Australian Government
Office of the Australian Information Commissioner

Our reference:

Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600

By email: legcon.sen@aph.gov.au

Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022

Dear Chair

Thank you for the invitation to make a submission to the Committee's inquiry into the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (the Bill).

The Office of the Australian Information Commissioner (OAIC) is an independent Commonwealth regulator, established to bring together three functions: privacy functions (protecting the privacy of individuals under the *Privacy Act 1988* (Cth) (Privacy Act) and other legislation), freedom of information functions (access to information held by the Commonwealth Government in accordance with the *Freedom of Information Act 1982* (Cth)), and information management functions (as set out in the *Australian Information Commissioner Act 2010* (Cth) (AIC Act)).

Businesses and government are collecting and holding an increasing amount of data in our modern economy, which is likely to increase as the digital economy grows. While this can enable innovation and economic growth, we have also seen several recent high-profile data breaches involving the personal information of millions of Australians and the resulting impacts this has had on the community.

It is essential that the Australian privacy framework provides the right regulatory tools to enable the OAIC to respond efficiently and effectively to privacy harms emerging through the digital environment and deter non-compliant behaviour. To that end, I welcome the targeted measures in the Bill that are being progressed ahead of the broader review of the Privacy Act, which will enhance the OAIC's ability to regulate in line with community expectations and protect Australians' privacy in the digital environment. I provide further comments about some of the key measures in the Bill below.

Extraterritorial operation of the Privacy Act

Currently, an overseas organisation must comply with the Privacy Act if the entity has an 'Australian link'.[1] An overseas organisation will have an Australian link if the organisation carries on business in Australia and it collects or holds personal information in Australia.

The Bill will remove the condition that an organisation has to collect or hold personal information in Australia, which will align the Privacy Act with the extraterritoriality provisions of the *Competition and Consumer Act 2010* (Cth) (Competition and Consumer Act).[2] This amendment will simplify requirements around the circumstances in which the Privacy Act extends to an act or practice of an organisation outside Australia and ensure consistency with other domestic legislative frameworks.

Increased penalties

The Bill will increase civil penalties for serious or repeated interferences with privacy to not more than the greater of: $50 million, three times the value of any benefit obtained through the misuse of the information, or if the value of the benefit obtained cannot be determined, 30 per cent of an entity's domestic turnover in the relevant period.

The increased penalties will mirror recent increases to the maximum penalties under the Competition and Consumer Act that were introduced through the *Treasury Laws Amendment (More Competition, Better Prices) Act 2022* (Cth).[3] This will ensure penalties under the Privacy Act are comparable with those of other domestic and international regulators. The OAIC welcomes the increased penalties which will help to incentivise compliance and ensure that penalties for privacy breaches act as a deterrent and are not seen merely as the cost of doing business in Australia.

Notifiable data breaches scheme

The Notifiable Data Breaches (NDB) scheme commenced in February 2018 and introduced new obligations for Australian Government agencies and private sector

[1] See s 5B(2) of the Privacy Act.

[2] See s 5 of the Competition and Consumer Act which sets out the circumstances in which the Act extends to conduct outside of Australia.

[3] At the time of writing, the *Treasury Laws Amendment (More Competition, Better Prices) Act 2022* had passed both Houses on 27 October 2022 but was awaiting Royal Assent.

organisations that have existing information security obligations under the Privacy Act.[4]

The NDB scheme requires regulated entities to notify individuals and the OAIC about eligible data breaches. A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates.[5]

The key objective of the NDB scheme is to enable individuals whose personal information has been compromised in a data breach to take remedial steps to lessen the adverse impact that might arise from the breach. By arming individuals with the necessary information, they will have the opportunity to take appropriate action, such as monitoring their accounts and credit reports or taking preventative measures such as changing passwords and cancelling credit cards.[6]

The NDB scheme also serves the broader purpose of enhancing entities' accountability for privacy protection. By demonstrating that entities are accountable for privacy, and that breaches of privacy are taken seriously, the NDB scheme works to build trust in personal information handling across the private and public sectors.

The OAIC currently has limited ability to compel the provision of additional information from notifying entities under the NDB scheme. For example, if an entity provides general or limited information about the kind or kinds of information involved in the breach, the OAIC does not have the ability to compel an entity to provide more detailed information. Similarly, the OAIC does not currently have the power to require the production of information or a document in circumstances where an entity is yet to notify, but where the OAIC may have reasonable grounds to suspect that there has been an eligible data breach (for example, through media reports or a tip-off).

The Bill will provide new information-gathering powers under the NDB scheme in relation to actual or suspected data breaches which will help to ensure the OAIC has a comprehensive knowledge of the information compromised in a breach, and other relevant facts and circumstances, to assess the particular risk of harm to individuals, and whether the recommendations about the steps that individuals should take in response to the eligible data breach outlined in a notification are sufficient. The ability to require the production of information will also help to inform whether a direction to notify should be issued under s 26WR of the Act.

---

[4] The NDB scheme is contained in Part IIIC of the Privacy Act.

[5] See s 26WE(2) of the Privacy Act.

[6] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016, pg 9.

Under s 33C of the Privacy Act, the OAIC may also conduct assessments of Australian Privacy Principle (APP) entities about whether personal information they hold is being maintained and handled in accordance with the APPs. The OAIC conducts assessments to facilitate legal and best practice compliance by identifying and making recommendations to address privacy risks and areas of non-compliance.[7]

The Bill will expand existing privacy assessment powers to enable the OAIC to assess an entity's compliance with the NDB scheme including the extent to which the entity has processes and procedures in place to assess suspected eligible data breaches and provide notice of eligible data breaches to the OAIC and to individuals at risk of serious harm. Privacy assessments are a valuable regulatory and educative tool to help identify and mitigate emerging privacy issues.

Information-sharing

Domestic and international collaboration is a key part of the OAIC's regulatory toolkit.[8] To ensure that the OAIC can efficiently and effectively cooperate with other regulators and entities during investigative and regulatory activities, it is critical that relevant information can be shared without unnecessary limitations. Currently, s 29 of the AIC Act provides that information may only be recorded, disclosed or otherwise used in the course of performing the same functions or exercising the same powers as those in the course of which the information was acquired.

This complicates sharing information and cooperating with other regulators or law enforcement bodies during the course of exercising functions. The Bill will provide clear circumstances in which the Commissioner may share information with other bodies where necessary, including law enforcement bodies, an alternative complaint body and State, Territory or foreign privacy regulators.

These measures will help to ensure that duplicative investigation and regulatory responses – both domestically and globally – are avoided and limited resources are directed appropriately.

---

[7] See the OAIC's *Guide to privacy regulatory action* at https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action

[8] For example, in November 2021, the OAIC and the UK's Information Commissioner's Office (ICO) concluded a joint investigation into the personal information handling practices of Clearview AI Inc. The investigation focused on the company's use of data scraped from the internet and the use of biometrics for facial recognition. The ICO and OAIC were recently awarded a Global Privacy Assembly Privacy and Data Protection Award in the Dispute Resolution and Enforcement Category for the joint investigation into Clearview.

More broadly, it is important to ensure that Australians are informed about privacy issues and reassured that the OAIC is discharging its duties.[9] The measures in the Bill will provide the clear authority to, amongst other matters, publish information such as an update about an ongoing privacy investigation or whether my office has been notified of a data breach, if it is in the public interest to do so.

Privacy Act Review

The Government's ongoing review of the Privacy Act is intended to ensure that our privacy framework empowers consumers, protects their data and best serves the Australian economy. The OAIC has engaged closely with the review since its commencement in 2020 and we have made two substantial submissions to the Attorney-General's Department with over 180 recommendations for reform designed to strengthen the privacy framework to prevent harms to individuals and that benefit the community and economy overall.[10]

Wider reform through the Privacy Act review is necessary to ensure that this framework is proportionate, sustainable and responsive to emerging privacy risks into the future. The OAIC will continue to work closely with the Attorney-General's Department as it develops its final report to Government this year.

Yours sincerely

Angelene Falk
Australian Information Commissioner
Privacy Commissioner

7 November 2022

[9] Explanatory Memorandum, Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022, pg 17.

[10] See the OAIC's Privacy Act Review – Issues Paper submission and Privacy Act Review – Discussion Paper submission.