Management of client privacy in the Australian public sector

Joint Committee of Public Accounts and Audit

Submitter:

Michael Sanderson

Introduction

I welcome the opportunity to make a submission to the Joint Committee of Public Accounts and Audit inquiry into the management of client privacy in the Australian public sector.

This submission addresses the terms of reference concerning privacy risk frameworks, compliance with the Privacy Act 1988, the ability of public sector entities to respond to data breaches, cyber threats and malicious actors, and the matters raised in Auditor General Report No. 12 of 2025 to 2026, Managing the Privacy of Client Information in Services Australia.

The central point of this submission is simple. Public sector client data is not ordinary administrative material. It is compulsory public trust information. Australians do not provide Medicare, Centrelink, child support, health, identity, family, disability, income and hardship information to the Commonwealth as ordinary market participants. They provide it because essential public services require it. That creates a heightened public duty.

Services Australia holds information on more than 27 million people. The Australian National Audit Office (ANAO) found that it was only partly effective in managing the privacy of client information, with deficiencies in risk management, data matching, record keeping, privacy impact assessments, transparency, reporting and assurance.

That is not a minor compliance problem. It is a public capability problem.

Public sector client data should be treated as sovereign public infrastructure

Client data held by Services Australia should be treated as sovereign public infrastructure. It should be publicly owned, publicly controlled, publicly accountable, properly segmented, resilient, auditable and protected by design.

The default position should be that public sector client data is held on public infrastructure, managed by public institutions and accessed only by authorised public officials. Private access should not be normalised as a matter of administrative convenience. Where private access is claimed to be necessary, it should be exceptional, specific, time limited, legally authorised, logged, independently auditable and publicly reportable.

Private involvement is not automatically unlawful, but it is never neutral. Every private contractor, platform provider, analytics provider, call centre provider, legal services provider, research contractor, technology supplier, subcontractor or support provider adds complexity. Complexity creates more access points, more interfaces, more audit obligations, more cyber exposure, more contract management risk, more breach notification risk and more distance between the affected person and the accountable public authority.

The Committee should therefore treat private access to Services Australia data as a structural privacy risk. The question is not whether private entities can be bound by contract. The question is whether contract-based privacy protection is good enough for information Australians are compelled to provide to the state.

Segmentation should be mandatory

The Committee should recommend strict segmentation of public sector client data.

No person should have access to a larger pool of information merely because it is administratively convenient to create a central repository. Access should be limited by program, role, lawful purpose, client need and operational necessity.

The ANAO report shows why this matters. Services Australia's Enterprise Data Warehouse held personal information across Centrelink, Medicare and Child Support. As of May 2025, there were 1,553 registered users, including 334 external users. A Services Australia review found that Centrelink data was not structured in a way that limited access to specific programs or payments, meaning external users could potentially view personal information not relevant to their work.

That is exactly the type of design failure this inquiry should address. Privacy risk is not created only by hackers. It is also created by over broad lawful access, poor segmentation, excessive permissions and weak internal architecture.

The proper rule should be that no one can see information they do not need, for a function they are not lawfully performing.

Cost should not be used as a barrier to public ownership and operation

Cost should not be treated as a threshold barrier to the Commonwealth developing a wholly publicly owned and operated client data system.

The Commonwealth is the issuer of the Australian dollar. It is not capital constrained in the same way as a household, business, council, state government or private corporation. The proper question is not whether the Commonwealth can find the dollars. The proper question is whether the system is necessary, whether the required real resources exist or can be developed, and whether those resources should be directed to protecting compulsory public data.

Nor should private sector expertise be treated as proof that private control is necessary. If the expertise exists in private enterprise, it exists in the labour force. The Commonwealth can employ, train and retain that expertise directly. Cyber security specialists, software engineers, data architects, privacy lawyers, system administrators, assurance staff and service delivery specialists do not become technically capable only because they sit behind a private contract.

Public capability is a policy choice.

