Australian Government
Attorney-General's Department

October 2024

Submission to the inquiry into the Privacy and Other Legislation Amendment Bill 2024

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 and Other Legislation Amendment Bill 2024 (the Bill) in response to the Committee's invitation on 20 September 2024.

Importance of privacy reform

The rapid evolution of technology is transforming the way Australians engage with each other, providing significant benefits and opportunities. However, advances in technology are also facilitating harms, like scams, fraud and doxxing, and research indicates the law has not kept pace with community expectations.[1]

There have been increasing calls for privacy reform over several years. The Privacy Act Review (Review) was undertaken following a recommendation by the Australian Competition and Consumer Commission in its 2019 Digital Platforms Inquiry. An almost three-year review process began in 2020 involving consultation with the business sector, media organisations, cybersecurity experts, individuals and civil society. Over 900 written submissions were received, and over 360 stakeholder meetings held, during the review and development of the Government response.

Following serious data breaches in 2022, the *Privacy Act 1988* (Cth) (Privacy Act) was amended to significantly increase penalties for serious or repeated privacy breaches and provide the Office of the Australian Information Commissioner (OAIC) with enhanced enforcement and information sharing powers.

This Bill is the next step in the Government's agenda to uplift Australia's privacy framework for the digital age. It implements an important first tranche of reforms that were agreed by Government in its September 2023 Response to the Review. One of the Review's proposals was the introduction of a statutory tort for serious invasions of privacy. The Government held a public consultation on doxxing in March 2024, in which there was broad support for the statutory tort as an additional remedy alongside criminal laws.

The Bill provides individuals with greater protection, transparency and control over their privacy. These protections are vital to the Government's broader agenda to ensure Australian's personal information is safe and secure and is used responsibly and in the interests of the Australian community. The Government will continue advancing a further package of privacy reforms based on proposals from the Review that were agreed in-principle, through further targeted consultation with stakeholders on draft provisions.

Strong privacy protection reforms are critical to the Government's efforts across a range of areas to ensure technology is deployed for the benefit of Australians. The measures in this Bill and future privacy reforms will support initiatives to protect children and adults from online harms, uplift cyber security across the economy, prevent and address scam and other fraudulent activity, ensure the adoption of safe and responsible Artificial

[1] OAIC Australian Community Attitudes to Privacy Survey, August 2023, available at: <https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2023>; Deloitte Australia Privacy Index 2023, available at https://www.deloitte.com/au/en/services/risk-advisory/analysis/deloitte-australian-privacy-index.html.

Intelligence and provide a comprehensive and consistent legal framework to support the use of automated decision-making by Government.

Overview of the Bill

This Bill strengthens privacy protections and outlaws doxxing.

- Schedule 1 of the Bill enacts the first tranche of reforms to the Privacy Act. The Government will continue progressing the remaining proposals which have been agreed in-principle.
- Schedule 2 of the Bill creates a new statutory tort for serious invasions of privacy.
- Schedule 3 of the Bill amends the *Criminal Code Act 1995* (Criminal Code) to introduce two new offences targeting the release of personal data in a manner that would be menacing or harassing.

Schedule 1 of the Bill amends the Privacy Act by explicitly recognising the public interest in privacy, introducing new penalties for breaches of privacy and enhancing enforcement powers available to the OAIC. It includes measures to streamline information sharing to respond to eligible data breaches and emergencies, and increases transparency in relation to substantially automated decisions with significant effect. It requires the Information Commissioner to develop a Children's Online Privacy Code. The Government will provide the OAIC with additional funding of $2.97 million over three years from 2024-25 to develop the Children's Online Privacy Code.

All Australians, and particularly vulnerable groups, are at risk when their privacy is seriously invaded. Schedules 2 and 3 of the Bill provide new civil and criminal tools to provide individuals with avenues for redress and hold abusers to account.

These reforms are the next step in creating a modern, fit-for-purpose privacy framework that protects the interests of all Australians. It also delivers on a commitment made by the Government following the National Cabinet held in May 2024 to address gender-based violence, by outlawing the practice of "doxxing", or the malicious release of personal data online.

Privacy Act reforms

Privacy codes

The Bill empowers the Information Commissioner to develop and register an APP code or Temporary APP code on the written direction of the Minister, if the Minister is satisfied that it is in the public interest to develop the code, and for the Information Commissioner to develop the code.

