Is Your Business Using AI? What You Need to Know About the Proposed Changes to Privacy Laws in Australia

Simone Basso
Associate, HWL Ebsworth Lawyers

The use of Artificial Intelligence (**AI**) is increasing at a swift rate. Not only has AI become a part of everyday life, it has also been heavily relied upon by businesses to increase productivity in the workplace. In fact, studies have shown that approximately 35% of businesses world-wide are using AI.[1] This is expected to grow significantly in the next few years.

However, many have also wondered about the downfalls of relying upon this technology. One of the features of AI is that, in order to improve and evolve its decision-making abilities, it requires access to data, including personal data.[2] An AI model which has access to personal data raises important questions about security, protection and other risks associated with the use of that data.

Those concerns came to the forefront in global news following the release of ChatGPT in November 2022. Although some time has passed, generative artificial intelligence technologies, such as ChatGPT, remain a consistent theme in tech news. Businesses are clearly striving to find a competitive edge by using these technologies in new and innovative ways.

One of the most common questions raised is whether the privacy law regime in Australia is equipped to deal with issues which might arise by a business relying on AI tools to expedite outcomes.

Privacy law in Australia is governed by the *Privacy Act 1988* (Cth) (**Privacy Act**).

On 16 February 2023, the office of the Attorney-General published the Privacy Act Review Report (**Report**). This Report proposed 116 reforms to the Privacy Act which were aimed at strengthening the protection of personal information and providing individuals with better control over their personal information. On 28 September 2023, the Australian Government published its response to the Report (**Response**).

More recently, on 12 September 2024, the House of Representatives tabled the *Privacy and Other Legislation Amendment Bill 2024* (**the Bill**). We will address below the potential changes to the privacy law regime, and how they may impact upon the obligations that a business will need to consider when using generative AI.

But first, what is generative AI?

What is Generative Artificial Intelligence?

Generative artificial intelligence is a type of technology which collects and processes information for the purposes of interacting with users in a responsive and conversational manner. The dialogue format makes it possible for it to answer follow-up questions, challenge incorrect premises, reject inappropriate requests, and even admit mistakes.[3] ChatGPT is an example of generative AI.

What are the proposed changes to the Privacy Act and how are they relevant to the use of generative AI?

In its Report, the office of the Attorney-General made 116 recommendations for reform of the Privacy Act. Of those 116 recommendations, 38 proposals were accepted in full by the Federal Government with a further 68 proposals being agreed 'in-principle'. The Bill aims to implement 23 proposals that were agreed in full and one of the 'agreed-in-principle' recommendations. Given the way in which AI tools operate, it is very likely that any reforms made to the Privacy Act will have some relevance to the future use of AI and its regulation. However, the following proposed amendments appear to be particularly relevant in this context:

- the proposal to introduce the regulation of automated decision-making in circumstances where personal information is being used in that process (Part 15 of the Bill); and

- updates to existing data security requirements under the Australian Privacy Principles (**APPs**) and, in particular, APP 11 (Part 5 of the Bill).

We consider the impact of these proposed reforms below.

Automated Decision-Making

Automated decision-making (**ADM**) refers to the deployment of technology to automate a decision-making process.

The Bill proposes a number of changes to the Privacy Act regarding ADM, which include the following:

- privacy policies should set out the types of personal information that will be used in automated decisions which could reasonably be expected to have a significant effect on an individual's rights or interests; and
- privacy policies should also contain high-level indicators of the types of automated decisions which could affect an individual's rights or interests, such as a decision to grant, or refuse to grant, a benefit to an individual, a decision that affects an individual's rights under an agreement, contract or arrangement, or a decision that affects an individual's access to a significant service or support.

Entities would be required to include certain information in privacy policies about the use of personal information to make automated decisions. This information would include:

- the kinds of personal information used in the operation of computer programs;
- the kinds of decisions made solely by the operation of computer programs; and
- the kinds of decisions for which a thing, that is substantially and directly related to making the decision, is done by a computer program.

In its discussion paper released following the publication of the Report, the Office of the Australian Information Commissioner (**OAIC**) noted that the benefit of ADM will only be fully enabled if the risks are appropriately mitigated. The OAIC also found that:

- 84% of Australians think that individuals should have a right to know if a decision affecting them is made using AI technology; and
- 78% of Australians believe that when AI technology is used to make or assist in making decisions, people should be told what factors and personal information are considered by the algorithm and how these factors are weighted.[4]

The consensus seems to be that the benefits of ADM can be far reaching, provided that the regulatory framework is equipped to deal with the use of ADM processes.

Security, Retention and Destruction of Personal Information

The Bill also proposes that a clarifying amendment be made to APP 11, which relates to the security of personal information. Under APP 11, entities are currently obliged to take 'such steps as are reasonable in the circumstances' to protect the personal information they hold from misuse, interference and loss and from unauthorised access, modification or disclosure.

The Bill clarifies that the reasonable steps required under APP 11 includes both technical and organisational measures. According to the Explanatory Memorandum:

- technical measures may include 'physical measures, and software and hardware – for example through securing access to premises, encrypting data, anti-virus software and strong passwords'; and
- organisational measures may include 'training employees on data protection, and developing standard operating procedures and policies for securing personal information'.

These amendments will necessarily require businesses to consider the measures which are appropriate to protect personal information having regard to their use of generative AI.

What's next?

The Bill will go to parliamentary committee for review. However, the next and final parliamentary sitting for the year is in November. Given the Bill is yet to undergo a final reading, the Bill may not be passed until next year.

The office of the Attorney-General has also forecast a second tranche of reforms following further consultation, describing the Bill as *'just the first stage of the Government's commitment to provide individuals with greater control over their personal information'*.

Notably, one of the much-anticipated proposals, which was agreed in principle but was not implemented within the Bill, is the insertion of an overarching requirement that any collection, use and disclosure of personal information needs to be 'fair and reasonable'. If this proposal were to be implemented at a later stage, it seems that such an amendment would be particularly relevant to the use of AI in the workplace.

Will Australia's privacy law regime be equipped to deal with AI after the reforms?

Just as in overseas jurisdictions, Australia is at a point where it must find the correct balance between allowing the use of generative AI in a way which optimises its features and extraordinary potential while protecting the personal information and rights of individuals.

It is inevitable that achieving that balance will involve added obligations and accountability for business. A number of regulatory models have been proposed internationally which adopt quite different approaches to finding the right balance by resisting burdening business with overly onerous obligations and restrictions while recognising that the rights of individuals need to be recognised and secured from the outset.

This is a rapidly evolving space and there will be fine-tuning as time goes on. There are many cases regarding AI already before the Courts, and the decisions in those cases will assist in determining where the line needs to be drawn.

If you have any concerns or questions about how the proposed reforms to the Privacy Act may impact your business, please reach out to our team.

This article was written by Simone Basso, Associate, and reviewed by Peter Campbell, Partner. ■

Endnotes

1. Nick G, '101 Artificial Intelligence Statistics [Updated for 2023]', *TechJury* (Online) <https://techjury.net/blog/ai-statistics/#gref>.
2. 'Big Data AI', *Qlik* (Web Page) <https://www.qlik.com/us/augmented-analytics/big-data-ai>.
3. 'Introducing ChatGPT', *OpenAI* (Web Page) <https://openai.com/blog/chatgpt>.
4. Office of the Australian Information Commissioner, 'Privacy Act Review – Discussion Paper', 23 December 2021 [17.4].