THE PRIVACY ACT AND LESSONS FROM DATA BREACHES IN THE PUBLIC SECTOR

Submission to the Parliament of Australia, Joint Committee of Public Accounts and Audit

Inquiry into the management of client privacy in the Australian public sector

May 2026

Protocol

Protocol

TABLE OF CONTENTS

ABOUT US

This Submission is a research product of a group of university students and recent graduates taking part in Protocol Policy Lab's Policy Research Program. The Program is a semester-long extracurricular program that provides young Australians the opportunity to conduct in-depth research on a current issue in Australian technology policy.

EXECUTIVE SUMMARY

This Submission responds to the following Terms of Reference:

a) The frameworks used to identify and manage privacy risks, and meet the requirements of the *Privacy Act 1988* (Cth) (***the Privacy Act***), in public sector entities that manage information on private individuals;

b) The ability of public sector entities holding personal information to respond effectively to data breaches, cyber threats, and malicious actors; and

c) Any matters contained in and associated with Auditor-General Report No. 12 of 2025–26: Managing the Privacy of Client Information in Services Australia.

This Submission will address the terms of reference in the following manner: firstly, by outlining the framework and issues surrounding the management of public sector data; secondly, by providing case studies of recent breaches of data held by public institutions; thirdly, by analysing current academic discourse and proposed changes to the legislative framework; and finally, by providing recommendations to implement stronger protections for personal information held by public sector entities.

Based on our research, we developed two key recommendations:

1. Strengthening the current Notifiable Data Breaches Scheme (**the NDB Scheme**) through establishing a clearer and objective risk threshold and severity mapping; and

2. Strengthening the current "reasonable steps" requirement for cybersecurity and data privacy management under the *Privacy Act* through articulating clearer and enforceable standards.

AUTHORS OF THIS SUBMISSION

Helena Bradshaw
Keona Rangwala
Sharan Sidhu
Elizabeth Thomas

SCOPE OF RESEARCH

The scope of this Submission is limited to legislative frameworks of privacy at the Commonwealth level. This Submission examines current statutory mechanisms, regulatory guidance and enforcement practices which are applicable to both the public and private sectors. This Submission does not consider privacy laws at the state or territory level.

This Submission identifies and analyses the relationship between core privacy frameworks and available critical infrastructure protections, particularly the *Privacy Act*.

INTRODUCTION

Commonwealth public sector entities hold the sensitive personal information of millions of Australians. The expansion of digital service delivery has increased the scale and consequences of privacy risks and data breaches. Unlike in the private sector, individuals often have limited choice in allowing public sector organisations to collect and store their information. This lack of choice makes the government's stewardship of that data a matter of fundamental public interest.[i]

Recent data breaches and the findings of Auditor-General Report No. 12 of 2025–26 (**the Report**) have exposed vulnerabilities in the capacity of some entities to protect personal information.[ii] In critical infrastructure sectors such as health, education and social services, public sector entities may collect information such as identification details, financial records, employment history and health data.[iii] This Submission focuses on two case studies: the recent audit of Services Australia, and the data breach at the Australian National University. These incidents suggest a gap between current privacy obligations under the *Privacy Act* and the operational capacity of some public sector entities to identify, assess and respond to breaches.

The significance of these risks is illustrated by Services Australia, which manages personal information for approximately 37.5 million Australians across Medicare, Centrelink and child support programs.[iv] The Report found that Services Australia is only partially effective in managing client privacy, and identified compliance deficiencies across risk management, data matching, record-keeping and transparency. The Report recorded 6,042 substantiated privacy incidents between 2022–23 and 2024–25.[v]

LEGISLATIVE FRAMEWORKS

The handling of personal information by Commonwealth public sector entities is governed primarily by the *Privacy Act*. The broader legal framework also includes the Australian Privacy Principles (**the APPs**), the NDB Scheme and the *Privacy (Australian Government Agencies — Governance) APP Code 2017* (**the APP Code**). Entities operating in critical infrastructure sectors have additional security and resilience obligations under the *Security of Critical Infrastructure Act 2018* (Cth) (***the SOCI Act***).

a) *Privacy Act 1988 (Cth)*

The *Privacy Act* contains 13 APPs which establish standards, rights and obligations for the collection, use, storage, disclosure, and access of personal information.[vi] The most relevant principles for this Submission are: APP 3, which regulates the collection of personal information; APP 5, which requires notification of collection; APP 6, which governs use and disclosure; and APP 11, which concerns the security of personal information.[vii]

APP 11 is particularly significant in the data breach context. It requires an APP entity that holds personal information to take reasonable steps to protect that information from misuse, interference and loss, and from unauthorised access, modification or disclosure.[viii] The *Privacy and Other Legislation Amendment Act 2024* (**the *Privacy Amendments Act***) clarified that "reasonable steps" now explicitly encompasses both technical and organisational measures.[ix]

The Office of the Australian Information Commissioner (**the OAIC**) is the national privacy regulator and is responsible for privacy guidance, complaint handling, investigations and enforcement under the *Privacy Act*.[x]

b) *Notifiable Data Breaches Scheme*

The NDB Scheme is established under Part IIIC of the *Privacy Act*.[xi] It requires regulated entities to notify the OAIC and affected individuals where there are reasonable grounds to believe an eligible data breach has occurred. An eligible data breach involves unauthorised access to, unauthorised disclosure of, or loss of personal information that is likely to result in serious harm.[xii] Where an entity merely suspects an eligible data breach, section 26WH requires it to conduct a reasonable and expeditious assessment and take all reasonable steps to complete that assessment within 30 days.[xiii]

c) *Privacy (Australian Government Agencies – Governance) APP Code 2017*

The APP Code is established under section 26G of the *Privacy Act*.[xiv] Its objectives are to enhance the privacy capability and accountability of agencies, promote good privacy governance, and build community trust and confidence in personal information handling practices.[xv]

The Code imposes additional governance obligations on Australian government agencies. Agencies must maintain a privacy management plan and measure and document performance at least annually.[xvi] A Privacy Officer must be designated to handle privacy enquiries, complaints and conduct privacy management plan reviews.[xvii] Agencies must also conduct privacy impact assessments (**PIAs**) for all high privacy risk projects and maintain a publicly accessible register of those assessments.[xviii]

Protocol

d) *Security of Critical Infrastructure Act 2018 (Cth)*

Acting alongside the *Privacy Act*, the *SOCI Act* aims to provide a framework for managing risks relating to critical infrastructure.[xix] Its statutory objectives include improving transparency over ownership and operational control, requiring responsible entities to identify and manage risks to critical infrastructure assets, imposing enhanced cyber security obligations, and enabling Commonwealth responses to serious incidents.[xx] The Act applies across eleven critical infrastructure sectors, including data storage and processing, higher education and health care.[xxi]

The *SOCI Act* imposes operational and cyber security obligations on responsible entities. Sections 30AC to AG include the requirement to adopt, maintain and comply with a critical infrastructure risk management program, subject to regular review, update and annual reporting.[xxii] The Act also imposes mandatory cyber incident reporting obligations. Section 30BC requires critical cyber security incidents to be reported to the relevant Commonwealth body within 12 hours of awareness, and section 30BD requires other cyber security incidents to be reported within 72 hours of awareness.[xxiii]

KEY ISSUES IN PUBLIC SECTOR DATA MANAGEMENT

The management of critical infrastructure data in the public sector faces several challenges due to a misalignment between regulatory frameworks provided by current legislation and the capacity of Commonwealth agencies in managing the risks associated with vast critical datasets.

