Australian Government
Attorney-General's Department

November 2022

Submission to the inquiry into the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022

Senate Legal and Constitutional Affairs Legislation Committee

Introduction

The Attorney-General's Department (the department) provides the following submission to the Senate Legal and Constitutional Affairs Legislation Committee on the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (the Bill) in response to the Committee's invitation dated 28 October 2022.

Overview of the Bill

The Bill amends the *Privacy Act 1988* (Privacy Act), the *Australian Information Commissioner Act 2010* (AIC Act) and the *Australian Communications and Media Authority Act 2005* (ACMA Act). The Bill includes amendments to increase penalties under the Privacy Act, provide the Australian Information Commissioner (the Commissioner) with greater enforcement powers, and provide the Commissioner and the Australian Communications and Media Authority (ACMA) with greater information sharing powers.

The Bill is being introduced now to address the more pressing issues arising from recent serious data breaches and cyber incidents, which have the potential to cause serious financial and emotional harm to Australians. The Bill promotes the need for robust privacy, security and data protection.

Increasing maximum penalties for a serious or repeated breach of privacy will incentivise entities to take strong privacy and cyber security measures to protect the personal data they hold. Setting these penalties at a higher level will accord with Australian community expectations about the importance of protecting their personal data. Higher maximum penalties will be complemented with a range of enhanced enforcement powers to equip the Commissioner with the tools necessary to take effective and efficient enforcement action where necessary, and greater information sharing powers to ensure regulators are able to work together to take prompt action in relation to data breaches to minimise harm to Australians.

As part of the October 2022-23 Budget, the Government provided an additional $5.5 million over two years to the Office of the Australian Information Commissioner (OAIC) to support the OAIC to respond to the Optus data breach (including undertaking an investigation). The Government also confirmed funding of $17 million over two years to support the OAIC respond to the increasing complexity of privacy complaints, and take effective enforcement action and litigation.

The Bill is the first step in the Government's agenda to ensure Australia's privacy framework is fit for purpose, and responds to new challenges in the digital era. The department's review of the Privacy Act (Privacy Act Review), which will report to the Attorney-General by the end of this year, will recommend further reform proposals to ensure Australia's privacy framework protects the personal information of Australians, supports an innovative economy and responds to new challenges in the digital age. Broader proposals, including measures to address the amount of personal information entities are collecting and how they are storing it, will be considered by the Privacy Act Review. It is appropriate that these reforms be considered holistically in this process given the range of complex and interconnected issues and other work across Government.

Penalties

To adequately protect Australians' personal information and promote effective deterrence, the Bill will increase maximum penalties under section 13G of the Privacy Act for a serious or repeated breach of privacy.

The maximum penalty for a body corporate will increase from a maximum of 2,000 penalty units (which is currently $2.22 million for a body corporate) to an amount not exceeding the greater of:

- $50 million:
- three times the value of any benefit obtained, or
- if the value of the benefit cannot be determined—30 per cent of a body corporate's adjusted turnover in the relevant period.

The maximum penalty for a person other than a body corporate will increase from a maximum of 2,000 penalty units (which is currently $444,000 for a person other than a body corporate) to a maximum penalty of $2.5 million.

Setting the maximum for these penalties at a higher level will accord with Australian community expectations about the importance of protecting their personal data, and will create strong incentives for entities to meet their existing obligations under the Privacy Act. Australian Privacy Principle 11 (APP 11) requires entities to take reasonable steps to protect personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. The type of steps that are reasonable to protect information will depend on the circumstances of the entity and the risks associated with personal information handled by the entity. Under APP 11, entities must also take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs.

These penalties will also mirror the recently increased Australian Consumer Law penalties under the *Treasury Laws Amendment (More Competition, Better Prices) Act 2022*. The Australian Competition and Consumer Commission's 2019 Digital Platforms Inquiry Final Report (DPI Report) recommended that the maximum penalties under the Privacy Act should be increased to mirror the penalties for breaches of the Australian Consumer Law as the lack of effective deterrence has enabled problematic data practices.

The increase in maximum penalties will be comparable to penalties in some other privacy frameworks. For example, the European Union's General Data Protection Regulation has a maximum penalty of €20 million or 4 per cent of a company's annual *global* turnover, whichever is higher. This has led to significant fines against large digital platforms, including a €746 million (AUD $1.15 billion) fine against Amazon, €405 million (AUD $626 million) fine against Meta Platforms, €225 million (AUD $348 million) fine against WhatsApp and €90 million (AUD $139 million) fine against Google.

Although the Bill proposes to increase the maximum penalties that can apply under the Privacy Act, a court would retain discretion to determine a penalty which is appropriate and proportionate to the seriousness of the misconduct and harm or potential harm. The court may consider factors such as the nature and extent of the contravening conduct, the damage or loss suffered, the size of the contravening entity and whether the entity has previously been found to have engaged in similar conduct.

As outlined in the OAIC's Privacy regulatory action policy, the OAIC's preferred regulatory approach is to facilitate voluntary compliance with privacy obligations and to work with entities to ensure best privacy practice and prevent privacy breaches. However, where a breach is particularly egregious, it is important that as part of the range of regulatory options available there is an option for penalties of sufficient magnitude to be available and considered.

Enforcement powers

The increase in maximum penalties will be complemented with a suite of new enforcement tools to ensure the Commissioner is able to effectively regulate when it is appropriate to do so. The Bill proposes new enforcement powers that include:

- expanding the types of declarations the Commissioner can make in a determination following a privacy investigation to:
    - require entities to publish notices about specific breaches of privacy or otherwise ensure those directly affected are informed
    - require entities to undertake external reviews to improve their practices to reduce the likelihood of them committing a breach again
- providing the Commissioner with new information-gathering powers to conduct assessments, and
- providing the Commissioner with new infringement notice powers to penalise entities for failing to provide information without the need to engage in protracted litigation.

To ensure the Privacy Act is fit for a global and digital world, the Bill will also amend its extraterritorial jurisdiction to ensure foreign organisations that carry on a business in Australia must meet the obligations under the Privacy Act, even if they do not collect or hold Australians' information directly from a source in Australia. With the evolution of technology, it can be difficult to establish that foreign organisations collect or hold personal information directly from Australia – for example, they may collect personal information from a digital platform that does not have servers in Australia, and transfer it to other entities overseas for processing and storage.

Strengthened Notifiable Data Breaches scheme

To ensure organisations are not falling short of the Notifiable Data Breaches scheme's requirements, which reduces opportunities for an individual to take steps to protect themselves following a data breach, the Commissioner would be empowered to undertake an assessment of an entity's compliance with the scheme's requirements, and provided new information-gathering powers to assess suspected or actual breaches.

Information sharing powers

To ensure Australians are informed about privacy issues and to promote effective regulation, the Bill will enhance the Commissioner's ability to share information, subject to certain requirements.

The Commissioner will have an express power to disclose information relating to determinations and assessments. For all other privacy information, such as information about ongoing investigations, the Commissioner may disclose that information if the Commissioner is satisfied it is in the public interest to do so.

The Commissioner will also be able to share information with enforcement bodies, alternative complaint bodies and privacy regulators for the purpose of the Commissioner or the receiving body exercising their functions and powers. The Bill will permit the Australian Communications and Media Authority to share information with any non-corporate Commonwealth entity responsible for enforcing a Commonwealth law where the information will enable or assist the entity to perform or exercise any of its functions or powers.

These powers will allow greater cooperation between regulators – for example, greater cooperation between the OAIC and the Australian Communications and Media Authority which have similar remit in regards to data.

Privacy Act Review

The DPI Report recommended broad reform of Australia's privacy framework to ensure it continues to effectively protect consumers' personal information in light of the increasing volume and scope of data collection in the digital economy. The terms of reference for the Privacy Act Review include consideration of:

- the scope and application of the Privacy Act
- whether the Privacy Act effectively protects personal information and provides a practical and proportionate framework for promoting good privacy practices
- whether individuals should have direct rights of action to enforce privacy obligations under the Privacy Act
- whether a statutory tort for serious invasions of privacy should be introduced into Australian law
- the impact of the notifiable data breach scheme and its effectiveness in meeting its objectives
- the effectiveness of enforcement powers and mechanisms under the Privacy Act and how they interact with other Commonwealth regulatory frameworks
- the desirability and feasibility of an independent certification scheme to monitor and demonstrate compliance with Australian privacy laws.

The department commenced the Privacy Act Review on 30 October 2020 and has undertaken a range of consultations and received many submissions on a broad range of reform ideas spanning the scope and application of the Privacy Act. The department is scheduled to complete the review and report to the Attorney-General by the end of this year.