the RTI Act to clarify that an agency or Minister may release documents following an informal resolution of a review	116
	(xi) clarify that the Information Commissioner may to report to the Speaker on systemic issues	Amends the IP Act and the RTI Act to expand the matters on which the Information Commissioner may report to the Speaker to include any matters relating to the performance of the commissioner's functions. *Note: Under s 135 of the IP Act, the Information Commissioner's functions include conducting reviews of privacy related issues of a systemic nature and reporting on them to the Speaker.*	66, 132
Impala Report Crime and Corruption Commission, *Operation Impala, A report on misuse of confidential information in the Queensland public sector,* Report, February 2020			
10	That the Criminal Code be amended to add a new offence of misuse of confidential information by public officers, to contain the following attributes: 3. The simpliciter offence which involves only access to the confidential information is to be a crime, punishable by 5 years imprisonment 7. The offence is to contain the following definition section: benefit 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	Amends the Criminal Code to: • refer to 'misuse of a restricted computer' rather than 'computer hacking and misuse' • convert the basic or simple offence into a misdemeanour • increase the penalty from 2 years to 3 years • clarify that 'benefit' is not limited to pecuniary benefits	4

Recommendation		How the Bill responds	Relevant clauses
	Note: only the most relevant parts of the recommendation have been included here.		
12	That a mandatory data breach notification scheme be implemented in Queensland and that the OIC be responsible for developing the scheme, and receiving and managing the notifications.	Amends the IP Act to establish a mandatory data breach notification scheme applicable to agencies. Gives the OIC new functions and powers relating to compliance with the scheme.	33 (proposed Ch 3A)
14(1)	That the OIC have own-motion powers under the IP Act to strengthen existing powers and better identify systemic issues arising from an act or practice of an agency.	Amends the IP Act to provide a power to investigate, on the Information Commissioner's own motion, an act, failure to act or practice of an agency which may be a breach of the privacy principles or other stated obligations under the IP Act.	35
16	That the IPPs and NPPs in the IP Act be amalgamated and strengthened, having regard to the APPs contained in the Privacy Act (Cth); and in particular the: • definition of "reasonable steps" in the fourth of each set of principles relating to security of data be further defined in accordance with the terms of Article 32 of the EU GDPR; and • definition of "personal information" be amended in the IP Act to accord with the current version contained in the Privacy Act (Cth).	Amends to IP Act to adopt a single set of privacy principles in, based on the Australian Privacy Principles (APPs) in the Commonwealth Privacy Act and referred to as the Queensland Privacy Principles (QPPs), in place of the National Privacy Principles (NPPs) applying to health agencies and the Information Privacy Principles (IPPs) applying to all other agencies. Amends the IP Act to align the definition of 'personal information' in the IP Act with the definition in the *Privacy Act 1988 (Cth)*.	22-26 33 (proposed Ch 3) 74 12
Windage Report Crime and Corruption Commission, *Culture and Corruption Risks in Local Government: Lessons from an investigation into Ipswich City Council*, Report, August 2018			
3(b)	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 RTI Act.	Amends the RTI Act to clarify the definition of 'public authority' and provide clearer criteria for when an entity may be declared as a public authority under the RTI Act	84, 85

Recommendation		How the Bill responds	Relevant clauses
Strategic Review Report PWC, *Strategic Review of the Office of the Information Commissioner*, Report, 26 April 2017			
(c)	Office of the Information Commissioner be given the legislative ability to accept privacy complaints at its discretion, without reference to a time period.	Amends the IP to remove the requirement for complainants to wait 45 business days from initial complaint to refer their complaint to the Information Commissioner.	48(3)
(d)	Office of the Information Commissioner be funded and supported to administer the collection and collation of performance reporting by agencies under the Acts. Reporting requirements should be rationalised to maximise value and minimise collection effort.	Amends the IP Act and RTI Act to transfer responsibility for preparing annual reports on the operation of the Acts from the responsible Minister to the information commissioner. Agencies/Ministers will be required to provide the Information Commissioner with necessary information.	67, 133
Coaldrake Report Prof Peter Coaldrake, *Let the sunshine in: Review of culture and accountability in the Queensland public sector*, Final Report, 28 June 2022			
10	Citizens' privacy rights be protected by implementation of mandatory reporting of data breaches.	Amends the IP Act to establish a mandatory data breach notification scheme applicable to agencies.	33 (proposed Ch 3A)

Appendix E – Queensland Privacy Principles proposed in the Bill[223]

QPP1	**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 any QPP code that binds the agency) 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).
QPP2	**Anonymity and pseudonymity** Individuals must have the option of not identifying themselves, or using a pseudonym in relation to a particular matter, unless the agency is required or authorised by law to deal with identified individuals, or it is impracticable to deal with individuals who have not identified themselves or who have used a pseudonym.
QPP3	**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* unless the individual consents, or an exception applies. The exceptions for collection of sensitive information are where: • the collection is required or authorised by law; • a 'permitted general situation exists' (see below, page 5); • the agency is a health agency and a 'permitted health situation' exists in relation to the collection (see below, page 5); or • the agency is a law enforcement agency and reasonably believes that collection of the information is reasonably necessary for, or directly related to, one or more of its functions or activities. An agency must only collect personal information by **lawful and fair** means. An agency must collect personal information **about an individual only from the individual unless**: • the individual consents to collection from someone else; or • the collection is required or authorised by law or a court or tribunal order; or • it is unreasonable or impracticable to do so.

[223] There are no QPP 7, 8 or 9 because the equivalent Australian Privacy Principle has not been adopted.

