PRIVACY

Australian privacy legislation is undergoing major legislative reform and directors need to know how to govern privacy risks within their organisations, writes Annelies Moens FAICD, managing director of cybersecurity and privacy consultancy Privcore.

MINDING YOUR OWN BUSINESS

Significant new avenues for compensation for individuals who have experienced privacy breaches have been proposed, with a direct right of action and, separately, a statutory tort for privacy recommended by the Attorney-General Department's *Privacy Act Review*, which was released in February.

The report follows on from recent amendments to the *Privacy Act 1988*, which came into force on 13 December 2022 with the *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022*. Those amendments have increased regulatory enforcement powers and penalties for serious interferences with privacy. For body corporates, the maximum penalty is the greater of:

- $50 million
- Three times the benefit received from the breach
- Where there is a benefit, but it cannot be determined, 30 per cent of revenue (minimum 12 months – maximum for the length of the breach activity).

These penalties are now among the highest in the world for serious interferences with privacy and also apply to overseas entities doing business in Australia. Serious interferences with privacy would likely include:

- Mishandling of sensitive personal information
- Adverse effects on large groups of individuals
- Impacting people experiencing vulnerability
- Repeated breaches
- Wilful misconduct
- Failure to take proper steps to protect personal information.

Further civil penalty regimes (mid and low-tier) are also proposed under the *Privacy Act Review* to deal with less serious interferences with privacy.

The newly enacted penalty regime (for serious breaches), the further civil penalty regimes (for less serious breaches) and the direct right of action – once updated legislation is passed – will apply in the context of significantly strengthened *Privacy Act* provisions. Funding for increased litigation costs and industry funding of the Office of the Australian Information Commissioner (OAIC) are proposed to be further investigated.

There are 116 proposals to strengthen and clarify the *Privacy Act*. Key changes directors need to be aware of are discussed below.

Legislating regulator interpretation and guidance

Cornerstone definitions, namely the definition of "personal information" and "consent" are proposed to be updated in the *Privacy Act*.

1 *Personal information*

It is proposed that the OAIC's broad interpretation of the definition of personal information outlined in its guidance be legislated and the definition accordingly clarified in the updated *Privacy Act*. That interpretation had been successfully challenged in court proceedings in 2017 in *Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4*, creating much uncertainty.

The proposed amendments intend to make clear that technical information – including IP address, device identifiers, location, online identifiers and inferred or generated information relating to an identified or reasonably identifiable individual – are personal information and therefore regulated. This is particularly relevant in online and mobile contexts where significant amounts of technical personal information are collected. The clarification that inferred or generated information can be personal information impacts access requests, as people generally don't know what inferences are made or generated about them. As such, inferred information generally carries high privacy risks. A new right to seek explanation of the handling of one's personal information is also being proposed, which is likely to affect automated decision-making.

> ***Penalties are now among the highest in the world for interferences with privacy and also apply to overseas entities doing business in Australia.***

2 *Consent*

Current OAIC guidance advises that for consent to be valid it must be voluntary, informed, current and specific, with individuals also having capacity to consent. The report proposes to legislate the OAIC's interpretation. It also proposes that consent needs to be unambiguous, supporting OAIC guidance that "an APP (Australian Privacy Principle) entity cannot infer consent simply because it provided an individual with notice of a proposed collection, use or disclosure of personal information. It will be difficult for an entity to establish that an individual's silence can be taken as consent" (APP Guidelines B40–B42).

Consent is relevant to the collection of sensitive personal information, use/disclosure for secondary purposes and as a basis for cross-border data flows. Consent is also proposed to be required for the handling of precise location information. Changes to targeted and direct marketing relying on opt-out consent are discussed below.

Strengthened requirements

1 *Data retention and breaches*

In the wake of the Optus and Medibank data breaches in late 2022, affecting millions of Australians, specific proposals focus on data retention periods and data breach reporting time frames. Maximum and minimum retention periods for storing personal information are proposed to be required in privacy policies. In the author's view, this should help organisations steer away from indefinite data retention towards data minimisation, and consider at the outset end-of-life-cycle destruction or de-identification parameters. Where information is de-identified, it is also proposed that entities should take reasonable steps to protect that information. Other laws currently requiring the retention of personal information are proposed to be reviewed to minimise the voluminous retention of personal information.

Notification of eligible data breaches to the OAIC are proposed to occur within a 72-hour time frame where the organisation is aware there

are reasonable grounds to believe an eligible data breach has occurred. Where organisations only suspect an eligible data breach, they still have 30 days to conduct an assessment to determine whether there are reasonable grounds to believe an eligible data breach has occurred.

2 *Fair and reasonable handling of personal information*

A new fair and reasonable objective test is proposed for the collection, use and disclosure of personal information at the outset, regardless of consent. This is intended to make organisations more accountable for the handling of personal information. Other measures, such as mandatory privacy impact assessments for high-risk privacy activities, will also assist in increasing organisational accountability. This is already required of Australian government entities.

Specific proposals relating to the handling of children's personal information and direct marketing, targeting and trading are also proposed. The proposed fair and reasonable test would require organisations to have regard to the best interests of the child in handling children's personal information. For example, direct marketing and targeting of children would be prohibited unless it is in their best interests. Notices and privacy policies would need to be clear and understandable where children's personal information is handled. A new children's privacy code – aligned with the UK Age Appropriate Design Code – is proposed for online services that children are likely to access.

3 *Direct marketing and targeting*

Opt-out requirements are proposed for targeting (in addition to the current direct marketing opt-out requirements). Targeting would include handling personal information, de-identified and unidentified information for the purposes of tailoring the likes of services and advertisements. This would likely mean online targeting (such as through cookies) would require either opt-in or opt-out consent, depending on whether personal information is involved.

4 *Individual rights*

A number of new individual rights are proposed, including a right to seek explanation as to how one's information is handled and from where it was obtained. Organisations will therefore need to maintain records from where they collect personal information, particularly where it is not collected directly from the individual concerned. Individuals are also proposed to be given rights to object to the handling of their personal information, rights to erasure and the de-indexation of internet search results in certain circumstances.

> ***Maximum and minimum retention periods for storing personal information are proposed to be required in privacy policies. This should help organisations steer away from indefinite data retention towards data minimisation.***

5 *International alignment*

While the recently amended *Privacy Act* and current proposed substantive changes are occurring in the wake of the Optus and Medibank data breaches, they have been in train for several years.

A backdrop to the review has involved international alignment. To that effect, current exemptions are proposed to be narrowed or removed entirely. Critically, the small business exemption is proposed to be removed, which affects about 95 per cent of Australian businesses. The employee record exemption for the private sector is also expected to be narrowed significantly. A controller and processor distinction as used in the EU General Data Protection Regulation is also proposed for the first time, introducing a level of complexity into the *Privacy Act*, which needs to be carefully considered. ■