Conflicting requirements under legislative frameworks

Notably, Commonwealth service delivery for social services, education and healthcare is defaulting to a primarily digital model, with a goal of reaching complete online flexibility by 2030.[xxiv]

Nonetheless, current legislative frameworks may not be able to support such a model and corresponding expansion. Conflicting requirements imposed by the *Privacy Act*, its subsidiary schemes and the *SOCI Act*[xxv] result in a regulatory environment which struggles to ensure that agencies are well-equipped to safeguard the information collected from critical services. A single cyber incident involving personal information held in, or connected to, a critical infrastructure asset may trigger obligations under both the *SOCI Act* and the NDB Scheme simultaneously. This makes government agencies' compliance with legal obligations complex because the regimes create different thresholds, reporting pathways and policy objectives.

As mentioned above, the *SOCI Act* has a cyber incident reporting regime to ensure that the Commonwealth has timely visibility of cyber incidents affecting critical infrastructure so that

the government can assess national security risks. Thus, the *SOCI Act* reporting mechanism is directed primarily to government visibility and critical infrastructure resilience as opposed to public disclosure to affected individuals. Section 22 of the *SOCI Act* expressly states the Register of Critical Infrastructure Assets is non-public.[xxvi] The Register of Critical Infrastructure Assets contains information about who controls and has access to critical infrastructure, used to help the government manage and assess risks to national security.[xxvii] Compliance with *SOCI Act* reporting may therefore not satisfy an entity's separate *Privacy Act* notification obligations, which require entities to notify the OAIC and affected individuals where there are reasonable grounds to believe a data breach has occurred.[xxviii]

Lack of enforceable deadlines for responding to data breaches

The regulations outlined by the *Privacy Act* do not provide a legally enforceable deadline for responding to a data breach. This is evident in both the 'serious harm' threshold for identifying an eligible data breach, and the stipulation of practicability when notifying affected individuals.[xxix] Neither phrase is defined in the Act or any subsequent legislative instruments, and so a report is dependent on the individual interest of an organisation, as opposed to the wider public interest.[xxx] In the public sector, this may be compromised or inhibited by political, reputational, or other arbitrary individual justifications. This subjective test is at odds with the 12 hour reporting window posited by the *SOCI Act*, which sets a legal requirement for the reporting of cyber security incidents to the Australian Signals Directorate's Australian Cyber Security Centre.[xxxi]

The NDB Scheme posits a window of up to 30 days to conduct a 'reasonable and expeditious' assessment of a suspected breach.[xxxii] Permitting public sector organisations to conduct investigations of suspected or ongoing data breaches in an extensive window may increase the risk of harm as delays in identifying, assessing and notifying breaches can reduce the ability of affected individuals to take remedial steps.[xxxiii] Simultaneously occurring data breaches may remain undetected for a prolonged period, developing to an extent which is difficult to control whilst compromising further data.[xxxiv] Additionally, already compromised data may be used to facilitate financial fraud or identity theft before individuals are made aware of the incident, developing beyond the control of the regulatory framework.[xxxv]

Limited protection provided by the Privacy Act

The *Privacy Act* has narrow application, potentially inhibiting its ability to protect substantial datasets. The Act, which applies to protect the 'personal information' of individuals, defines this phrase as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable'.[xxxvi] This fails to encompass multifaceted data often found in critical infrastructure including metadata which falls outside the statutory definitions of 'personal' and 'sensitive' information.[xxxvii] Whilst this data can be de-identified, a risk of re-identification through 'jigsaw identification' exists, where anonymised data can be cross referenced and combined from both public and private sources to identify specific individuals.[xxxviii] Moreover, consideration is absent in the *Privacy Act* as to the relationships between government

entities and third party providers, where third parties are not held to the same reporting obligations as public organisations, regardless of their mutual management of public data.[xxxix] As such, the *Privacy Act* does not address the risks associated with modern, multifaceted datasets.

CASE STUDIES

Case Study 1: Organisational Discrepancies at Services Australia

The Auditor-General Report concerning Services Australia's management of privacy found several instances where current legal frameworks were not sufficient for the protection of critical infrastructure data, or where the agency did not fulfil its obligations.

The Report found that the agency set internal deadlines for reporting data breaches, of within 3 business days to the OAIC and 10 business days for affected individuals following a breach assessment.[xl] This is beyond the regulations of the *Privacy Act*, and theoretically mitigates risks of subjective action. However, the agency frequently failed to meet these targets; 71% of NDBs between 2018-19 and 2024-25 were reported to the OAIC '50 or more days after Services Australia became aware of the incident'.[xli]

Secondly, the Report found that the agency failed to process 72% of its confirmed NDBs within the required 30-day period, between 2019 and 2025.[xlii] Whilst the agency justified its inability to meet internal reporting targets due to its undertaking of complex assessments that aim to support vulnerable customers, a failure to complete such assessments in the 30-day period heightens risks for individuals.[xliii] This is demonstrated by an increase from 7 maliciously motivated NDBs in the 2022-23 period to 82 in the 2024-25 period.[xliv]

Thirdly, the Report discusses the need for entity compliance to effectively enact the existing data management framework. The Report found that Services Australia failed to fulfil its PIA obligations as per the APP Code, failed to complete preliminary privacy threshold assessments, was delayed in adding PIAs to the public register and made several overall record keeping discrepancies.[xlv] The effectiveness of the APP code and the wider *Privacy Act* to reduce critical infrastructure data breaches is hence partially dependent on the receptiveness of an organisation, and their engagement with a proactive privacy regulatory framework.

Finally, the Report found that legislative gaps in the *Privacy Act* inhibit Services Australia's ability to protect critical infrastructure data. The Report makes reference to the organisation's 'Third Party Compromise Plan', which, whilst a response to data leaks involving public infrastructure, carries no 'legislated authority' to compel a private party to disclose a data breach where critical infrastructure data has been compromised.[xlvi] Reliance on media, affected individuals and delayed advice from other Commonwealth agencies inhibits an organisation's ability to respond promptly to developing data breaches, for an indefinite period.[xlvii]

Case Study 2: Attacks on Modern, Complex Data Sets at the Australian National University

The issues observed in Services Australia's data management practices are not isolated to service delivery, and occur across several areas of critical infrastructure data. The Incidental Report on the Breach of the Australian National University's Administrative Systems (**the ANU Report**) illustrates the limitations of legislative frameworks in proactively preventing significant data breaches through its discussion of the 2019 Australian National University cyber attack.[xlviii] ANU acted swiftly in the aftermath of the attack in contrast to the resistance demonstrated by Services Australia in fulfilling its obligations under the *Privacy Act*. However, this case study remains a crucial example of the risks posed by current legal frameworks to individuals' data privacy.

Firstly, the *Privacy Act*'s scope of individual privacy protections is centred on 'personal' and 'sensitive' information.[xlix] The ANU Report draws attention to the process by which ANU's administrative data was breached. The 'Enterprise Systems Domain' ('ESD') network was covertly targeted, a database consisting of 'human resources, financial management, student administration and enterprise e-forms systems'.[l] Using third-party commercial tools to extract combined records from this multifaceted database, the perpetrator acquired the requisite data necessary to engage in a strategy of 'jigsaw identification', which the Act's narrow definition of 'personal information' may fail to encompass.[li] The Act's definitions of information are difficult to apply to the multilayered databases of modern organisations, which, as observed at the ANU, consist of the data of individuals across several areas.[lii] This scattered data is then vulnerable as a unit, risking the privacy of individuals.

Secondly, the functional risks posed by a substantial statutory assessment window are illustrated by the persistent, volatile threat environment observed during the ANU cyber attack. As opposed to the 30 days stipulated in the NDB Scheme, the ANU report outlines the relative immediacy of the organisation's public disclosure of the attack, which occurred after two weeks.[liii] The ANU report also highlights continuous malicious attempts to regain access to the compromised ESD, followed by an almost immediate secondary attack following public disclosure.[liv] Resultingly, the NDB Scheme's 30 day assessment period poses a significant risk to critical public infrastructure data. By allowing at-risk organisations to delay discovery and intervention, vulnerable networks are exposed to ongoing exploitation and secondary attacks.

Finally, the subjective nature of the *Privacy Act*'s 'serious harm' threshold, alongside the organisational cooperation required to enforce pre-existing frameworks illustrates the tension between public transparency and individual interests.[lv] The Act's reliance on undefined, subjective thresholds of 'serious harm' and practicability results in a lack of incentive for organisations to engage in transparency when publicising data breaches.[lvi] This tension is highlighted by the contrast between ANU's proactive response to its cyberattack, and Services Australia's lack of engagement with regulatory frameworks.[lvii] Notably, the ANU Report states that the report was "the first of its kind in Australia following a cyber attack on a public institution", with the purpose of "encourag[ing] disclosure of these attacks more broadly"[lviii]. ANU's voluntary report indicates that a stronger, legally robust framework may normalise transparency and disclosure, as opposed to the current reliance upon individual organisational structure.

CURRENT ACADEMIC DISCOURSE & PROPOSED CHANGES

The current academic discourse around the capacity of the *Privacy Act* to respond to critical infrastructure data breaches explores the progress of the phased out 2024 reforms to the *Privacy Act* and the current gaps which persist within and amongst the relevant privacy frameworks.[lix] While the recent reforms, introduced by the *Privacy Amendments Act,* aim to modernise the framework, there are structural limitations which complicate the Act's application across complex data ecosystems like those in critical infrastructure sectors. The increasing frequency of breaches in Australia has caused significant changes in how private information is regulated, particularly when it comes to organisations which rely more heavily on cloud platforms, APIs and automated systems.[lx]

One significant issue found within the *Privacy Act* are the small businesses and employee records exemptions for reporting requirements.[lxi] The current exemption model creates a blind spot in critical infrastructure supply chains, where third-party vendors may handle sensitive data that falls outside the regulatory coverage.[lxii] As a result, not all entities involved in critical infrastructure operations are subject to consistent reporting obligations or privacy safeguards, undermining the overall integrity of reporting frameworks. This regulatory gap is expected to change through the upcoming reforms, with the government in principle agreeing to remove the exemption and requiring small businesses to meet the same privacy obligations as larger organisations, including handling data breaches and securing personal information.[lxiii]

Furthermore, the operation of the NDB Scheme is of concern as the current requirement to only notify when a breach is 'likely to result in serious harm' provides a benchmark predicated on a subjective assessment of the harm.[lxiv] This allows entities to impose an internal subjective threshold for determining the severity and seriousness of a breach or the potential harm of a breach under investigation. The lack of defined parameters can lead to inconsistent reporting practices and delayed responses, which are particularly problematic within the critical infrastructure privacy context where timely action is essential to contain the breach.

Additionally, the APPs, especially APP 11, have been criticised for its reliance on the 'reasonable steps' standard which has been interpreted as a reactive rather than proactive measure, focusing on the responses after a breach rather than preventative measures.[lxv]The *Privacy Amendments Act* addresses these gaps to some extent by explicitly requiring 'technical and organisational measures', which signals a shift toward more proactive and accountable data protection practices in Australia.[lxvi]

Another current significant discourse refers to the scope limitations within the *Privacy Act* which further complicates its application to critical infrastructure.[lxvii] The *Privacy Act* primarily regulates personal information, however, there are gaps identified in how such information is defined and handled within the critical infrastructure systems, meaning that some sensitive data may fall outside its protections. This is compounded by the overlap with the *SOCI Act*, which imposes separate and often faster reporting requirements. The interaction between

these regimes creates compliance complexity as organisations must navigate multiple and sometimes misaligned obligations.

The *Privacy Amendments Act*, which is being implemented over 2025 and 2026, seeks to address these challenges. The reforms introduce stronger regulatory powers, higher penalties, expanded individual rights and a statutory tort for serious invasions of privacy. These changes reflect a broader shift from the static documentation-based compliance towards operational accountability, requiring organisations to demonstrate how data is handled through real-time systems, including across third-party platforms.

Separately, there are parallel ongoing initiatives such as the Children's Online Privacy Code consultations and the push to operationalise Data Sharing Agreements and Data Processing Agreements which signal a move toward more granular and enforceable data governance.[lxviii] These developments at the Commonwealth level emphasise transparency, cross-border data controls and lifecycle accountability for personal information in the critical infrastructure sector.

RECOMMENDATIONS

1. ***Strengthening the current NDB Scheme through establishing a clearer and objective risk threshold and severity mapping***

Our Working Group recommends that policymakers strengthen and clarify the current NDB Scheme through the introduction of a more objective and tiered harm threshold for organisations to refer to and be obligated to assess data breaches and security incidents against. The current "likely to result in serious harm" test lacks definitional clarity and requires subjective assessment from organisations in determining the reporting responsibilities pursuant to the *Privacy Act*.[lxix] Establishing a clearer criteria which refers to predefined risk categories and mandatory reporting requirements for certain types of incidents (such as ransomware attacks or breaches involving critical infrastructure systems) regardless of severity in the first instance would improve consistency, timeliness and regulatory oversight.

2. ***Strengthening the current "reasonable steps" requirement for cybersecurity and data privacy management under the Privacy Act through articulating clearer and enforceable standards***

We also recommend that there should be greater emphasis placed on proactive cybersecurity obligations through the embedding of clearer and enforceable standards within the current "reasonable steps" requirement. This could include mandating baseline security controls such as encryption, multi-factor authentication, and continuous monitoring and requiring organisations to demonstrate real-time visibility over data flows.[lxx] In aligning these requirements with existing data privacy frameworks like the *SOCI Act*, the overall compliance complexity would be reduced, creating a more unified and effective response mechanism to cyber threats under the *Privacy Act*.

CONCLUSION

This Submission has evaluated the efficacy of current frameworks and legislation in adequately identifying and managing privacy risks at the Commonwealth level to meet the requirements of the *Privacy Act*. Commonwealth public sector entities are holders of data across health, education and social services, yet this Submission has found limitations that inhibit the ability to effectively respond to data breaches and secure the highly sensitive information of the Australian public in a rapidly changing and evolving digital landscape.

The current legislative framework includes the amalgamation of the *Privacy Act*, supported by the Australian Privacy Principles, the Notifiable Data Breaches scheme and the Privacy (Australian Government Agencies — Governance) APP Code, alongside the Security of Critical Infrastructure Act, involving additional obligations for entities in critical infrastructure sectors. However, key issues in the management of public sector data have been identified, highlighting prominent gaps between the current legislation and Commonwealth agency capacities to identify, rectify and assess data breaches. The case study on the recent audit of Services Australia highlighted its limitations in reporting data breaches in a timely manner due to internal resource constraints and the *Privacy Act*'s omission of critical infrastructure data, demonstrating challenges in ensuring organisational receptiveness to legislative frameworks.

Moreover, the case study on the recent data breach at the Australian National University presents the gaps in the current legislation in preventing data breaches in light of the changing requirements of a contemporary digital landscape. This is evident in the narrow scope of the *Privacy Act* despite increasingly complex data sets, the delays to discovery and hence intervention, and the subjectivity of harm thresholds, which undermine the ability to effectively mitigate the risk of data breaches. Therefore, this Submission recommends the strengthening of the objectivity of risk thresholds under the current NDB Scheme to improve the timeliness and robustness of regulatory oversight. Secondly, further emphasis should be placed on strengthening the standards for security control under the 'reasonable steps' requirement of the *Privacy Act* to improve and unify the capacity to comply. Such measures, designed to minimise the gaps between the current legislation and their objectives to meet the requirements of the *Privacy Act* amidst rapid technological transformation, may reduce the occurrence and risks of data breaches and their privacy implications for Australian individuals. This would preserve Commonwealth public entities' social licence and security, whilst allowing for the use of public data for its intended purpose in servicing the public good.