QPP4	**Dealing with unsolicited personal information** An agency must take the following steps if it receives personal information it did not solicit: • decide whether or not it could have collected the personal information under QPP 3 if it had solicited it; **and** • if the agency decides it could not have collected the personal information under QPP 3 and the information is not contained in a public record — the agency must destroy or de-identify the information as soon as practicable, if it is lawful and reasonable to do; **or** • if the agency decides it could have collected the personal information under QPP 3 or the information is contained in a public record or the agency is otherwise not required to destroy or de-identify the information, the agency may retain the personal information but must deal with it in accordance with QPPs 5 to 13.
QPP5	**Notification of the collection of personal information** At or before the time or, if that is not practicable, as soon as practicable after, an agency collects personal information about an individual, the agency must take steps, if any, that are reasonable in the circumstances to notify the individual of specified matters that are reasonable in the circumstances or to ensure the individual is aware of such matters. The specified matters include: • the identity and contact details of the agency; • the fact and circumstances of the collection; • if the collection is required or authorised by law, the name of the law; • the purposes of collection; • the main consequences (if any) for the individual if the personal information is not collected; • any other agency, entity or kind of agency or entity to which the agency usually discloses personal information ; and • information about the agency's QPP privacy policy.

QPP6	**Use or disclosure of personal information** If an agency holds personal information about an individual which was collected for a particular purpose (the primary purpose) the agency must not use or disclose the information for another purpose (secondary purpose) unless the individual has consented to the use or disclosure of the information, or an exception applies. The exceptions include where: • 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, or for sensitive information, directly related to the primary purpose; • the use or disclosure is required or authorised by law; • a permitted general situation exists (see below); • the agency is a health agency and a permitted health situation exists in relation to the use or disclosure (see below); • the agency reasonably believes that the secondary purpose is reasonably necessary for one or more enforcement related activities of a law enforcement agency (the agency must make a written note of the use or disclosure); the disclosure is made to an authorised officer or employee of ASIO following a request from ASIO and written certification that the information is required in connection with ASIO's functions; • the use of disclosure of the personal information by an agency is necessary for research, or the compilation or analysis of statistics, in the public interest in the stated circumstances.
QPP10	**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 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.
QPP11	**Security of personal information** An agency must take reasonable steps to protect personal information it holds from misuse, interference or loss, and from unauthorised access, modification or disclosure. If an agency no longer needs personal information for a purpose for which the information may be used or disclosed under the QPPs, and the information is not contained in a public record, and the agency is not required by law to retain the personal information the agency must take reasonable steps to destroy the information or ensure it is de-identified.
QPP12	**Access to personal information** If an agency holds personal information about an individual the agency 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 12 if the agency is required or authorised to refuse to give the individual access to that information by or under the *Right to Information Act 2009* (RTI Act) or any other Queensland Act that provides for access by persons to documents.

QPP13	**Correction of personal information** If agency holds personal information about an individual, and either the agency is satisfied that the information is inaccurate, out of date, incomplete, irrelevant or misleading, or an individual request the agency to correct the information, the agency must take reasonable steps to correct the personal information to ensure that it 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. This requirement is subject to any limitation in the RTI Act or any other Queensland Act regulating the amendment of personal information. If an agency refuses to correct the personal information as requested by the individual, and the individual requests that agency associate a statement with the information that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading, the agency must take reasonable steps to do so.

Source: Department of Justice and Attorney-General, Briefing paper, 19 October 2023.

Appendix F – Abbreviations and acronyms

Abbreviations/acronyms	Definition
APP	Australian Privacy Principle
Bill	Information Privacy and Other Legislation Amendment Bill 2023
CCC	Crime and Corruption Commission
Coaldrake Report	Prof Peter Coaldrake, *Let the sunshine in: Review of culture and accountability in the Queensland public sector*, Final Report, 28 June 2022
Corporations Act	*Corporations Act 2001* (Cth)
Commonwealth Privacy Act	*Privacy Act 1988* (Cth)
Department/ DJAG	Department of Justice and Attorney-General
FLP	Fundamental legislative principle
HRA	*Human Rights Act 2019*
IP Act	*Information Privacy Act 2009*
LGAQ	Local Government Association of Queensland
LSA	*Legislative Standards Act 1992*
MDBN scheme	Mandatory Data Breach Notification Scheme
NPP	National Privacy Principle
OIC	Office of the Information Commissioner
QCAT	Queensland Civil and Administration Tribunal
QHRC	Queensland Human Rights Commission
QLS	Queensland Law Society
QPP	Queensland Privacy Principle
Review Report	Department of Justice and Attorney-General, *Review of the Right to Information Act 2009 and Information Privacy Act 2009*, Report, October 2017
RTI Act	*Right to Information Act 2009*
SI Act	*Statutory Instruments Act 1992*
Strategic Review Report	PWC, *Strategic Review of the Office of the Information Commissioner*, Report, 26 April 2017
Windage Report	Crime and Corruption Commission, *Culture and Corruption Risks in Local Government: Lessons from an investigation into Ipswich City Council*, Report, August 2018

Statement of Reservation

LNP Opposition Statement of Reservation

Information Privacy and Other Legislation Amendment Bill 2023

The LNP members share the concerns of the LGAQ about the ability for Local Governments, especially smaller regional, remote and First Nations Councils, to properly fulfill their obligations as outlined in the legislation.

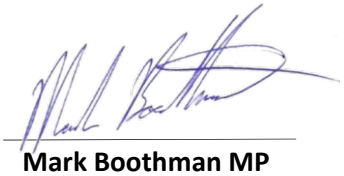
This will place further cost burdens on Councils who simply do not have the resources to fulfill these new requirements. Consequently, this will place additional costs on rate payers exacerbating the cost-of-living crisis Queensland finds itself in.

James Lister MP

Deputy Chair

Member for Southern Downs

23 November 2023



Mark Boothman MP

Member for Theodore

23 November 2023