A narrow contract price is also a poor measure of cost. Private involvement may appear cheaper only because the full public cost is pushed out of view. Contract management, duplicate assurance, external legal advice, audit, breach response, fragmented accountability, loss of internal capability, compensation, delay, secrecy claims and loss of public trust all have costs.

A private arrangement is not cheaper in any meaningful public sense if it increases complexity, expands the attack surface, weakens public control or requires additional oversight to manage risks that direct public operation would reduce.

Frontier AI makes the risk more urgent

Frontier AI should be treated as a material privacy risk in this inquiry.

The risk environment is no longer limited to ordinary unauthorised access or accidental disclosure. Frontier AI increases the speed, scale and sophistication of identity fraud, impersonation, phishing, document fabrication, social engineering, automated scraping, pattern recognition and exploitation of compromised personal information.

A breach of Services Australia data in this environment would not merely expose static records. It could provide fuel for automated harm at national scale.

Frontier AI also creates internal public administration risks. AI tools may be used to summarise records, analyse calls, detect fraud, prioritise compliance activity, triage claims, draft correspondence, identify patterns, support decision making or analyse large datasets. Where those tools operate on compulsory public data, they should be treated as high risk by default.

No Services Australia client information should be entered into, processed by, retained by, trained into or made accessible to an AI system unless there is clear legal authority, public justification, strict data minimisation, independent testing, full audit logging, human accountability and public reporting.

This is particularly important where AI capability is supplied by private vendors. Private AI involvement adds the same risks as private data processing generally, but with added opacity. Model architecture, training data, inference behaviour, prompt retention, output reliability, vendor access, subcontracting, offshore processing and model drift can all be difficult to audit.

The Committee should not accept assurances that AI use is safe merely because a contract says so.

Data matching requires stronger transparency and control

Data matching should be treated as a high-risk privacy activity, not as a routine administrative function.

The ANAO found that Services Australia no longer undertakes data matching under the Data matching Program Assistance and Tax Act 1990 and instead follows voluntary guidelines. The ANAO found this reduces transparency and accountability to Parliament, and that there was no documented rationale or legal advice to underpin the change. It also found that Services Australia had published only 13 of 32 data matching protocols.

This is not a theoretical concern. The Robodebt Royal Commission demonstrated the harm that can follow from opaque, automated and poorly governed data practices. The lesson is not merely that one unlawful scheme should not be repeated. The broader lesson is that data matching involving vulnerable people, income support, identity and state power must be transparent, legally robust and subject to public accountability.

The Committee should recommend that all data matching involving public sector client data be subject to mandatory publication of protocols, mandatory privacy impact assessment, clear legal authority, independent review and public reporting to Parliament.

Public reporting should be strengthened

The ANAO found that Services Australia does not publicly report on privacy incidents, complaints or notifiable data breaches.

That is not acceptable for an agency holding compulsory information about almost the entire population.

Privacy should protect people, not shield institutions. Agencies should not be able to rely on privacy, security, legal privilege or commercial confidentiality as a general excuse to avoid public reporting on privacy performance.

The Committee should recommend mandatory annual public reporting by Commonwealth entities on privacy incidents, privacy complaints, notifiable data breaches, breach response timeliness, privacy impact assessments, contractor access, data matching activities, use of AI systems and implementation of audit recommendations.

The absence of transparency is itself a privacy risk. If the public cannot see the scale and pattern of privacy failure, the public cannot assess whether the system is improving.

Penalties must reach individuals, not only institutions

Penalties should not be aimed only at departments and corporations.

Departments and corporations can breach legal duties, but they act through people. Privacy failures occur because individuals design systems, approve access arrangements, issue instructions, ignore warnings, fail to implement audit findings, permit excessive data sharing, accept weak contractor controls, delay breach response or tolerate poor governance.

Institutional penalties have a place, but they are not enough. A financial penalty imposed on a Commonwealth department may move money within the public sector without creating a sufficient behavioural consequence for the people responsible.

A serious privacy regime should include personal accountability where a privacy breach results from recklessness, knowing disregard, sustained neglect, concealment, failure to act on known risk, or instruction to proceed despite clear privacy danger.

This is not about punishing honest mistakes by frontline staff operating under pressure. It is about ensuring that responsibility sits where power sits. Senior officials, executives, system owners, contract managers and decision makers who control the architecture of privacy risk should not be able to hide behind the institutional name of a department.

If they make, approve or tolerate decisions that expose Australians' personal information, the accountability framework should be capable of reaching them personally.

The demand side of privacy abuse should also be penalised

The Committee should also examine the demand side of privacy abuse.

A privacy regime is incomplete if it focuses only on the agency that lost, mishandled or disclosed information. It must also reach any individual or entity that knowingly solicits, procures, purchases, induces, receives, retains, analyses, sells, trains systems on or otherwise uses unlawfully obtained public sector client data.

This is particularly important for Services Australia information. Medicare, Centrelink, child support, family, income, health, disability, identity and hardship information is not ordinary commercial data. Any private entity that knowingly seeks to obtain or exploit that information outside lawful authority should face serious consequences.

The law should not allow a privacy breach to become a commercial opportunity.

There should be appropriate protections for lawful whistleblowing, protected disclosure, journalism, legal representation, authorised advocacy, audit, investigation and genuine public interest activity. The target should be knowing exploitation, not accountability activity. But where the conduct is commercial, malicious, reckless or knowingly unauthorised, the regime should be severe.

Privacy protection must follow the data, follow the access, follow the instruction and follow the benefit.

Recommendations

Recommendation 1

The Committee should recommend that public sector client data be treated as sovereign public infrastructure and that the default position be public ownership, public operation, public infrastructure and public accountability.

Recommendation 2

The Committee should recommend that private access to public sector client data be exceptional, legally authorised, time limited, logged, independently auditable and publicly reportable.

Recommendation 3

The Committee should recommend mandatory segmentation of Services Australia data by program, lawful function, role, operational need and individual authorisation.

Recommendation 4

The Committee should recommend that Services Australia be required to publish a clear account of which private entities can access, process, store, analyse or support systems containing client information, subject only to genuinely necessary security redactions.

Recommendation 5

The Committee should recommend that cost not be accepted as a threshold objection to the Commonwealth building a wholly publicly owned and operated client data system, where the required real resources exist or can be developed.

Recommendation 6

The Committee should recommend that all AI use involving public sector client data be treated as high risk by default and be subject to privacy impact assessment, algorithmic impact assessment, public reporting, human accountability and a prohibition on training external models with client information.

Recommendation 7

The Committee should recommend that all data matching involving public sector client data be subject to mandatory publication of protocols, clear legal authority, privacy impact assessment, independent review and reporting to Parliament.

Recommendation 8

The Committee should recommend mandatory public reporting of privacy incidents, privacy complaints, notifiable data breaches, breach response timeliness, privacy impact assessments, contractor access, data matching activities and implementation of privacy audit recommendations.

Recommendation 9

The Committee should recommend that privacy penalties extend to responsible individuals where serious or repeated privacy failures result from recklessness, knowing disregard, sustained neglect, concealment, failure to act on known risk or instruction to proceed despite clear privacy danger.

Recommendation 10

The Committee should recommend specific penalties for any individual or entity that knowingly solicits, procures, purchases, induces, receives, retains, analyses, sells, trains systems on or otherwise uses unlawfully obtained public sector client data.

Conclusion

This inquiry should not be treated as a narrow compliance exercise.

Services Australia holds compulsory, high sensitivity information about Australians at national scale. The ANAO has found that its management of client privacy is only partly effective. That finding should be treated seriously. It shows that privacy protection cannot safely rely on internal policies, voluntary transparency, fragmented contractor controls and after the fact institutional penalties.

The Commonwealth should build the public systems, public workforce, public cyber capability, public data architecture and public assurance framework needed to protect this information directly.

Where Australians are compelled to provide personal information to the state, the state must not treat that information as an ordinary administrative asset. It is public trust information. It should be held, managed, segmented and protected under public control.