Australian National University
National Security College

Walking the talk on citizen data

Olivia Shen

Key points

- Recent hacks should be a wake-up call for Commonwealth agencies which continue to underinvest in the security and governance of personal information.
- A major government data breach is a matter of 'when' not 'if'.
- Such a breach could seriously compromise national security, the economy, service delivery, and public trust.
- Government is not holding itself to the same standards it expects corporations to meet when it comes to protecting citizen data.

Key recommendations

- The Data and Digital Government Strategy should include minimum data security standards that Commonwealth Government agencies must meet and report on.
- All agencies should build and maintain data inventories and have clear procedures in place for sharing data and managing data breaches.
- The Office of the Australian Information Commissioner (OAIC) should have greater muscle to enforce privacy standards and conduct privacy assessments of highly sensitive datasets held by government.
- Investment in data skills and literacy within government should be accelerated.

In the wake of last year's Optus and Medibank cyber attacks, the Australian Government moved quickly to crack down on data breaches. This included increased penalties of up to $50 million or 30 per cent of turnover for companies that seriously or repeatedly expose Australians' personal information. Attorney-General Mark Dreyfus has also promised an overhaul of privacy laws in response to the recommendations of a long awaited *Privacy Act* review.

The government has sent a clear signal that companies must do more to prevent data breaches. But what about the data risks and responsibilities inside government?

As Cyber Security Minister Clare O'Neil acknowledged in an interview: "we've got to come at this conversation with a sense of humility. Government holds more private information about Australians than anyone else in the community." Minister O'Neil's call for humility is welcome, but it must be matched by a serious improvement of how government agencies manage their data.

Big data in government

Data drives business and innovation in the digital age. It is vacuumed up by corporations to better target customers and increase market share. It is traded by actors both good and bad. It is a building block for some of the most profound technological advances of our time, from artificial intelligence to gene editing.

In a world of big data, government is one of the biggest collectors of unique and sensitive information. Government has special legal powers to collect personal information – from identity documents to movement records – and it is a massive incidental collector of administrative data in the course of delivering services and keeping the country running.

There are clear and legitimate reasons for government to collect and hold the data that it does. Law enforcement and intelligence agencies rely on citizen data to protect Australians and Australia's interests. Data is also essential for meeting public expectations for more streamlined and effective digital government, from welfare provision to taxation. Key government initiatives like myGov, the Consumer Data Right, and the Trusted Digital Identity Framework are underpinned by secure and trusted data exchange.

Yet government does not hold itself to the same data security standards it expects industry to meet. Indeed, government often gets a specific carve-out. The *Privacy Act* covers most Australian Government agencies but does not cover a number of intelligence and national security agencies. Nor does it cover state, territory, and local government agencies, public hospitals, and public schools. Unlike private companies, there are no specific penalties for government agencies who repeatedly expose citizens' data.

One might argue that government should be trusted to regulate itself. But there's plenty of evidence to suggest this isn't enough. Government continues to be one of the top five sectors responsible for data breaches under the Notifiable Data Breach Scheme.[1] According to the Australian National Audit Office (ANAO), 72 per cent of Commonwealth entities have not fully implemented baseline cyber security mitigations known as the Essential Eight.[2] Security concerns have been raised about multiple Commonwealth agencies storing data in Chinese-owned facilities.

The recent MOVEit attack in the US demonstrates how government agencies and the data they hold make for attractive targets for cyber criminals. Even when government is not the primary target, it is impacted by hacks along its supply chain. The Russian attack on law firm HWL Ebsworth, for example, has potentially compromised personal information held by two of its clients – the National Disability Insurance Scheme and, ironically, the OAIC.

A serious breach of citizen data is almost inevitable. If government wants to have credibility with industry and the public on data governance, it needs to get its own data house in order.

Wading through a data swamp

Organisations sometimes operate under a naive misconception that the data they collect lands effortlessly in a pristine 'data lake', ready to be stored, analysed, used and shared. The reality is more often like a muddy swamp. Pipes go in and out carrying data of questionable provenance, age, and quality. Over time, more data is added to the swamp and gets replicated in different formats and locations. Version control and corporate knowledge are lost. Meanwhile, the organisation's policies around data use are opaque and nascent at best. No one quite knows who is responsible for which datasets and there's limited oversight of what data is being accessed, by who, and for what purpose. Soon enough, these sprawling caches of degraded, under-utilised data present more of an organisational risk than a potential asset.

This haphazard, complacent approach to data management is endemic in government. It leads to situations like the Department of Home Affairs having variable figures for how many Australian citizens there are depending on which database you query. Or it leads to electoral roll data, one of the most complete and legally protected datasets on Australians, left running on decades-old legacy platforms.

Consider the policy risks of the data swamp too. What government actions or advice is being informed by bad data? As technology advances and government looks to adopt more automation and artificial intelligence, systems built on a data swamp are more likely to be inaccurate, opaque, and harmful.

Data security isn't just cyber security

Although data security intersects and overlaps with cyber security, they are not one and the same. Cyber security focuses on protecting the technology, platforms and devices that store and process data. Things like patching, encryption, application controls, and authentication. Security at the level of data is about the confidentiality, integrity, and availability of the data you hold.

Data security is vitally supported by cyber security, but it is also about mundane things like labelling your data, archiving or destroying data, navigating the myriad of laws that affect data sharing and use, and properly training staff. These are matters of risk mitigation, policy, culture, and good governance, not technical cyber wizardry.

The Optus hack provides a good example of how cyber security and data protection must work hand in glove. Millions of licence and passport numbers were exposed because Optus retained this information about its customers, sometimes years after they stopped being customers. Rachael Falk, CEO of the Cyber Security Cooperative Research Centre (and who is now advising the government on a new cyber strategy), points out that there was no justification for such data gluttony. Indeed, damage from the Optus hack would have been limited had they not been holding unnecessary data.[3]

Senior decision makers who continue to conflate cyber security with data security will inevitably under-invest in ongoing data capabilities. But one of the lessons we ought to learn from recent breaches is that citizen data cannot be simply offloaded to ICT areas to manage.

Data uplift

Government agencies have received increased funding and technical support for cyber security hardening in recent years, combined with increased obligations for public reporting. A similar uplift in government data security is needed. With $9.9 billion invested in REDSPICE, comparatively little has been invested in data maturity.

Given the varying levels of data maturity across government, a dedicated data security program should seek to lift all agencies to a minimum standard. Minimum standards and common approaches not only improve data security, they also facilitate greater and more trusted data sharing between agencies.

Funding should be provided for all agencies to prioritise the following:

- Create data inventories that provide a clearer picture of what data agencies hold, where they hold it, and who the data custodians are.
- Establish clear internal procedures for managing data breaches and reporting them in a timely manner, consistent with OAIC best practice.
- Adopt the 'Five Safes framework' to assess different levels and types of data risk, and apply proportionate controls for citizen data. Think of the Five Safes as the Essential Eight of data sharing. The framework is already in use with the Australian Bureau of Statistics and the Australian Institute of Health and Welfare, as well as the national statistical organisations of the UK and New Zealand.

Action on these fronts will go some way towards cleaning up the data swamps that currently proliferate across government.

Of course, good data practices can only be sustained by a capable workforce. Bureaucrats cannot manage what they do not understand and data literacy in government remains low. The 2021 Australian Public Service (APS) Agency Survey found that 70 per cent of agencies identified data as a top skill shortage, second only to ICT or digital skills.[4] It's telling that human error is responsible for the majority of Australian Government data breaches, whereas data breaches in industry are mostly caused by malicious cyber attacks.

Current workforce initiatives tend to rely on staff to be responsible for their technical uplift with limited guidance or support from managers. Agencies should be more proactive and accelerate training for generalist APS staff to become more data literate. Ideally this would include foundational data and privacy training for all staff who work with citizen data, as well as more advanced training for staff who are data custodians or otherwise authorised to make decisions about data access and use.

Looming privacy reforms

The government is currently considering 116 proposals from the *Privacy Act* review. These will be the most significant changes to privacy laws in nearly half a century and government agencies won't be immune. Proposal 27.1, for example, would, if adopted, introduce a statutory cause of action for serious invasions of privacy by any person or entity,

With privacy reforms on the horizon, additional funding should be provided to OAIC to conduct independent privacy impact assessments (PIAs) of highly sensitive datasets held by government agencies, such as identifiable health data and movement records, which are both subject to complex and overlapping legislative requirements. OAIC should perform checks on how government agencies are protecting the data they collect and make recommendations for improvement. In limited circumstances, OAIC's remit should include confidential PIAs of data held by national security agencies if a potential breach would severely harm the privacy of Australians.

Privacy advocates have long criticised the underfunding of OAIC, which has hampered its ability to enforce privacy law, much less educate and advise. OAIC cannot and should not assess all data. But with better resourcing, it can be more active in helping public sector organisations understand the value and risks of its datasets and meet public expectations for their protection.

Finally, accountability mechanisms ought to be strengthened. A privacy code for Australian Government agencies has existed under the *Privacy Act* since 2017.[5] Without reporting mechanisms though, compliance is mixed. An updated code should require Secretaries to report publicly to OAIC on whether their agencies are meeting baseline standards like maintaining a data inventory, having a privacy management plan, and conducting PIAs. It would also encourage Secretaries to seriously think about their agencies as big data organisations.

Government as an exemplar

In June, a Data and Digital Government Strategy was quietly released for consultation. The strategy is welcome and offers some positive starting points for improving how the APS uses and protects citizen data. However, the devil is in the detail of what the government is willing to fund and how agencies will be held accountable.

For too long, data security has been a blind spot that attracted no dedicated investment and expertise, or was left to cyber security fixes that inevitably prove inadequate.

But if the government refuses to look critically at its own data security practices, it is only a matter of time before a government agency is responsible for a far worse data breach than Optus, Medibank, or Latitude. With the government signalling an increasingly interventionist approach to protecting citizen data, government itself needs to walk the talk on good data security and lead by example.

Notes

1. 'Notifiable Data Breaches Report: January–June 2021', *Office of the Australian Information Commissioner*, 23 August 2021, https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-januaryjune-2021.
2. 'Cyber Security Strategies of Non-Corporate Commonwealth Entities', *Australian National Audit Office*, 19 March 2021, https://www.anao.gov.au/work/performance-audit/cyber-security-strategies-non-corporate-commonwealth-entities.
3. Rachael Falk, 'No, Optus doesn't need to keep your sensitive information for so long', *Sydney Morning Herald*, 25 September 2022, https://www.smh.com.au/business/consumer-affairs/no-optus-doesn-t-need-to-keep-your-sensitive-information-for-so-long-20220925-p5bkt6.html.
4. *Australian National Audit Office*, op. cit.
5. 'Privacy (Australian Government Agencies — Governance) APP Code 2017', *Federal Register of Legislation*, 26 October 2017, https://www.legislation.gov.au/Details/F2017L01396.

About the authors

Olivia Shen is a Director at the ANU National Security College. She has worked in number of national security roles in government, most recently in data policy and artificial intelligence. She has been a visiting scholar at the Lowy Institute and a Fulbright Scholar at the Centre for Strategic and International Studies.

About the series

Policy Options Papers offer concise evidence-based recommendations for policymakers on essential national security issues. Papers in this series are peer-reviewed by a combination of expert practitioners and scholars.

David M. Andrews is the series editor and Acting Policy Manager at the ANU National Security College. He is responsible for mobilising the College's research and resident expertise to influence and inform current public policy debates.

About the College

The National Security College (NSC) is a joint initiative of The Australian National University and Commonwealth Government. The NSC offers specialist graduate studies, professional and executive education, futures analysis, and a national platform for trusted and independent policy dialogue.

E national.security.college@anu.edu.au

W nsc.anu.edu.au

@NSC_ANU

National Security College