Privacy108
We Protect Privacy

PO Box 3295
Yeronga QLD 4104
Level 12, 259 Queen St
Brisbane QLD 4000

Submission to the Senate Standing Committee on Legal and Constitutional Affairs regarding the *Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022*

Thank you for the opportunity to make submissions in response to the draft ***Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022***

The Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 would amend three Commonwealth Acts to:

- increase penalties for serious or repeated interferences with privacy,
- enhance the Australian Information Commissioner's enforcement powers, and
- provide the Australian Information Commissioner and the Australian Communications and Media Authority with greater information sharing powers.[1]

We note that this Bill has been introduced, following earlier discussion papers considering more comprehensive reform of the Australian Privacy Act. It is our submission that any amendments to the Privacy Act only be made as part of the comprehensive reforms that have been under consideration by the Australian government for three years. Privacy 108 and many others have invested significantly in the review and submission of feedback on those proposed reforms.

Changes to penalties and the powers of the Office of the Australian Information Commissioner (OAIC) as proposed in the Bill should be just one part of the complete overhaul that is required to bring Australia's privacy laws into line with both community expectation as to the level of protection that should be afforded to their personal information, and international standards.

We are strongly of the view that these changes should be implemented together with the other amendments as foreshadowed in the *Privacy Act Discussion Paper 2021*.

Information policy

We noted in our response to the *Privacy Act Discussion Paper 2021* that there was much activity in the space of information processing, digital platforms and regulation of on-line behaviours. Some of this activity included:

- Department of Home Affairs current consideration of Improving cyber security practices by a range of measures including mandatory codes of practice;
- Allowing law enforcement greater and easier access to data including encryption back doors and co-operation with foreign governments (e.g. the recent CLOUD agreements)

[1] Explanatory Memorandum, 1.

- Increasing the ability for sharing of personal data between government agencies via Data Sharing legislation;
- Increasing the ability to share consumer data but only in limited industry sectors via the Consumer Data Rights program;
- Targeting digital platforms in specific areas, such as paying for news content and anti-trolling but not others;
- Increasing the security obligations of critical infrastructure providers;
- Considering laws to target ransomware.

At the same time, we continue to see seeing growing concern around the use of facial recognition technology, ad tech, dark patterns and artificial intelligence.

It was our view at the time, and even more so now, some 12 months down the track, that it is difficult to provide a comprehensive response to the any proposed changes to Australia's privacy law without considering all relevant initiatives, together with the concerns already facing Australian businesses and people.

We strongly recommend that the government consider adopting a coherent, high level policy position covering information processing (from both a personal data protection and security lens) to help provide a strategic direction and clarity for Australian businesses and government agencies. This would help address the overlap and tensions between competition law, consumer protection, anti-discrimination and protection of privacy and other human rights, while supporting a vibrant, innovative economy and society. Without this high-level strategic direction, amendments to the Privacy Act will continue to be a game of catch up by Australia trying to keep pace with more agile, future focused nations who are able to leverage support for innovation and business, while at the same time respecting a deeply rooted understanding of the importance of the protection of personal data as a key tenet of their liberal democratic way of life.

OAIC funding

We submit that one of the most effective measures that could be taken to improve the way the personal information of Australians is collected, used, disclosed, stored, secured and disposed of is to increase and ensure the on-going sustained funding and resourcing of the OAIC.

The OAIC must have adequate funding, including high remuneration packages, to be able to attract and retain the skills and capabilities required for it to help steer covered entities through the complexities of privacy law and to develop a shared understanding and application of our Australian privacy principles between the regulator and the regulated community. Without the ability to effective exercise its powers, there is little point in providing or extending the powers of the OAIC.

Data Minimisation and retention

One of the most fundamental ways to reduce potential harm from events like the recent Optus Data Breach is to require entities to consider the data that they are collecting retaining, and the justification for that retention.

Although covered by APP 11, to date there has been little focus on the implementation of that principle by the OAIC, or clear statements as to what the office's compliance expectations are.

We recommend that data minimization be considered as a core stand-alone APP.

We also recommend that consideration be given to more prescriptive requirements for the retention of personal data. These might include requiring covered entities to identify, for the different categories of personal information that they collect and hold:

- The basis for retention;
- The retention period that applies;
- The extent to which the personal information can be pseudonymized or anonymized.

Whistle-blower protections

We have read and agree with the submission from the Australian Computer Society relating in to whistleblower protection. Cyber security professionals currently have no clear whistleblower protections, which gives no outlet for reporting corporate malfeasance safely and privately.

Existing whistleblower laws and mechanisms could readily be expanded to incorporate cyber security reporting.

Submissions on the Bill

Subject to the above, and our preference for the introduction of comprehensive reform, we are generally in favour of the proposed amendments.

However, we submit the following changes for consideration:

- Remove the limitation on penalties only applying to 'serious or repeated interferences with privacy'. Instead, leave it to the court to determine the appropriate penalty in the particular circumstances. The inclusion of this threshold is a barrier to the use of the power by the OAIC.
- Simplify the calculation of the new civil penalty, recognising that the benefits from a privacy interference will rarely be quantifiable.
- Increase the spectrum of enforcement mechanisms and penalty options available to the Information Commissioner, at least in line with the recommendations of the Privacy Act Review Discussion Paper.
- Introduce a provisions supporting the funding of the OAIC through an industry funding arrangement (as proposed in the Privacy Act Review Discussion Paper).
- Legislate a direct right of action allowing individuals to bring claims for breach of the *Privacy Act 1988*, so individuals have the option to directly purse recourse for interferences with privacy.
- Specifically recognise the right for class action suits based on a new individual right to sue, to help drive urgent improvement in the compliance landscape in Australia.

- Align the extra-territoriality provisions with those in Article 3(2) of the European Union General Data Protection Regulation to provide consistency between the privacy regimes of Australia and the EU and other jurisdictions.
- Require entities impacted by the proposed extra-territoriality provisions to have a local establishment or appoint an Australian representative (to support enforcement under the extended territoriality provisions).
- Include limitations around the right to share information, including notice to affected individuals, specific limitations on purpose of sharing and a specific time limit for retention.
- Give the Commissioner power to require the appointment of an independent adviser to report directly to the Commissioner, at the investigated entity's cost.

Please let us know if we can provide any clarification about our response.
Thank you for your consideration.

Yours Sincerely,

Dr Jodie Siganto CISSP, CISM, CIPM, CIPP/E, CIPT
CEO
E: