Office of the Information Commissioner
Queensland

27 November 2020

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 Issues Paper: Review of the *Privacy Act 1988* (Cth)

The Queensland Office of the Information Commissioner (OIC) welcomes the opportunity to provide a response to the Review of the *Privacy Act 1988* (Cth) (*Privacy Act*) Issues paper (Issues 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 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

It is critical that the *Privacy Act* remains fit for purpose in an increasingly interconnected digital world. Developments in Artificial Intelligence and technology will necessitate an increased need for stronger privacy and data security measures to be adopted and implemented. The recent findings of the *Australian Community Attitudes to Privacy Survey 2020* conducted by the Office of the Australian Information Commissioner demonstrate changing community expectations around handling of personal information. Meeting community expectations becomes critical for consumers, business and governments in building trust.

OIC provides strong support for aligning the *Privacy Act* with the 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 under the GDPR, reducing complexity and the regulatory compliance burden for Australian businesses working across international borders. New Zealand has recently introduced 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.

OIC's submission contains high level comments in addition to responses to some of the specific questions posed by the Issues Paper.

Definition of Personal Information

OIC supports aligning the definition of 'personal information' in the *Privacy Act* with the definition of personal information in the GDPR. As outlined in the Issues Paper, Article 4(1) of the GDPR stipulates that 'personal data means any information relating to an identified or identifiable natural person' and provides a non-exhaustive list of identifiers by which an identifiable natural person may be referenced. This would allow technical data such as location data and IP addresses to be considered personal information, providing greater certainty about the meaning of personal information following the decision by the Full Federal Court in *Privacy Commissioner v Telstra Corporation Ltd* (the Grubb case).[1] Alignment of the definition of personal information with the definition in the GDPR also has the benefit of enhancing global interoperability of privacy laws.

Small Business, Employee Records and Political Parties Exemptions

It is OIC's view that the small business exemption, employee records exemption and political parties exemption is becoming harder to justify and their relevance questioned in an increasingly digital world. OIC notes that back in 2010, the Australian Law Reform Commission (ALRC) recommended removal of the above exemptions.[2]

Placing obligations on small business, and other organisations such as registered political parties, to comply with the requirements of the *Privacy Act* enhances accountability and transparency in the handling of often large volumes of personal information. Preservation of these exemptions results in significant gaps in privacy protections. In respect of the small business and political parties exemptions, OIC notes the following:

Small business exemption

ABS data reports that as at 30 June 2019, there were 2,375,753 actively trading businesses in the Australian economy.[3] In 2018-19, 93.0% of businesses (2,209,450) had a turnover of less than $2million,[4] falling outside the regulatory regime of the *Privacy Act* and resulting in large gaps in the regulation of private sector handling of personal information.

OIC supports removal of the small business exemption on the grounds of fairness, equity, information security, accountability and transparency. Small business, if it supplies services for government, is required to be bound by the *Privacy Act*. A large number of small businesses are already likely to be bound to comply with the *Privacy Act*, significantly reducing the regulatory burden on small business should the existing exemption be removed. Continuing the

---

[1] *Privacy Commissioner v Telstra Corporation Ltd* [2017] FACFC 4.

[2] https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/list-of-recommendations-5/part-e-exemptions/

[3] https://www.abs.gov.au/statistics/economy/business-indicators/counts-australian-businesses-including-entries-and-exits/latest-release

[4] https://www.abs.gov.au/statistics/economy/business-indicators/counts-australian-businesses-including-entries-and-exits/latest-release

exemption creates the potential for increased cyber security risks as the small business may be the weakest links in the supply chain to attack larger more valuable information and data assets.

Political parties exemption

OIC notes that the justification for the existing exemption for political parties and political acts and practices was based on the importance of freedom of political communication to Australia's democratic processes. Political parties have access to vast amounts of personal information contained in electoral databases, including contacts individual voters have with parliamentarians and electorate offices.

In the context of compulsory voting and increasing concerns about risks posed by manipulation of private information by social media platforms to target and sway the political views of voters, it is OIC's view that retention of this exemption is no longer fit for purpose and should be removed. The Cambridge Analytica example is illustrative of the significant risks posed to the integrity of the electoral process when personal information is misused for political ends.

OIC further agrees with the view previously expressed by the Australian Law Reform Commission that 'in the interests of promoting public confidence in the political process, those who exercise or seek power in government should adhere to the principles and practices that are required of the wider community'.[5]

Ethical use and deployment of Artificial Intelligence (AI)

It is OIC's view that a revised *Privacy Act* incorporates legislative restrictions on the types of decisions that can be fully automated. While OIC welcomes the development of ethical AI frameworks, privacy protections contained in these frameworks are not enforceable. Adoption of legislative restrictions modelled on those provided in the EU under the GDPR are recommended. The GDPR prohibits use of solely automated processing for decisions that produce legal or other significant effects for individuals (unless specific exemptions apply). It also creates rights for individuals who are affected by automated processing.

A first step in reform of the *Privacy Act* is adoption of Article 22 i.e. the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, and potentially article 21 (right to object). Notice of processing is an important first step in building trust through transparency as governments increasingly look to automate government processes and pursue digital transformation. This is critically important, particularly following examples such as Robodebt and the trailing of AI technology in the detection of distracted drivers.

OIC will continue to advocate for legislative reform of Queensland's privacy laws, including for the ethical use of AI as outlined above.

Right to erasure

OIC supports further exploration of adoption of a 'right to erasure' into the *Privacy Act*. A 'right to erasure', also known as the 'right to be forgotten', is provided by Article 17 of the GDPR. In accordance with Article 17, the right is

---

5 https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/41-political-exemption/exemption-for-registered-political-parties-political-acts-and-practices/

not absolute and only applies in certain circumstances. The 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.

Any legislated right to erasure needs to ensure adequate exemptions are provided for a range of legitimate purposes including compliance with legal obligations, record keeping and archival purposes, and public interest considerations. The retention of records is fundamental to transparency and accountability underpinning the various FOI/RTI regimes.

Security of Personal Information

It is OIC's view that Article 32 of the GDPR provides greater specificity with respect to the security requirements agencies are expected to apply as opposed to the current the current 'reasonableness test' contained in the Australian Privacy Principles (APPs). The Queensland Crime and Corruption Commission, in its report on misuse of confidential information in the Queensland public sector,[6] recommended the definition of 'reasonable steps', in amalgamated and strengthened privacy principles in Queensland's privacy laws, be further defined in accordance with the terms of Article 32 of the GDPR, following evidence led by OIC during public hearings.

This is particularly important in providing small to medium businesses, not subject to information security standards, greater clarity regarding the organisational and technical measures required to be put in place to ensure adequate security.

Notifiable Data Breaches Scheme

The Notifiable Data Breaches Scheme appears to be functioning well and is a critical element in managing data breaches and mitigating privacy risks for individuals. It also is a necessary element for Australia to achieving adequacy under the GDPR. As states and territory look to adopt this requirement in their jurisdictions, it is critical that there is national consistency to ensure the efficacy of the system. Different timeframes and thresholds can cause community uncertainty and unnecessary anxiety as demonstrated by the PAGE UP world-wide 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,[7] and seek alignment with the requirements of the Notifiable Data Breaches Scheme under the *Privacy Act*.

A Statutory Tort of Privacy

It has been the consistent finding of a number of reviews and inquiries that Australia's privacy regulatory framework does not provide individuals with

---

[6] 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

[7] 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'.

adequate remedies for serious invasions of privacy.[8] OIC supports adoption of a statutory tort of privacy recommended by the ACCC in its *Digital Platforms Inquiry – Final Report* (DPI) as previously recommended by the ALRC.[9] As noted by the ACCC, this cause of action provides protection for individuals against serious invasions of privacy that may not be captured within the scope of the *Privacy Act*. A statutory cause of action for serious invasion of privacy, if enacted, should be enacted by the Commonwealth, in a new Commonwealth Act.

OIC further 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 DPI report, providing individuals with a direct right of action would give individuals greater control over their personal information and provide an additional incentive for APP entities to comply with their obligations under the Act.

Adoption of a Statutory National Bill of Rights or Charter should also be considered to provide baseline protection of human rights, including the protection of the right to privacy. While a number of states have sought to introduce human rights legislation, enactment at the national level would be most effective, particularly as part of the regulatory framework for artificial intelligence.

Adequate Resourcing for the Regulator

Revisions to the *Privacy Act* that result in new and/or enhanced regulatory functions for the Office of the Australian Information Commissioner require adequate resourcing to ensure the effectiveness of any enhanced regulatory regime. This is particularly critical in meeting challenges posed by a range of external factors impacting on service delivery, including transition to a digital economy and the broader scope of entities recommended to be regulated to provide greater protection of the community from harm, and build confidence and trust in how personal information is handled. A strong legislative framework together with appropriate resourcing to ensure OAIC can regulate, guide and champion greater protection of the community from harm, will position Australia well to meet evolving future challenges.

Your sincerely

Rachael Rangihaeata
Information Commissioner

Phil Green
Privacy Commissioner

[8] In its 2008 Report, *For Your Information: Australian Privacy Law and Practice*, the ALRC recommended that federal legislation should provide for a statutory cause of action for serious invasions of privacy. The ALRC's 2014 report, *Serious Invasions of Privacy in the Digital Era* recommended that a statutory tort of serious invasions of privacy should be introduced by way of a standalone Federal Act. The 2016 New South Wales Legislative's Council Inquiry on *Remedies for the serious invasion of privacy in New South Wales* and the Victorian Law Reform Commission, *Surveillance in Public Places: Final Report 18* (2010), Ch.7 made similar recommendations.

[9] ACCC, Digital Platforms Inquiry (n 1) 493.