APP codes provide specificity about how the Australian Privacy Principles (APPs) apply in particular circumstances. For example, the Australian Government Agencies – Governance APP Code 2017 sets out specific requirements for Government agencies to comply with the obligation in APP 1.2 to take such steps as are reasonable in the circumstances to implement practices, procedures and systems to ensure compliance

with the APPs and deal with inquiries or complaints. APP codes provide entities with certainty on how to comply with their obligations and provide individuals with transparency about how their information will be handled. Increased flexibility in how APP codes may be developed will assist with making new codes to provide clarity on how new privacy obligations will apply in different circumstances, including in the context of new and emerging technologies.

Children's privacy

The Bill requires the Information Commissioner to develop and register a Children's Online Privacy (COP) Code, that would apply to regulated entities that provide social media services, designated internet services or relevant electronic services that are likely to be accessed by children. The COP Code would be an enforceable APP code that specifies how these entities must comply with privacy obligations in relation to children. This recognises that children merit special privacy protection as they may be less aware of the risks and consequences associated with the handling of their personal information, particularly online.

The COP Code will require entities covered the code to design their services in a manner that protects children from harm. Alongside other Government measures, such as setting a minimum age for children to access social media, it will improve online safety for children. Further reforms will consider additional proposals to increase privacy protections for children – including in relation to harmful targeting and trading in children's personal information, and requiring entities to have regard to the best interests of the child when handling their personal information.

Information sharing declarations

The Bill amends the emergency declaration provisions currently in the Privacy Act. This will enable emergency declarations to be more targeted by requiring that the scope of personal information handling under emergency declarations be specified within the declaration, instead of allowing wide sharing of personal information in a declared emergency or disaster. This will strike a better balance between protecting individuals' privacy, and enabling effective and coordinated responses to an emergency or disaster.

The Bill also empowers the Minister to make a declaration which will authorise entities to handle personal information in a manner specified within the declaration in order to prevent or reduce the risk of harm to individuals in the event of an eligible data breach. Individuals affected by a data breach are exposed to risk of serious harms including identity fraud, reputational damage and blackmail. Unauthorised access or disclosure of personal information in a data breach can cause significant financial loss, emotional distress and have serious, ongoing consequences for individuals. Sharing information under these circumstances will enable entities such as banks to act quickly to prevent the misuse of compromised credentials. Safeguards are included to ensure that a declaration can only be made for a purpose that is related to preventing or reducing a risk of harm to individuals arising from a misuse of personal information from the eligible data breach

Technical and organisational measures to secure information

The Bill clarifies the expected scope of measures that entities should consider when determining how to protect personal information as required under APP 11.1. The Bill promotes the importance of implementing technical and organisational measures (such as encrypting data, securing access to systems and premises, and

undertaking staff training) to address information security risks. Such measures minimise the risk of data breaches and harm arising from cyber incidents, which can cause significant detriment to affected individuals.

Further privacy reforms will include consideration of additional measures to enhance security obligations – including requiring entities to comply with a set of baseline privacy outcomes and set maximum and minimum retention periods for personal information held.

Enhancing the safe, free flow of information overseas

The Bill introduces a mechanism to prescribe countries and binding schemes that provide substantially similar privacy protections to the APPs. This will provide greater certainty to disclosing entities about the standard of privacy protections in prescribed countries enhancing the flow of information across national borders while ensuring privacy is respected. Further reforms will consider measures to enhance safe overseas data flows.

New civil penalties and enhanced enforcement mechanisms

The Bill introduces new tiered civil penalties commensurate with the seriousness of the interference with privacy. These amendments will provide more enforcement options to the Information Commissioner to deter non-compliance and address a gap in the enforcement of privacy protections which allowed the Information Commissioner to seek civil penalties only for the most serious or egregious interferences with privacy. Lesser penalties and an infringement notice scheme for breaches of the Act that are less serious will allow the Information Commissioner to resolve matters more efficiently and proportionately.

The Bill also increases flexibility in the event of an interference with privacy by:

- allowing the Information Commissioner to issue a determination requiring a respondent to perform any reasonable act or course of conduct to prevent or reduce reasonably foreseeable future loss or damage – such as requiring entities to engage service providers such as identity theft and cyber support providers to give support to affected individuals for a certain time period after a cyber security incident, and
- expanding the jurisdiction of the Federal Court of Australia and the Federal Circuit and Family Court of Australia to make orders other than civil penalties if the Court is satisfied there has been contravention of a civil penalty provision - such as orders for compensation or orders to take steps to minimise further impacts to individuals impacted by the interference with privacy.

To ensure a robust and consistent regulatory framework to monitor compliance and enforce protections in the Privacy Act and other Acts under which the Information Commissioner has responsibility, the Bill triggers the standard monitoring and investigation powers in Part 2 and Part 3 of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth). This will allow the Information Commissioner to resolve matters more efficiently, and improve successful regulatory outcomes.

The Information Commissioner will also be empowered to conduct public inquiries into specified matters as directed by or subject to Ministerial approval. Public inquiries would enable the Information Commissioner to examine acts and practices that may illustrate systemic or industry-wide issues relevant to individuals' privacy. These provisions would support the Information Commissioner's privacy functions, including by

indicating where further education and guidance may assist entities to comply with requirements in the Privacy Act or where to target regulatory efforts.

Greater transparency over automated decisions

The safe and responsible development and deployment of new and emerging technologies, including automated decision making (ADM), presents significant opportunities for enhancing productivity and facilitating economic growth, and improving outcomes for Australians across the areas of health, environment, defence and national security. However, ADM systems may pose privacy risks as they can use personal information about individuals to assist or replace the judgement of human decision makers in ways which may have significant impact, with little transparency. Providing individuals with greater transparency on ADM allows them to understand how an entity handles their personal information and for what purposes, and allows them to take further action if there has been a breach of their personal privacy.

The Bill requires entities to include information in privacy policies about the kinds of personal information used in, and types of decisions made by, computer programs that use personal information to make decisions that could reasonably be expected to significantly affect the rights or interests of an individual. Further privacy reforms will progress measures to increase the transparency of ADM – including by providing individuals a right to request meaningful information about automated decisions that have a significant effect on an individual's rights or interests. This proposal will be further considered as part of a second package of privacy reform measures, and in the context of the developing a consistent legislative framework for the use of ADM in the delivery of government services to ensure consistency in approaches.

Statutory Tort

The Bill creates a new statutory tort for serious invasions of privacy. It will address gaps in existing privacy protections and provide a flexible framework to address current and emerging privacy risks. Individuals will be able to take action in court on their own behalf, and seek a remedy for a broader range of invasions of privacy than existing laws. As such, the tort may provide an additional avenue for redress for victims of doxxing. To enhance access to justice, individuals will be able to commence actions in state and territory courts as well as federal courts.

Individuals will have a cause of action if they suffer a serious invasion of their privacy, either by an intrusion into their seclusion or by misuse of information, in circumstances where a person in their position would have had a reasonable expectation of privacy. Only intentional or reckless invasions are actionable. A mistake – such as an accidental data breach – or mere negligence would not be sufficient. There is no requirement for a plaintiff to prove damage as a result of the invasion, however the damage or harm a plaintiff suffers will be a relevant factor in assessing the seriousness of the invasion, and the remedies that may be awarded.

The tort model recognises that privacy interests must be balanced against other important interests. Where there is evidence of a competing public interest, the plaintiff must satisfy the court that the public interest in protecting their privacy outweighs it. This balancing exercise is a key element of the cause of action, and recognises that a plaintiff should not be able to claim that a wrong has been committed where an invasion of privacy is justified in the public interest. For example, an individual's privacy may legitimately be invaded in

the course of taking action to protect them from serious harm, for example in a bushfire or other emergency situation.

A range of defences will be available, for conduct that is:

- required or authorised by law,
- incidental to defend a person or property
- undertaken with consent, or
- necessary because of a serious threat to life, health and safety.

Certain defences that are available for defamation actions will also apply: absolute privilege, publication of public documents, and fair reporting of proceedings of public concern. The rationale for protecting these communications from liability, which is underpinned by public interest considerations, is as applicable to the tort as it is to defamation actions.

The Australian Law Reform Commission (ALRC), Privacy Act Review and a number of other inquiries have recommended the enactment of a statutory tort for serious invasions of privacy. The tort enacted by Schedule 2 of this Bill is closely based on the model recommended in ALRC Report 123, with additional exceptions for journalism, law enforcement and intelligence agencies. These exemptions are important to protect press freedom and ensure that legitimate activities of government can be delivered effectively. Children under 18 will also be exempt from liability because children do not have the same level of understanding as adults of the implications of their conduct.

