



**Making privacy core business**

**The shape of things to come:  
Review of the Australian Privacy Act  
Status at 22 November 2022**



**Privcore Pty Ltd**

ACN: 167 388 178

ABN: 46 167 388 178

Email: [operations@privcore.com](mailto:operations@privcore.com)

Website: [www.privcore.com](http://www.privcore.com)

Address: Level 14, 5 Martin Place, Sydney NSW 2000, Australia

## Data breaches accelerate review of the Australian Privacy Act

Between September and October 2022, Australia experienced two of its worst data breaches, with the [Optus](#) and [Medibank](#) data breaches each exposing the personal information of almost half of Australia's population. This included highly valuable and sensitive data including identity and health information.

During Parliamentary sitting weeks in October and November 2022, the Government reacted almost immediately to those breaches with a [privacy bill](#) and [telecommunications regulation](#) amendments. Let me take a step back before taking you through the current state of play.

The Australian Competition and Consumer Commission's (ACCC) Digital Platform Inquiry catalysed the [current review of the Privacy Act](#). The review commenced in October 2020 through the release by the Attorney-General's Department (AGD) of an Issues Paper. After 166 submissions to the Issues Paper, the Department released a Discussion Paper in October 2021, which attracted 207 submissions. Since early this year, Australians have been waiting on the final report outlining the recommended changes to the Privacy Act.

That report was further delayed due to the Government having to consider quickly how to respond to the Optus and Medibank data breaches, which have undermined Australia's security globally through the exposure of a significant portion of its population's identity information.

This means changes to the Privacy Act will occur in stages. The first stage of changes affect six key areas, each discussed in turn:

- 1) Substantially increasing penalties for serious or repeated interferences with privacy
- 2) More practical options for the Office of the Australian Information Commissioner (OAIC) to deal with persons refusing or failing to provide information
- 3) Expanding the OAIC's information sharing powers
- 4) Expanding information gathering powers and assessments under the Notifiable Data Breach scheme
- 5) Clarifying the extra-territorial application of the Privacy Act
- 6) Clarifying types of declarations in determinations

### **Substantially increasing penalties for serious or repeated interferences with privacy**

The substantial increase in penalties in the Privacy Act are intended to line up with recently enacted increased penalties in the Australian consumer law, which received Royal Assent

on 7 November 2022 (the [Treasury laws amendment \(more competition, better prices\) Act 2022 \(Cth\)](#)). For body corporates the maximum penalty is the greater of:

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

For non-body corporates the maximum penalty is \$2.5M.

Relevant revenue will be based on definitions in the [A New Tax System \(Goods and Services Tax\) Act 1999 \(Cth\)](#), particularly any revenue that falls within supplies made by the body corporate and related body corporates and revenue that falls within the indirect tax zone.

### **More practical options for the OAIC to deal with persons refusing or failing to provide information**

The bill repeals the criminal penalty provisions for refusing or failing to provide information or to answer a question or produce a document or record. It is replaced with a civil penalty provision. A new criminal penalty is reserved for refusing or failing to provide information or to answer a question or produce a document two or more times. A new infringement notice power for the OAIC is also introduced, which enables the OAIC to impose non-criminal penalties and thus does not require the OAIC to refer the matter to the Commonwealth Director of Public Prosecutions.

### **Expanding the OAIC's information sharing powers**

The OAIC has had Memoranda of Understanding with a number of regulators, including the UK Information Commissioners Office, Personal Data Protection Commission Singapore, ACCC, ACMA, Inspector-General of Intelligence and Security, the Australian Digital Health Agency and [so forth](#).

The Bill seeks to expand information sharing powers to include the sharing of personal information and broadens the scope of entities with whom the OAIC can share information, including the eSafety Commission. The sharing can only occur in line with exercise of powers and functions and must be in the public interest.

### **Expanding information gathering powers and assessments under the notifiable data breach scheme**

A new section to enable the OAIC to gather information to assist it assess risks of harm to individuals whose personal information may have been compromised, regardless of whether it has been notified or not under the notifiable data breach scheme. The Bill also proposes that the OAIC be given an additional assessment power with respect to assessing

compliance with the notifiable data breach scheme. When information is not provided, then the OAIC can issue infringement notices as set out above.

### **Clarifying the extra-territorial application of the Privacy Act**

The bill clarifies that organisations that do not collect or store personal information directly from Australia are still bound by the Act where they carry on business in Australia. Privcore views this amendment as a pre-emptive measure to ensure that should the High Court of Australia find in favour of Facebook Inc USA's argument, that it is not bound by the Australian Privacy Act, that any such precedent would be overridden by this change in the Privacy Act.

### **Clarifying types of declarations in determinations**

The bill provides the OAIC with powers to instruct respondents in determinations to publish statements about their conduct, engage independent advisors to review conduct the subject of complaint, and provide reviews to the OAIC.

### **Next steps**

On 27 October 2022, this first tranche of amendments to the Privacy Act was sent to the Senate Legal and Constitutional Affairs Legislation Committee (the Committee) for inquiry. Thirty-two written submissions were [published](#) and public [hearings](#) were held on 17 November 2022. On 22 November 2022, the Committee tabled its [report](#) recommending the Bill be passed subject to two recommendations to be considered as part of the broader privacy law reform process. The first relates to extra-territoriality and ensuring that the legislative remit extends to foreign entities only in relation to Australians' personal information. The second is in relation to defining the terms 'serious' and 'repeated interferences' of privacy within the legislation, rather than in OAIC guidance materials.

It is expected the Bill will commence the day after it receives Royal Assent.

Towards the end of 2022, the AGD intends to release its final report recommending further changes to the Privacy Act. There are ~67 proposals for change tabled in AGD's Discussion Paper. Privcore has [summarised](#) those that have attracted the most comments from business. The Committee's report also considers focus should be given particularly to data minimisation, safe harbour mechanisms, compensation for harms and the introduction of a statutory tort of privacy.

Please note that Privcore provides privacy risk management advice, not legal advice.

## About Privcore

Privcore's team with over 40 years' combined experience helps business and government make privacy core business, so they can deliver services with the trust and confidence of customers and citizens. Privcore conducts privacy impact assessments, privacy health checks or audits, data breach prevention and recovery, privacy by design, builds privacy programs, provides advice, policies and conducts research into privacy and cybersecurity.

Annelies Moens, CIPP/E, CIPT, FIP, FAICD, CMgr FIML, a Superstar of STEM in 2021-2022 and a privacy professional practising since 2001 founded Privcore. She has led and conducted hundreds of privacy consulting deliverables globally. She is a former President of the International Association of Privacy Professionals which she co-founded in Australia and New Zealand in 2008. She has been instrumental in shaping and building the privacy profession in Australia and New Zealand and influencing privacy developments in APEC. She also has extensive privacy regulatory experience and resolved hundreds of privacy complaints whilst working at the Australian privacy regulator.



“My role is to protect one of the most valuable and vulnerable resources in the world - information about people.”

ANNELIES MOENS  
Privacy expert

Science & Technology AUSTRALIA

SUPERSTARS OF STEM