Australia: Significant changes proposed to Australia's privacy regime

Australian government releases a long-awaited report on review of the Privacy Act, proposing wholesale amendments to Australia's flagship privacy legislation.

In brief

The Commonwealth Attorney-General's Department has released its long-awaited report (the "**Report**") on its review of the *Privacy Act 1988* (Cth) ("**Privacy Act**"), which proposes widespread amendments to Australia's flagship privacy legislation. Stakeholders have until **31 March 2023** to provide feedback to the government on the proposals.

The Report proposes amendments across three areas:

- **Scope and application of the Privacy Act** - while the principles-based approach to regulation would be retained, some revisions would be made to clarify and broaden the scope and application of the Privacy Act. Most notably, definitions would be added and amended to provide clarity (for example, to confirm that technical and inferred information is captured), geo-location tracking data would be subject to consent requirements, de-identified information would be regulated to a certain extent, and certain exemptions - including the employee records exemption - would be narrowed or removed completely.
- **Protections** - personal information would be subject to enhanced protections, including through the introduction of new EU-inspired rights for individuals and an overarching requirement that collection and handling of personal information must be objectively "fair and reasonable". Collection notices and consent requirements would be enhanced and might ultimately be standardized. Records would need to be kept regarding purposes of processing and entities would be expected to appoint a privacy officer. Additional transparency would be mandated for certain automated decision making. Privacy impact assessments would be compulsory prior to undertaking high privacy risk activities, and special requirements would apply in respect of vulnerable people's and children's personal information. Direct marketing, targeting and trading in personal information would be more heavily regulated, with individuals having clear rights to opt out. Other key proposals include: revisions to security, retention and destruction obligations; adoption of a limited controller-processor distinction; and changes in respect of overseas data flows and extraterritorial application of the Privacy Act.
- **Regulation and enforcement** - the range of available penalties for non-compliance would be expanded to cover a clarified and expanded range of conduct. Australia's privacy regulator, the Office of the Australian Information Commissioner ("**OAIC**"), would enjoy expanded powers including the right to require entities to identify and mitigate loss and damage that could result from their privacy failings. Other notable changes include: allowing individuals a direct right of action to seek relief for interferences with their privacy; a statutory tort for serious invasions of privacy; and changes to the notifiable data breach scheme, including a 72-hour notification deadline.

Contact Information

Anne-Marie Allgrove
Partner
Sydney

Anne Petterd
Partner
Sydney

Toby Patten
Partner
Melbourne

Adrian Lawrence
Partner
Sydney

Caitlin Whale
Partner
Sydney

Key takeaways

If the proposals are enacted, they will bring some further clarity and detail to existing aspects of Australian privacy law. The proposed requirements will also impact how businesses across the Australian economy collect and handle individuals' personal information.

Many businesses, large and small, will need to make some changes to their processes and policies in order to achieve compliance with the proposals. For multinationals whose processing is subject to the EU General Data Protection Regulation ("**GDPR**"), several of the proposals will be familiar territory.

The recommended changes to the enforcement regime are also notable from a business risk management perspective and complement the major reform to penalties under the Privacy Act which occurred in December 2022.

Next Steps

The Government is seeking stakeholder feedback on the proposals raised in the Report, with the deadline set at **31 March 2023**. This provides businesses only a limited window to consider and respond to many complex and significant changes which are proposes throughout the Report and which may materially affect their business. Interested stakeholders should take this opportunity to contribute to what could be a once-in-a-generation reform to Australian privacy law. Certain proposals (e.g. the removal of the small business exemption) require further stakeholder consultation, suggesting that some reforms may still be some way off. Interested parties should listen out for further consultation opportunities to present themselves.

Context

The Report has been a long time coming: the review of the Privacy Act commenced in 2020 under the previous government, with an Issues Paper and Discussion Paper published for consultation in September 2020 and October 2021 respectively.

With the review being a complex and slow-moving process, and in light of significant data breaches impacting several household names and government agencies, some legislative amendments were made in December 2022 to increase penalties and OAIC powers under the Privacy Act. The Report acknowledges and builds on those changes, advocating for a major shift in Australian privacy regulation which cherry-picks some concepts from the EU GDPR and other jurisdictions' privacy laws to bolster protections for individuals in Australia.

