Committee Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600
legcon.sen@aph.gov.au

Privacy Legislation Amendment (Enforcement and other measures) Bill 2022 (Cth)

This submission responds to the Committee's invitation to comment on the *Privacy Legislation Amendment (Enforcement and other measures) Bill 2022* (Cth).

In summary, the Bill provides a belated and regrettably inadequate response to systemic weaknesses in Australian data protection law, evident in recent data breaches involving Optus, Medibank and Harcourt. It offers a foundation for community consideration of proposals for a large-scale updating of the *Privacy Act 1988* (Cth) and for a broader updating of privacy law in the other Australian jurisdictions, where we have an uneven and often moth-eaten patchwork of state/territory statutes and administrative protocols regarding information privacy (ie government data collection), surveillance devices and practices such as strip searches.

The Bill does not reflect overseas benchmarks regarding corporate and individual responsibility, for example the US Federal Trade Commission's recent requirement regarding Drizly's chief executive after a major data breach. Australia remains behind trading partners such as the European Union and United States.

The Bill does not address concerns regarding regulatory incapacity on the part of the Office of the Australian Information Commissioner (OAIC), a regulator with a defective corporate culture and inadequate resource base evident in for example a reluctance to take action or even to quickly acknowledge that the Optus breach was of concern.

There is little point giving powers to a watchdog that prefers to have a kip in its kennel rather than performing its duties by barking and biting, unlike the Australian Competition & Consumer Commission and overseas peers. Ongoing community disquiet about underperformance on the part of the OAIC is not addressed by the 'may' rather than 'must' approach in the Bill.

The Bill should be strengthened and regarded as a stop-gap ahead of large-scale rewriting of the 1988 Act (including establishment of a statutory cause of action for serious invasions of privacy) and concerted action by the Attorneys-General to ensure a coherent national privacy regime through uniform surveillance and other privacy law.

In particular the Bill should provide for a requirement that –

- commercial entities covered by the Privacy Act must have cyber-insurance, a requirement analogous to other business insurance
- public/private sector entities that have experienced a data breach must pay for replacement of passport, driver licence cards, credit cards and other identifiers
- public/private sector entities that have experienced a data breach must pay for 'credit watch' services for a period of two years

- reports by consultants about an entity's data handling framework must be provided to the OAIC and must be evaluated by the OAIC rather than treated as a tick-box exercise.

The Bill should also expressly authorise the sharing by the Office of the Information Commissioner of breach-related information with the Australian Competition & Consumer Commission (ACCC), consistent with the ACCC's responsibilities regarding 'digital platforms' and the need to move beyond the current balkanised regulatory framework.

Specific comments follow.

Basis

The submission reflects research and teaching over the past twenty years, including teaching graduate units on cybersecurity, consumer protection, public sector data management and privacy alongside chapters in a leading legal practitioner data protection resource and multiple scholarly publications.

The submission also reflects membership of OECD data protection working parties, participation in Internet Industry Association working parties and former membership of the Board of the Australian Privacy Foundation. (The submission is independent of the Foundation.)

The submission does not represent what would be reasonably construed as a conflict of interest.

Penalties

Penalties have two functions. They deter negligence or deliberate wrongdoing. They also signal to the community at large and to individual actors (executives, line officers, an organisation's competitors) that behaviour is inappropriate.

On that basis the penalty provisions in the Bill are inadequate. For large commercial entities the sums are likely to be regarded as an acceptable cost of doing business rather than a meaningful deterrent that is reflected in for example the departure of senior executives and in systemic improvement of information handling practice (such as implementation of a policy to not collect and store personal data 'just because we can').

The proposed penalty regime is particularly inadequate given the discretion given to the OAIC and that regulator's history of failing to use its soft and hard power, for example its

- failure to quickly condemn disregard of the Australian Privacy Principles (APP),
- history of interpreting the APP on a lowest common denominator basis and
- history of refraining from imposing penalties.

Unsurprisingly that ongoing failure is reflected in what the Explanatory Statement for the Bill refers to the community need for "reassurance" about the effectiveness of the OAIC and – just as saliently – inadequate prevention by leading corporations such as Optus and Medibank. Civil society disquiet, recurrent voiced over more than ten years, is exacerbated by the lack of information provided by the OAIC when that agency eventually reports on its investigation.

Enforcement powers

The Bill is commendable in providing the OAIC with enhanced enforcement powers, in particular amending the extraterritorial jurisdiction of the Privacy Act and new powers to

conduct assessments. Given the preceding comments a key issue is whether the OAIC will use those powers on a proactive and transparent manner, something that is a matter of its

- overall resourcing (inadequately addressed in budgets over the past ten years and in the stance by the then Attorney-General George Brandis that the Commission should be abolished because it was unnecessary),
- weak in-house expertise,
- corporate culture.

Observers can be forgiven for characterising it as a watchdog that is underfed, scared to emerge from its kennel and overly prone to licking the hand that grudgingly feeds it. As highlighted above, its underperformance compares badly with that of overseas peers and domestic regulators such as the ACCC.

The provision of new powers is accordingly welcome but only part of the solution in providing a national privacy regime that is fit for purpose in a world of pervasive data collection, big data analysis and institutional understandings that personal data – including data provided on a mandatory basis – is a matter of corporate ownership rather than custodianship.

Information sharing powers

The proposed information sharing provisions are commendable and serve to offset the incapacity noted above.

In building a more robust and citizen-centred privacy regime the OAIC should be expected to make the most of authorisation to publish a determination or information relating to an assessment on the OAIC website, providing guidance to other actors and importantly offering observers with a basis for evaluating the agency's operation. The latter is salient as a matter of public trust and as consequence of the OAIC's traditional resistance to scrutiny under the Freedom of Information (FOI) regime, ironic given the Freedom of Information Commissioner position within the OAIC but understandable given a former Public Service Commissioner's characterisation of FOI as "pernicious", a characterisation sadly not refuted by the OAIC.

Information seeking

Scope to issue an infringement notice for a failure to cooperate in an investigation under the Act is important and should be regarded as a matter of shaping expectations rather than merely allowing the Commissioner "to resolve matters more efficiently". On that basis the OAIC should be alert to opportunities to use the power.

Empowerment to require an entity to engage an independent suitably qualified adviser is a step forward, as is empowerment of the Commissioner to conduct an assessment of an entity's compliance with the Notifiable Data Breaches (NDB) scheme. Both provisions necessitate expertise on the part of the OAIC is the regulation is to be more than a tick-box exercise.

They also require timely and readily accessible disclosure regarding how the assessment was undertaken and what were the results, consistent with reference to providing "Australians with greater visibility of emerging privacy issues and whether an entity who holds their personal information has breached the Privacy Act".

The Explanatory Statement refers to ensuring the Commissioner has "comprehensive knowledge of the information compromised in an eligible data breach to assess the particular risk of harm to individuals". Importantly, the community – rather than merely the OAIC – needs that knowledge in order to mitigate harms such as identity theft, assess the

trustworthiness of the entity that failed to prevent the data breach, evaluate whether the entity needed to collect/retain/share data, and evaluate the performance of the OAIC.

Given that the OAIC includes the Information Commissioner and Freedom of Information Commissioner it is reasonable to expect the OAIC to adopt a proactive pro-disclosure philosophy.

Civil and criminal penalties

A preceding comment highlighted the inadequacy of penalties in the Bill, both in terms of scale (unlikely to deter a corporation such as Microsoft and Meta, particularly a corporation that will choose to 'out lawyer' the OAIC) and in terms of the broad discretion offered to the OAIC.

Penalties must be construed on a holistic basis. The proposed infringement notice provision in subsection 66(1) is a derisory $2,664 for a person and $13,320 for bodies corporate, with a maximum civil penalty of $13,320 for individuals and $66,600 for bodies corporate. Inadequate penalties reward rather than deter misbehaviour. We should be conscious that the real cost to individuals of data breaches (in terms of time and payment for replacement identity documentation) affects people who are underprivileged rather than merely those who are wealthy. We should also be conscious that the cost to a handful of those people will outweigh the penalty imposed under 66(1).

Establishment of a separate criminal offence under 66(1AA) is commendable. Given comments above regarding the inadequacy of the OAIC's corporate culture and the frustration experienced by civil society advocates in seeking a more responsive privacy regulator the Commissioner should be mindful of actively using the provision – and being readily *seen* to use the provision – to shape expectations.

As part of the Government's exploration of updating of the Privacy Act (as part of the current review of the Act) consideration should be given to reinforcement of the deterrent through disqualification of executives and a requirement – modelled on that evident in the FTC's 2022 response to the Drizly data breach – that private sector executives will be obligated to implement meaningful information security programs when they move to another corporation.

The preceding comments may strike some Committee members as disproportionate or unduly critical of a government agency. We can assume that officials are conscientious. That conscientiousness is not however the same as being effective in terms of meeting community needs and accountability. Privacy protection is of concern to ordinary Australians. It is a matter of individual and institutional cultures. Large-scale data breaches such as the recent Optus and Medibank instance are inevitable in cultures where organisations regard themselves as owners rather than custodians of personal information, inadequate thought is given to whether it is imperative to retain and store data, governments offer simplistic solutions such as mandatory 'digital identifier' schemes, regulators lack capacity and penalty regimes are inadequate to deter substandard data system design, implementation and remediation.

Dr Bruce Baer Arnold
Associate Professor, Law
University of Canberra

7 November 2022