

October 2023

UPDATE

Summary: Government response to Privacy Act Review Report

1. Government Response | Privacy Act Review Report

On 28 September 2023 the Federal government issued the [Government Response \(Response\)](#) to submissions received on its [Privacy Act Review Report](#).

The government responded to each proposal with “agrees”, “agrees in-principle” or “noted” stating that it intends to release draft legislation and undertake “targeted consultation” in relation to matters where it “agrees”. The designation “agrees in principle” indicates that the items will proceed “subject to further engagement with regulated entities and a comprehensive impact analysis...” It appears that matters noted will go no further.

The most important changes in each category are summarized as follows:

Agrees

Regulation of PI collected from children and the vulnerable

A child will be defined as an individual who has not reached 18 years of age. There will be a Children’s Online Privacy Code that applies to online services “likely to be accessed by children”. The OAIC will update guidance on capacity and consent to reflect developments in supported decision making.

Regulation of Journalism

The conditional exemption for journalism is to be subject to standards overseen by a regulator (to be determined).

New regulation of Automated decision making.

Privacy policies are to include a statement of the “types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on individual rights.” High level indicators of the types of decisions with a legal or similarly significant effect on individual rights will be included in the Act and supplemented by OAIC guidance. Individuals will have a right to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made.

A lower bar for collecting PI for research.

There will be a legislative provision that permits a broad consent to be granted by the data subject for her or his information to be used for research.

Enhanced security obligations

In APP 11.1 (relating to Data Security) “reasonable steps” will be defined to include technical and organizational measures. The OAIC is to enhance guidance on the reasonable steps that should be taken to secure personal information (PI), de-identify and destroy PI.

New regulatory powers

The Information Commissioner will have power to make binding codes. There will be tiers of penalty for breaches of the Act, including low-tier and mid-tier civil penalties.

A serious interference with privacy is to be defined to include:

- (a) those involving 'sensitive information' or other information of a sensitive nature
- (b) those adversely affecting large groups of individuals
- (c) those impacting people experiencing vulnerability
- (d) repeated breaches
- (e) wilful misconduct, and
- (f) serious failures to take proper steps to protect personal data.

The broad spectrum of investigation powers in Part 3 of the *Regulatory Powers (Standard Provisions) Act 2014* will be made available to the Information Commissioner.

On determining a complaint, the Commissioner will have power to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss. A power for the Federal Court and Federal Circuit court to make any order it sees fit in response to a privacy matter is to be added to the act. The Attorney general is to be given discretion to share information with the aim of reducing harm in event of a data breach.

Agrees in-principle

Changes to the scope of the Act

PI is to "relate to" (rather than be "about") an individual. Collection is to expressly cover PI that is "inferred or generated" and changes will provide clarity on the meaning of "reasonably identified" and "de-identified". "Sensitive information" is to expressly include genomic information and sensitive information that is inferred.

After further consultation the government will remove the small business exception and significantly narrow the employee records exemption. Data processors (with limited responsibility for compliance) will be introduced as a concept into the Act.

More regulation of PI.

Media organization are to be subject to media privacy standards to be developed by the OAIC, independent audit and review, record destruction obligations and mandatory data breach notification.

There is to be new generally definition of data subject consent including OAIC guidance. Regulated online organizations must adopt the "framework of the Act" as default privacy settings. Consent will be required to trade in PI (except trading in PI relating to children where it is to be banned).

Direct marketing to children will be prohibited unless the PI was collected from the child and is in the child's best interests. APP11 will be amended to require "baseline privacy outcomes."

New administrative obligations related to PI

Regulated organisations will be subject to an overarching requirement that collection, use and disclosure (including targeted advertising) must be "fair and reasonable in the circumstances" and will be required to

- More information must be included in APP5 collection notifications.

- conform privacy policies and collection notices to standardized templates, layouts and terminology.
- undertake a Privacy Impact Assessment for any activity with high privacy risks.
- ensure that PI not collected from the data subject was originally collected in accordance with APP3.
- make a record of the purposes for which PI is collected used and disclosed.
- designate a senior officer as “responsible for privacy” within the regulated entity.
- comply with administrative guidance to be issued on collecting PI from children including that collection notices be understandable by children and to “have regard to the best interest of the child.”
- provide information about targeted advertising including clear information about use of algorithms and profiling to recommend content.
- establish their own maximum and minimum data retention periods for PI.
- use standard contractual clauses for offshore data transfers.
- consider the risks of overseas disclosure of PI before sending it offshore.

Financial institutions to “act appropriately in the interest of customer who may be experiencing financial abuse or may not longer have the capacity to consent.” The government supports changes to the MDBN scheme to introduce a 72-hour time limit an ongoing disclosure and an obligation to advise data subjects of the steps they should take to reduce any adverse impact of the breach.

New individual rights

Data subjects are to receive a right to:

- Withdraw consent and a requirement to have default settings in line with the Act.
- Access to an explanation of their PI on request.
- Object to the collection and use of PI.
- Receive a written response with reasons, a right of erasure, extended right of correction.
- Have PI de-indexed from online search results.
- Receive “reasonable assistance” to exercise rights under the Act,
- Have a response to requests within a reasonable timeframe.
- Be informed regarding the kinds of PI that may be stored overseas.
- Opt-out of use or disclosure of PI for direct marketing.
- If their PI is to be stored offshore, be advised that privacy protection may not apply to them.
- Be notified of their rights at the point of collection.

Industry funding

“Investigation” of an industry funding model is agreed in principle. “Further consideration” of a contingency litigation fund a contingency against costs awarded against the OAIC is agreed in principle.

Direct rights of Action

The creation of a direct right of action of for interference with the privacy of an individual and statutory tort for a serious invasion of privacy are both agreed in principle.

“Noted”

It appears that the government does not intend to act on :

- Proposal to add protections for de-identified information.
- Proposals to prohibit re-identification of personal information from a source other than the individual concerned.

- Any of the proposals to regulate personal information collected and used by political organisations.

2. What will Generative AI do to legal practice?

Earlier this year, I was interviewed by the Sharon Givoni, the General Editor of the LexisNexis Internet Law Bulletin on the future of legal assistance considering the impact of generative AI. The article appears in 2023, Vol 25 No 9 of the Internet Law Bulletin. You can read a copy here:

[ChatGPT: The future of legal assistance? An interview with Patrick Fair](#)

3. Telecommunications Ambassador 2023.

I am delighted to share that I was made a Telecommunications Ambassador at the Annual ACOMM Awards Dinner. The award was said to be in recognition of years of work on telecommunications and internet related law and policy. The award was presented by the Minister for Communications the Hon Michelle Rowland MP and the CEO of Communications Alliance John Stanton:



Please contact me if you have any questions regarding the matters discussed in this update.
patrick@patrickfair.com 0411361534

You can subscribe to updates like this one at www.patrickfair.com