In depth

The Report makes 116 proposals across three key areas. It is necessary to read the Report to gain a full understanding of all the proposals and the motivations behind them. As quick reference, the most significant proposals for business are summarized below:

1. Scope and application of the Privacy Act

Key proposed changes to the scope and application of the Privacy Act include:

- **Personal information:** amend the definition of "personal information" to clarify what it is intended to cover. Personal information would be information or an opinion which "relates to" an identified or reasonably identifiable individual, emphasizing the relationship between the information and the individual which would be established through context. This would make it clearer that technical and inferred information can be personal information. Guidance would also be provided on what information is likely to fall within the definition and when an individual will be considered "reasonably identifiable".
- **De-identified information:** protect de-identified information to a certain extent, in relation to security, cross-border disclosure and notifiable data breaches, reflecting that keeping information de-identified may involve continuous attention. De-identification would be characterized as a process, informed by best available practice. Re-identification would be generally prohibited and further consultation is proposed around a potential criminal offence for malicious re-identification.

- **Sensitive information:** adjust the definition of "sensitive information" to refer to information which "relates to" an identified or reasonably identifiable individual. Expand the definition to include genomic information and clarify that sensitive information can be inferred from "proxy" non-sensitive information.
- **Geo-location tracking data:** require an individual's consent to handle their precise geolocation tracking data.
- **Exemptions:** amend or remove several exemptions from the requirements of the Privacy Act:
    - **Small business exemption:** eventually, remove the exemption, subject to further consultation, a support package and potential adjustments to certain compliance requirements for small business. In the short term, the exemption would not apply to collection of biometric information for use in facial recognition technology, nor to businesses that obtain consent to trade in personal information.
    - **Employee records exemption:** extend enhanced privacy protections to private sector employees, balancing various goals such as improved transparency for employees and adequate flexibility for employers. Crucially, employers would be required to protect employee personal information and notify employees and the OAIC of data breaches involving employee personal information where this is likely to cause serious harm. Exactly how this would be achieved is left open, however, with further consultation and consideration contemplated.
    - **Political and media / journalism exemptions:** narrow the political exemption and provide that acts and practices subject to the revised exemption have to meet certain requirements (e.g. that they are fair and reasonable). Media organizations wishing to rely on the journalism exemption would also need to meet new requirements (e.g. comply with security and destruction obligations for personal information and the notifiable data breach scheme). These changes will have significant implications for the entities which have been relying on these exemptions. Such entities would be advised to review the detail of the proposed changes for more information.
- **APP codes:** empower the Information Commissioner to make privacy codes of practice ("**APP codes**"). APP codes could be made where the Attorney-General directs or approves that the making of the code is in the public interest or that there is unlikely to be an appropriate industry representative to develop the code. Such APP codes would be subject to a mandatory public consultation period lasting at least 40 days. Temporary APP codes lasting up to 12 months could be developed where urgently required (e.g. in an emergency situation such as a pandemic) without a formal public consultation.
- **Emergencies:** improve the Emergency Declarations regime, by allowing declarations to be targeted to specific entities, classes of entities, types of personal information, or specified acts or practices. Declarations should also be able to be made in relation to ongoing emergencies.

2. Protections

The Report proposes a wide range of changes to the protections contained in the Privacy Act. Most notably:

- **Fair and Reasonable:** introduce a requirement for collection, use and disclosure of personal information to be fair and reasonable, assessed objectively from the position of a reasonable person. This requirement would apply irrespective of whether an individual consented, but would not apply where an exception obviates the need for consent. The Privacy Act could outline a series of factors to take into account in considering what is fair and reasonable, such as: the reasonable expectations of the individual; the kind, sensitivity and amount of personal information; and risk of unjustified adverse impact or harm. This proposal builds on suggestions made by the Australian Competition and Consumer Commission (ACCC), in its 2019 Digital Platforms Inquiry report, that consideration should be given to greater protections for consumer data, such as requiring all use and disclosure to be by fair and lawful means. The addition of an overarching fairness and reasonableness requirement may make it easier for the OAIC to take enforcement action in response to sharp data handling practices, supplementing ACCC enforcement action via consumer law channels, for example on the basis of misleading or deceptive conduct.

- **High Privacy Risk Activities:** formal privacy impact assessments (PIA) would be required prior to undertaking high privacy risk activities (as described above). Use of facial recognition technology and other use of biometrics might also be subject to additional regulation, and entities would be expected to inquire into whether indirectly collected information was originally collected in a compliant manner. The OAIC would also have a greater role in developing practice-specific guidance for new technologies and emerging privacy risk areas.
- **Collection notices and consents:** expressly require collection notices (statements given to individuals at or about the time their information is collected) to be clear, up-to-date, concise and understandable, and include additional information, such as the circumstances surrounding the collection, use or disclosure of personal information for any "high privacy risk activities". According to the Report, this refers to activities that are "likely to have a significant impact on the privacy of individuals", and the legislation and OAIC guidance could clarify when activities would qualify. Illustrative examples given include: handling of sensitive information, or children's personal information, on a large scale; online tracking, profiling and delivery of personalized content and advertising to individuals; and sale of personal information. The Report also suggests creating standardized templates and layouts for privacy policies and collection notices, including terminology and icons.
- **Consent:** update the definition of "consent" to provide that it must be voluntary, informed, current, specific, and unambiguous. Most of these concepts are referred to in current guidance, so this would not represent a big shift. But the new reference to "unambiguous" may make it more difficult to rely on implied consent in some contexts. Further clarity would hopefully be provided by updated and expanded OAIC guidance. Other consent-related proposals include express recognition of the ability to withdraw consent, guidance for online services on how to design consent requests, and an ability for individuals to give broad consent for research purposes.
- **Organizational accountability:** entities should have to determine and record the purposes of collection, use and disclosure of personal information at or before the time of collection. It would be mandatory for entities to appoint or designate a senior employee responsible for privacy, i.e. have a privacy officer.
- **Online privacy by default:** with respect to digital businesses, online privacy settings should reflect a privacy by default approach, being clear and easily accessible to end users.
- **Individual Rights:** make changes to the rights of individuals, including introducing new rights modelled on the EU GDPR:
    - A right to **access and explanation**, including identification of the source for the information and what the information has been used for.
    - A right to **object** to the collection, use or disclosure of personal information, and a corresponding obligation for entities to respond in writing with reasons.
    - A right to request **erasure** of personal information, subject to exceptions. Where information has been provided by or shared with third parties, the entity receiving the request would need to inform individuals of the third party and notify the third party/ies of the request, unless this is impossible or involves a disproportionate effort.
    - A right to have personal information **de-indexed**, i.e. removed from search engine result lists, where the information is sensitive, relates to children, is excessively detailed or is inaccurate, incomplete, irrelevant or misleading.
    - An extended right of **correction** also covering generally available publications online over which an entity maintains control.
- **Direct marketing, targeting and trading:** direct marketing, targeting and trading in personal information should be defined and regulated. "Targeting" would be subject to restrictions and transparency requirements, even where the information used does not relate to an identified or reasonably identifiable individual. Additional consent requirements would apply for trading, and individuals would have an unqualified right to opt-out of their personal information being used or disclosed for direct marketing and from targeting advertising.