New criminal offences to address the harms caused by doxxing

The widespread use of social media and online platforms has significantly increased the ability for individuals to access or gain another's personal information, and to maliciously release that information online – an act known as 'doxxing'. Doxxing can expose victims to significant and enduring harm, including public embarrassment, humiliation or shaming, discrimination, stalking, identify theft and financial fraud, and threats to their life and safety, and the lives and safety of their families and friends. This can, in turn, inflict significant psychological harm on their victims. These harms can be enduring. Once a perpetrator has maliciously released a person's personal details online, that person can be subjected to continuing harassment, abuse, discrimination, identity theft, and threats, unless and until they take significant steps to mitigate that harm which may include closing online accounts, changing contact details, moving residential address, or replacing their identity documents.

Schedule 3 of the Bill addresses this challenge by amending the *Criminal Code Act 1995* (Criminal Code) to create new offences in Part 10.6 of the Criminal Code, targeting the release of personal data in a manner that would be menacing or harassing.

Section 474.17C – Using a carriage service to make available etc. personal data of one or more individuals

The proposed new section 474.17C is a standalone offence that applies where a person:

- uses a carriage service to make available, publish or otherwise distribute personal data of one or more individuals; and
- does so in a way that reasonable persons would regard as being menacing or harassing towards those individuals.

The offence includes a note which provides an example of the type of conduct covered by this offence. It provides that publishing the name, image and telephone number of an individual on a website and encouraging others to repeatedly contact the individual with violent or threatening messages is conduct covered by this section and this conduct is more commonly referred to as doxxing.

The proposed new offence will be punishable by a maximum penalty of 6 years' imprisonment. This is a higher maximum penalty than section 474.17 of the Criminal Code, which makes it an offence to use a carriage service to menace, harass or cause offence. This reflects the serious harms caused by doxxing, the potentially enduring nature of these harms, and the significant steps that a victim may need to take to mitigate these harms.

Section 474.17D – Using a carriage service to make available etc. personal data about one or more members of certain groups

The proposed new section 474.17D is a standalone offence that applies where a person:

- uses a carriage service to make available, publish or otherwise distribute personal data of one or more members of a group;
- the person engages in the conduct in whole or in part because of the person's belief that the targeted group is distinguished by race, religion, sex, sexual orientation, gender identity, intersex status, disability, nationality, national or ethnic origin; and
- the person does so in a way that reasonable persons would regard as being menacing or harassing towards those individuals.

Subsection 474.17D(3) provides that for the purposes of subsection 474.17D(1)(c), it is immaterial whether the group is actually distinguished by the attributes listed in paragraph 474.17D(1)(c). There is no requirement that the person or persons actually have or share that protected attribute. It will be sufficient that they are members of any group, including that the offender had 'grouped' them, and engaged in their conduct because of their belief that the group was distinguished by these attributes.

The offence includes a note which provides an example of the type of conduct covered by this second offence. It provides that publishing the names, images and residential addresses of members of a private online religious discussion group across multiple websites, and encouraging others to attend those addresses and block entryways or otherwise harass the members of the group. is conduct covered by the offence.

The proposed new offence will be punishable by a maximum penalty of 7 years' imprisonment. This higher maximum penalty reflects the seriousness of such conduct. Doxxing persons because of a belief that they are part of a group that shares one or more protected attributes is particularly serious in nature, as it is likely to instil fear or anxiety in victims where there is a history of, or ongoing, persecution or prejudice and can encourage or incite other persons who share discriminatory views in relation to the protected group to engage in similar menacing or harassing conduct towards the victims.

Next steps

The Government has committed to progressing further reforms to the Privacy Act based on the proposals from the Review that were agreed in-principle.

The department will undertake targeted consultation on draft provisions to progress the outstanding legislative proposals from the Government response to the Review, which will ensure the details of an updated privacy framework for the digital age are appropriate and workable in a diverse range of contexts. This will build on the extensive consultation to date with a broad range of stakeholders interested in protecting Australian's privacy and will ensure that the right balance is struck between protecting people's personal information, and allowing it to be used and shared in ways that benefit individuals, society and the economy. The targeted consultation will inform the Government's decision making on next steps in relation to Privacy reforms.