[i] Australian National Audit Office, *Managing the Privacy of Client Information in Services Australia*, Auditor-General Report No 12 of 2025–26 (ANAO, 2026) ('ANAO Report No 12').

[ii] Australian National Audit Office, *ANAO Report No 12* (n 1).

[iii] Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines: Chapter B — Key Concepts* [B.2], [B.107].

[iv] Services Australia, Annual Report 2024–25 (Report, 2025) https://www.servicesaustralia.gov.au/sites/default/files/2025-10/annual-report-2024-25.pdf

[v] ANAO Report No 12 (n 1).

[vi] *Privacy Act 1988* (Cth) sch 1 ('*Privacy Act*').

[vii] Ibid APPs 3, 5, 6, 11.

[viii] *Privacy Act* (n 6) cl 11.2.

[ix] *Privacy and Other Legislation Amendment Act 2024* (Cth) sch 1 ('*Privacy Amendments Act*').

[x] *Privacy Act* (n 6) s 27.

[xi] Ibid s 26WA–26WR.

[xii] Ibid s 26WE.

[xiii] Ibid s 26WH.

[xiv] Ibid s 26G; Office of Australian Information Commissioner, *Privacy (Australian Government Agencies – Governance) APP Code 2017* (OAIC, 2017) ("*APP Governance Code*").

[xv] OAIC, *APP Governance Code* (n 14) s 4.

[xvi] OAIC, *APP Governance Code* (n 14) s 9.

[xvii] Ibid s 10.

[xviii] Ibid s 14.

[xix] *Security of Critical Infrastructure Act 2018* (Cth) s 3 ('*SOCI Act*').

[xx] Ibid.

[xxi] Ibid s 9, sch 2.

[xxii] Ibid ss 30AC–30AG.

[xxiii] Ibid ss 30BC–30BD.

[xxiv] Department of the Prime Minister and Cabinet (Cth), *Australian Data Strategy: The Australian Government's Whole-of-Economy Vision for Data* (Report, [2021]) [32] https://www.finance.gov.au/sites/default/files/2022-10/australian-data-strategy.pdf.

[xxv] *SOCI Act* (n 19).

[xxvi] Ibid s 22.

[xxvii] Cyber and Infrastructure Security Centre, *Registering a Critical Infrastructure Asset* (Guidance, November 2025) 4 https://www.cisc.gov.au/resources-subsite/Documents/register-critical-infrastructure-assets.pdf.

[xxviii] *Privacy Act* (n 6) s 26WA–26WR.

[xxix] *Privacy Act* (n 6) s 26WL.

[xxx] Julian Fell, Georgina Piper and Matt Liddy, 'This is the most detailed portrait yet of data breaches in Australia', *ABC News* (online, 23 March 2023) <https://www.abc.net.au/news/2023-03-28/detailed-portrait-data-breaches-oaic-disclosures/102131586>.

[xxxi] *SOCI Act* (n 19) s 30BC; Cyber and Infrastructure Security Centre, Department of Home Affairs, *Security of Infrastructure Act 2018 General Guidance for Critical Infrastructure Assets* (Factsheet, 2025) <https://www.cisc.gov.au/resources-subsite/Documents/cisc-factsheet-soci-obligations.pdf>.

[xxxii] *Privacy Act* (n 6) s 26WH.

[xxxiii] Office of the Australian Information Commissioner, *Notifiable Data Breaches Report: January to June 2023* (Report, September 2023).

[xxxiv] Office of the Australian Information Commissioner, *'Part 1: Data Breaches and the Australian Privacy Act'*, (Web Page, February 2025) <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-1-data-breaches-and-the-australian-privacy-act.>.

