Office of the Information Commissioner
Queensland

15 October 2019

Level 7
133 Mary Street
Brisbane Q 4000

PO Box 10143
Adelaide Street
Brisbane Q 4000

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

ABN: 70 810 284 665

Office of the National Data Commissioner
PO Box 6500
CANBERRA ACT 2600

Submission: Data Sharing and Release Legislative Reforms Discussion Paper

The Queensland Office of the Information Commissioner (**OIC**) welcomes the opportunity to provide a submission in response to the Data Sharing and Release Legislative Reforms Discussion Paper (**Discussion Paper**).

About the OIC

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

Queensland's RTI Act recognises that government-held information is a public resource and that openness in government enhances accountability. The RTI Act represents a clear move from a 'pull' model' to a 'push model' emphasising proactive and routine release of information and maximum disclosure of information unless to do so would be contrary to the public interest.

Opening up government-held information, including data, is consistent with, and an important part of Queensland's right to information 'push model'. OIC supports data sharing and release strategies and initiatives that maximise disclosure of government-held information to the community, carefully balanced with other important public interests such as appropriately safeguarding the community's privacy.

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

The Information Privacy Act in Queensland

Queensland's *Information Privacy Act 2009* (**IP Act**) recognises the importance of protecting the personal information of individuals. It creates a right for individuals to access and amend their own personal information and provides rules or 'privacy principles' that govern how Queensland government agencies collect, store, use and disclose personal information. OIC has regulatory oversight of Queensland Government agencies' compliance with requirements under the IP Act. Queensland government agencies include local governments, Queensland State Government departments, public universities, hospitals and health services and public authorities.

The Office of the Information Commissioner is an independent statutory authority.

The statutory functions of the OIC under the Information Privacy Act 2009 (Qld) (IP Act) include commenting on the administration of privacy in the Queensland public sector environment.

This submission does not represent the views or opinions of the Queensland Government.

OIC's submission

OIC provides the following high level comments in response to some of the key issues raised by the Discussion Paper:

1. Proposed Privacy measures

OIC notes that the Department of Prime Minister and Cabinet (**Department**) has accepted in full or in principle all eight recommendations from the Privacy Impact Assessment (**PIA**).[1] OIC welcomes proposed measures to strengthen privacy safeguards in the Data Sharing and Release (**DS & R**) Framework, including:

- restricting on-sharing of data
- facilitating data sharing only and not compelling sharing or release
- data custodians will not be allowed to share data for compliance, assurance, national security and law enforcement purposes under the DS&R legislation
- DS&R legislation will not authorise the release of personal information as open data; and
- specific accreditation for the handling of personal information.

By way of general comment, OIC notes that the Department will be finalising a list of secrecy provisions to be exempt from the override and the issue of commercial use remains uncertain. OIC may wish to provide further comment on the list of finalised exemptions and the issue of commercial use during proposed public consultation on the draft legislation.

OIC notes that binding guidance issued by the National Data Commissioner will be in the form of Data Codes, applicable to anyone operating under the DS&R legislation. OIC considers the Data Codes provide sufficient flexibility to guide and support entities to adhere to best practice in the application of the legislation as technology evolves. The ability of the DS&R Framework to respond to the privacy challenges posed by emerging issues, such as technological developments in the re-identification of data, is an important privacy safeguard.

2. State and Territory Data

OIC notes that the Discussion Paper states that the Commonwealth is working towards building a national system, but State and Territory data will not initially be in scope. The timing for a national data system and participation by states and territories is unclear.

OIC also notes that it will be a requirement for State and Territory users to be covered by the Commonwealth *Privacy Act 1998*, or a State or Territory Law that provides equivalent protection to the *Privacy Act 1988*[2] including the Australian Privacy Principles relating to privacy notification requirements and security standards.[3]

It appears unlikely the *Information Privacy Act 2009* (QLD) would meet the test of equivalency with the Commonwealth Privacy Act,[4] presenting a range of challenges for

---

[1] Discussion Paper at page 29.
[2] Discussion Paper at page 31.
[3] This issue was raised in the PIA 2.1.4 Key Policy Postion 3: Covering the States and Territories and in Recommendation 4.
[4] The IP Act does not impose a mandatory obligation on Queensland Government agencies to notify OIC or affected individuals in the event of a privacy breach. Agencies may be subject to additional mandatory data breach notification obligations through other legislative requirements, such as the Information security incident reporting requirements under the Queensland

participation by this jurisdiction. The application of the *Privacy Act 1988* to this jurisdiction raises complex legal and implementation issues for government and participants.

3. Consent

The Discussion Paper notes that *the Office of the National Data Commissioner will encourage the use of consent where appropriate when applying the Data Sharing Principles, although the legislation will not require it in all circumstances.*[5] In accordance with the *Privacy Act 1988*, consent is not the only basis for the secondary use and disclosure of personal information. A range of other exceptions apply, including where the use or disclosure is authorised or required under an Australian law. In circumstances where the secondary use or disclosure of personal information is authorised or required under DS&R legislation, consent may not be necessary or appropriate.

However, OIC notes that the issue of consent is complex and rapid technological developments, such as Artificial Intelligence and Big Data, pose significant challenges for the traditional consent model, including the ability of individuals to exercise meaningful consent to the handling of their personal information. OIC also acknowledges that 'consent and the individual autonomy it protects do not override all other interests, and reflects the balance between privacy and other public interest objectives inherent in the Privacy Act'.[6]

Community expectations about how their personal information is managed and shared are changing. For example, the ACCC in their *Digital Platforms Inquiry* final report made a number of recommendations to strengthen privacy regulation in Australia, including amending the definition of personal information and strengthening consent requirements to require that consents are freely given, specific, unambiguous and informed and that any settings for additional data collection must be preselected to 'off'.[7]

The ACCC also recommended requiring consent whenever personal information is collected, used or disclosed by an entity subject to the Privacy Act, unless the personal information is necessary to perform a contract to which a consumer is a party, required under law, or otherwise necessary in the public interest.[8]

OIC agrees with the view expressed in the PIA that the major obstacle to developing a social licence (for the DS&R framework) is that the 'overall approach is basically a mandatory scheme (for consumers) with no consent provisions.'[9] The PIA also noted that 'although the proposed framework includes numerous privacy safeguards and a

---

Government Enterprise Architecture (QGEA), the Commonwealth Notifiable Data Breaches (NDB) scheme and the *My Health Records Act 2012* (Cth).

[5] Discussion Paper at page 9.

[6] Office of the Australian Information Commissioner, Discussion Paper on Consent and Privacy – submission to the Office of the Privacy Commissioner of Canada, https://www.oaic.gov.au/engage-with-us/submissions/discussion-paper-on-consent-and-privacy-submission-to-the-office-of-the-privacy-commissioner-of-canada/#the-apps-consent-transparency-and-notice

[7] Australian Competition and Consumer Commission (ACCC), Digital Platforms Inquiry – Final Report at page 24.

[8] Australian Competition and Consumer Commission (ACCC), Digital Platforms Inquiry – Final Report at page 24.

[9] Galexia Privacy Impact Assessment on the Proposed *Data Sharing and Release (DS&R) Bill* and Related Regulatory Framework [Final] 28 June 2019 at page 45

significant public benefit, the Framework does not include measures for individual consent or control'.[10]

In the absence of mandated consent, OIC supports the need for guidance and advice by the Office of the National Data Commissioner about when and how consent should be built into the Data Sharing Principles.

Transparency and accountability are essential to building community trust and acceptance of the public benefits of appropriate data sharing under the DS&R Framework. This requires meaningful community engagement and ongoing communication to promote the public benefit of the scheme, counter concerns over the absence of consent and lack of control over sharing of their personal information.

Community concerns over privacy intrusions and secondary use of data, whether real or merely perceived risks, have potential to undermine community trust and confidence in the DS&R Framework and inhibit the realisation of public benefits sought by the sharing of data. The lessons learned from the roll-out of changes to the My Health Record scheme in 2018 underline the importance of securing the trust and confidence of the user to the success of the scheme. In an environment of declining levels of trust in government, this becomes increasingly important.

OIC looks forward to the opportunity to provide feedback on the Exposure Draft of the Data Sharing and Release Legislation in early 2020.

Yours sincerely

Rachael Rangihaeata
Information Commissioner

[10]Galexia Privacy Impact Assessment on the Proposed *Data Sharing and Release (DS&R) Bill* and Related Regulatory Framework [Final] 28 June 2019 at page 45.