- **Automated decision-making:** automated decision-making using personal information should be regulated where the decision may have a significant effect on an individual. Individuals would be entitled to request meaningful information about how such decisions are made.
- **Security, retention and destruction:** amend the Privacy Act to make it clear that reasonable steps to secure personal information includes taking technical and organizational measures. Baseline privacy outcomes should be set for securing personal information, following industry and government consultation. Outcomes could be informed by the government's cyber security strategy, with technical advice from the Australian Cyber Security Centre providing additional direction for security guidance. OAIC guidelines should provide further clarity around the reasonable steps entities are expected to take to destroy or de-identify personal information. De-identified information would also need to be kept secure. Entities should set and periodically review time periods for the retention of personal information. Retention periods should be specified in privacy policies.
- **Controllers and processors:** introduce limited concepts of "controllers" (entities who determine the purposes for and means of processing personal information) and "processors" (entities which process personal information on behalf of controllers), similar to the GDPR. In relation to information processed for a controller, processors would be subject only to a limited range of obligations under the Privacy Act, regarding openness and transparency, security and data breach reporting.
- **Overseas data flows:** make provision to prescribe laws and binding schemes in other jurisdictions which provide "substantially similar" protection to the Privacy Act. This would enable entities to rely on an exemption from the obligation to take reasonable steps to ensure that overseas recipients of personal information do not breach the Privacy Act. Additionally, standard contractual clauses should be created to facilitate compliant overseas disclosures, and collection notices should indicate the types of personal information which may be disclosed to overseas recipients. Enshrine OAIC guidance on the meaning of "disclosure" in statute, and consider introducing an exception to overseas disclosure requirements for online publications.
- **Extra-territorial application:** consult on amending the Privacy Act's extra-territorial application provisions to stipulate that an "Australian link" requires personal information which is "connected with Australia".
- **Children and vulnerable people:** existing OAIC guidance on children and young persons and capacity should be maintained, but a few changes should be made, for example, to codify that consent is only valid with appropriate capacity. Collection notices and privacy policies should be made understandable for children and there should be a Children's Online Privacy Code for online services likely accessed by children, which addresses how their best interests should be supported, broadly aligning with the UK Age Appropriate Design Code. Additional limitations would apply around direct marketing to children, and targeting children. Further guidance and consultation around protecting the vulnerable is also recommended.

3. Regulation and enforcement

The third section of the Report proposes some important changes to regulation and enforcement:

- **Regulator enforcement powers:** expand the powers of the OAIC to investigate breaches of civil penalty provisions and provide them with the power to undertake public inquiries and reviews. This would include powers to search premises, make copies of documents specified in a warrant and seize evidential matter. Empower the OAIC to require respondents to complaints to take action to identify, mitigate and redress actual or foreseeable loss suffered by an individual in the event of an interference with privacy. The OAIC should also have the power to undertake public reviews and inquiries as approved or directed by the Attorney-General.
- **Penalties:** amend the recently-updated civil penalty provisions of the Privacy Act to remove the word "repeated" and clarify what is a "serious" interference with privacy that could attract those penalties up to the (potentially very high) maximum limit specified in the legislation. A "serious" interference would involve: sensitive information or other information of a sensitive nature; adverse effects for a large number of individuals; impacts for people experience vulnerability; repeated breaches; wilful misconduct; and/or serious failures to take proper steps to protect personal information. Additionally, widen the range of penalties available for breach of the Privacy Act by introducing:

- a new **mid-tier civil penalty** provision for interferences with privacy that do not have a "serious" element, but which may nevertheless attract Court-imposed remedies such as pecuniary penalties, conduct and compensation orders; and
- a **low-level civil penalty** provision allowing the OAIC to issue infringement notices for administrative breaches of the Privacy Act, such as failure to have a clearly expressed and up-to-date privacy policy.

- **Other remedies:** give courts flexibility to make any orders they find appropriate after a contravention of civil penalty provision has been established. Additionally, introduce:
  - a **direct right of action** for individuals and representative proceedings for classes of individuals to seek relief from an alleged interference with their privacy; and
  - a **statutory tort** for serious invasions of privacy which fall outside of the Privacy Act.
- **Notifiable data breach scheme:** amend the scheme to require entities to:
  - notify the Commissioner of an eligible data breach within **72 hours after becoming aware**, and notify individuals whose information is affected as soon as practicable, (information could be provided in phases if not all details are immediately available);
  - take reasonable steps to implement practices, procedures and systems to respond to data breaches; and
  - notify of additional matters, being the steps that the entity has taken or intends to take to respond to a breach including, where appropriate, steps to reduce any negative impacts on affected individuals.

With thanks to Fletcher O'Connor (Associate), Emily Notowidjojo (Seasonal Clerk), Anton Nguyen (Associate) and Liz Grimwood-Taylor (Senior Knowledge Lawyer) for their input to this alert.