[xxxv] Ibid.

[xxxvi] *Privacy Act* (n 6) s 6(1) (definition of '*personal information'*).

[xxxvii] Ibid s 6(1) (definition of '*sensitive information'*).

[xxxviii] Teresa Scassa and Amy Conroy, 'The Privacy/Transparency Balance in Open Government' in A Ojo and J Millard (eds), *Government 3.0: Next Generation Government Technology Infrastructure and Services* (Springer, 2017) 333, 339, 341.

[xxxix] OAIC, *ANAO Report No 12* (n 1) 12.

[xl] OAIC, *ANAO Report No 12* (n 1) 57.

[xli] Ibid.

[xlii] Ibid 60.

[xliii] Ibid 62.

[xliv] Ibid 59.

[xlv] Ibid 51, 53.

[xlvi] Ibid 30.

[xlvii] Ibid.

[xlviii] Australian National University, *Incidental Report on the Breach of the Australian National University's Administrative Systems* (Report, 2019) ('*ANU Report*').

[xlix] *Privacy Act* (n 6) s 6(1) (definition of '*personal information'* and *'sensitive information'*).

[l] ANU Report (n 48) 2.

[li] Ibid 6; Scassa and Conroy (n 38) 339, 341; *Privacy Act* (n 6) s 6(1) (definition of '*personal information'*).

[lii] ANU Report (n 48).

[liii] *Privacy Act* (n 4) s 26WH; ANU Report (n 48) 3.

[liv] ANU Report (n 48).

[lv] *Privacy Act* (n 6) s 26WL.

[lvi] Ibid.

[lvii] ANAO Report (n 1) 51, 53.

[lviii] ANU, *ANU Report* (n 48) 1.

[lix] *Privacy Amendments Act* (n 9).

[lx] Office of the Australian Information Commissioner, *Notifiable Data Breaches Report: July to December 2024* (Report, May 2025).

[lxi] *Privacy Act* (n 6) s 6D.

[lxii] auDA, *Submission to the Attorney-General's Department: Privacy Act Review Report* [Report, 31 July 2023] <https://www.auda.org.au/news-insights/submissions/submission-attorney-generals-department-privacy-act-review-report/>.

[lxiii] Small Businesses Development Corporation, *What changes to the Privacy Act mean for small businesses* (Blog, 07 October 2024) <https://www.smallbusiness.wa.gov.au/blog/what-changes-privacy-act-mean-small-businesses>.

[lxiv] *Privacy Act* (n 6) pt IIIC.

[lxv] Bird & Bird, *Privacy by Design: The Standard for Information Systems Under Australian Law* (Webpage, 8 May 2025) <https://www.twobirds.com/en/insights/2025/australia/privacy-by-design-the-standard-for-information-systems-under-australian-law>.

[lxvi] *Privacy Amendments Act* (Cth) (n 9).

[lxvii] Jill Slay AM, *Independent Review of the Security of Critical Infrastructure Act 2018* [Report, 2018] <https://www.homeaffairs.gov.au/cyber-security-subsite/files/independent-review-soci-act-final-report.pdf>.

[lxviii] Children's Online Privacy Code (consultation for children and parents), *Office of the Australian Information Commissioner,* (Webpage, 2 July 2025) <https://www.oaic.gov.au/engage-with-us/consultations/childrens-online-privacy-code-consultation-for-children-and-parents>. ; Intergovernmental Agreement on Data Sharing, *Department of Finance* (Webpage, 19 December 2025) <https://www.finance.gov.au/government/public-data/data-and-digital-ministers-meeting/intergovernmental-agreement-data-sharing>.

[lxix] *Privacy Act* (n 6) s 26WL.

[lxx] Office of the Australian Information Commissioner, *Guide to Securing Personal Information* (Guide, June 2018) pt B; Australian Signals Directorate, *Essential Eight* (Web Page) https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight.