Office of the Information Commissioner
Queensland

10 January 2022

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

Attorney-General's Department
Australian Government
3-5 National Circuit
BARTON ACT 2600

By email: PrivacyActReview@ag.gov.au

Response to Privacy Act Review Discussion Paper

The Queensland Office of the Information Commissioner (**OIC**) welcomes the opportunity to provide a response to the Privacy Act Review 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 the personal information they hold.

OIC's statutory functions include receiving and 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 decisions of agencies and ministers about access to, and amendment of, information under the RTI and IP Act.

OIC's Submission

OIC provided an earlier submission in response to the release of the Issues Paper in October 2020. OIC's position, as outlined in our earlier submission, on key areas of reform remains unchanged. OIC has consistently advocated for alignment of privacy laws across national and international jurisdictions, to the greatest extent practicable. In an increasingly interconnected digital world, it is critical that Australian privacy laws remain fit for purpose. The emergence of new technologies, such as artificial intelligence, will necessitate a strengthened privacy framework to ensure the immense economic and other benefits these new technologies can deliver are appropriately balanced with the protection of an individual's privacy.

While OIC considers the technology neutral principles-based framework underpinning the *Privacy Act 1988* (Cth) (**Privacy Act**) provides the required flexibility to respond to new and emerging technologies, the existing regulatory framework requires updating and strengthening to ensure it strikes the right balance between competing rights and interests in an increasingly complex and digitised economy characterised by seamless data flows across borders.

Community expectations around privacy and the handling of their personal information are changing. Key findings of the *Australian Community Attitudes to Privacy Survey 2020* shows that privacy is a major concern for 70% of Australians while 87% want more control and choice over the collection and use of their personal information.[1] Meeting community expectations becomes critical for consumers, business and governments in building trust. Striking the right balance in a strengthened privacy framework will assist in meeting changing community expectations around personal information handling.

As outlined in OIC's earlier submission in response to the Issues Paper, OIC provides strong support for aligning the Privacy Act with the EU General Data Protection Regulation (**GDPR**) to enhance global interoperability of privacy laws to protect data flows across borders. Closer alignment would assist Australia seek adequacy status under the GDPR, reducing complexity and the regulatory compliance burden for Australian businesses working across international borders. New Zealand has made similar legislative changes consistent with the GDPR requirements. Japan has also achieved adequacy status under the GDPR. It is OIC's view that Australia will ultimately be disadvantaged should it fail to pursue adequacy status.

Strengthening and updating the framework underpinning the Privacy Act will, by necessity, require states and territories to reform and update their own privacy frameworks to align more closely with any revised Privacy Act. Failure to do so will lead to further a widening of the gap between privacy protections afforded under the Privacy Act and state and territory legislative frameworks. The impact of lack of nationally consistent privacy laws is not limited to the protection of an individual's privacy. The current patchwork of privacy laws across Australian jurisdictions presents ongoing challenges for regulatory compliance for government agencies and businesses and the implementation and success of a range of national data sharing and other initiatives. OIC will continue to advocate for reform of Queensland's privacy laws.

OIC's submission does not respond to each question in the Discussion Paper, rather the submission provides high level comments on key themes and specific issues in the Discussion Paper. As noted earlier, OIC reiterates earlier comments made in response to the Issues Paper.

1. Scope and Application of the Privacy Act

- Definition of personal information
  As noted in the Discussion Paper, the Privacy Act's application to technical information became uncertain following the decision in *Privacy Commissioner v Telstra Corporation Ltd* [2017] FCAFC 4. OIC supports amending the definition of 'personal information' in the Privacy Act to replace 'about' with 'relates to' to capture a greater range of information from which an individual could be identified, including technical and inferred personal information. Greater alignment of the definition of personal information with the definition in the GDPR has the benefit of enhancing global interoperability of privacy laws.

- Current exemptions
  For the reasons outlined in OIC's response to the Issues Paper, OIC considers retention of the small business exemption, employee records

[1] https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/acaps-2020-infographic

exemption and political parties' exemption is becoming increasingly difficult to justify and may not accord with changing community expectations. Preservation of these exemptions results in significant gaps in privacy protections and contributes to lack of accountability and transparency in the handling of personal information. While OIC notes the potential regulatory impact of the proposed removal of these exemptions, OIC considers this impact is substantially reduced by the extensive range of regulatory tools and guidance material available to assist these entities meet their regulatory obligations.

2. Protections

- Right to erasure of personal information

  While OIC provides in-principle support for a legislative right to erasure, the Discussion Paper highlights the diverse views of stakeholders and the complexities of balancing the right to erasure with other competing rights and interests. While the GDPR provides a useful model to draw upon, exceptions must be tailored to the Australian context.

  OIC previously submitted that an adoption of a right to erasure requires careful exploration and an appropriate balance needs to be struck with other competing rights and interests such as the freedom of expression, including the freedom to seek and receive information, as defined in various human rights laws. OIC notes the Discussion Paper states that Australian law only recognises the freedom of political communication as a constraint on legislative and executive power.[2] The *Human Rights Act 2019* (Qld) protects the rights to freedom of expression[3] and any legislated right to erasure in the Privacy Act has the potential to infringe on state based human rights legislation.

  As such, OIC considers any legislated right to erasure should provide for exceptions. At a minimum these exceptions should include compliance with legal obligations under an Australian law or court or tribunal order, record keeping and archival obligations and public interest considerations. The public interest balancing test in the Freedom of Information (**FOI**) Act or other legislated right to information frameworks, including the RTI Act may provide a useful model. As noted in OIC's earlier submission on the Issues Paper, the retention of records is fundamental to transparency and accountability underpinning the various FOI/RTI regimes.

- Automated decision-making

  As noted in the Discussion Paper, the use of Artificial Intelligence (**AI**) is becoming increasingly common across government agencies and the private sector with levels of automation being provided for in a variety of Commonwealth legislation.[4]

  The submission by the Office of the Australian Information Commissioner (**OAIC**) to the Australian Human Rights Commission (**AHRC**) *Human Rights and Technology Paper* noted that while AI has

[2] Discussion Paper at page 120.
[3] Section 21.
[4] Discussion Paper at page 137.

the 'potential to yield great benefits, including in predictive capabilities', it can also have 'significant impacts on privacy'.[5]

The Discussion Paper proposal at 17.1 is to require privacy policies to include information on whether personal information will be used in Automated Decision-Making (**ADM**) which has a legal, or similarly significant effect on people's rights. As outlined in OIC's earlier submission in response to the Issues Paper, adoption of legislative restrictions modelled on those provided in the EU under the GDPR are recommended. While privacy protections contained in policies and other ethical AI frameworks are welcome, they are not enforceable. The significant impacts ADM can have on an individual's privacy and other rights warrant legislated, enforceable protections. OIC also considers there is likely to be considerable uptake in the adoption of AI across government agencies and the private sector in the future. In the absence of a strong regulatory framework, the risks posed to an individual's privacy is significant.

3. Regulation and Enforcement

- Enforcement
  OIC supports the adoption of additional enforcement mechanisms and powers for the OAIC to support an updated and strengthened Privacy Act, including the proposal to create tiers of civil penalty provisions to give the OAIC more options so they can better target regulatory responses (24.1) and provide OAIC with the power to require an Australian Privacy Principle (**APP**) entity to identify, mitigate and redress actual or reasonably foreseeable loss or damage suffered by individuals.

  OIC also considers the effectiveness of additional enforcement mechanisms and powers requires adequate resourcing of the regulator. As submitted previously by OIC, a strong legislative privacy framework together with appropriate resourcing will assist in ensuring OAIC can regulate, guide and champion greater protection of the community from harm and position Australia to meet evolving future challenges.

- A direct right of action
  OIC supports giving individuals a direct right to action enabling individuals to directly apply to a court to seek compensation for an act or practice that is an interference with their privacy. As noted by the ACCC in the Digital Platforms Inquiry report, providing individuals with a direct right of action would give individuals greater control over their personal information and provides an additional incentive for APP entities to comply with their obligations under the Act.

- A statutory tort of privacy
  OIC supports Option 1: introduction of a statutory tort for invasion of privacy as recommended by the Australian Law Reform Commission Report 123. As previously submitted by OIC, a statutory cause of action for serious invasion of privacy should be enacted by the Commonwealth, in a new Commonwealth Act.

[5] OAIC, *Submission to AHRC Human Rights and Technology Inquiry Issues Paper* (Web page, 19 October 2018) cited in Discussion Paper at p137.

- Notifiable Data Breaches Scheme
  As outlined earlier, lack of consistency in privacy laws within Australia and across international jurisdictions contributes to gaps in privacy protections and increases the compliance burden for organisations and entities subject to the varying schemes. Different timeframes and thresholds can cause community uncertainty and unnecessary anxiety as demonstrated by the PageUp world-wide data breach.

  While accepting complete harmonisation is difficult to achieve, states and territories looking to adopt this requirement in their respective jurisdictions, through a voluntary or mandated scheme, should seek to align with the requirements of the Notifiable Data Breaches Scheme under the Privacy Act to the greatest extent practicable. This includes aligning with critical elements of the NDB Scheme such as definitions, timeframes, and thresholds. Greater alignment between the various notifiable data breach schemes allows jurisdictions to draw upon shared regulatory guidance and tools to assist agencies and entities comply with their regulatory obligations and minimise the risk of harm to individuals in the event of a data breach.

  OIC will continue to support the introduction of a mandatory data breach scheme in Queensland, recommended as part of legislative reform to Queensland's privacy legislation,[6] and seek alignment with the requirements of the Notifiable Data Breaches Scheme under the Privacy Act.

Yours sincerely

Rachael Rangihaeata
Information Commissioner

Paxton Booth
Privacy Commissioner

[6] Recommendation 12, Crime and Corruption Commission Queensland, *Operation Impala – Report on misuse of confidential information in the Queensland Public Sector*, February 2020; Recommendation 13, Report on the review of the *Right to Information Act 2009* and *Information Privacy Act 2009* (Review report), October 2017. Recommendation 13 of the Review report states 'conduct further research and consultation to establish whether there is a justification for moving towards a single set of privacy principles in Queensland, and whether a mandatory data breach notification scheme should be introduced'.