Data Sharing in the Australian Public Sector after the Optus and Medibank Incidents: Taking Reasonable Steps to Prevent Data Breaches

Serena Syme Hildenbrand*

Abstract

In this article I identify weaknesses in the framework for public sector data sharing in Australia. Many Australian public sector agencies must share personal information they hold, potentially increasing the risk of a data breach. I consider the legal standard expected of data holders under the *Privacy Act 1988* (Cth) to take 'reasonable steps' to protect the data, including in light of the 2022 Optus and Medibank breaches. For public sector data, legislated data sharing frameworks also apply, overriding some statutory protections and introducing potential areas of weakness and confusion. One concern is public sector reliance on the unsuitable 'Five Safes' data sharing principles, adopted into statutes with an apparent absence of critical examination. Data sharing agreements ('DSAs') may assist, but often fail to do so due to vague standards and contractual omissions. To meet the reasonable steps standard, I argue that public sector data holders should ensure that their DSAs require data recipients to have appropriate security governance and risk management in place (ideally including compliance with an independent security standard) and impose obligations regarding data retention, staff training, and auditing. To assist in meeting the reasonable steps standard, security risk assessments should also be undertaken as standard data sharing practice.

Please cite this article as:
Serena Syme Hildenbrand, 'Data Sharing in the Australian Public Sector after the Optus and Medibank Incidents: Taking Reasonable Steps to Prevent Data Breaches' (2025) 47 *Sydney Law Review* 21383: 1–34 <https://doi.org/10.30722/slr.21383>.

* PhD candidate, Deakin University, Faculty of Business and Law, Deakin Law School, Burwood, Victoria, Australia; Associate Director of Data Sharing (driver and vehicle data), Department of Transport & Planning, Victoria, Australia. Email: shildenbrand@deakin.edu.au.
ORCID iD: https://orcid.org/0009-0004-2664-5381. The views expressed in this article are my own and not necessarily those of the Department. I thank my supervisory team of Shiri Krebs, Matthew Groves and Bruce Chen for their ongoing support and valuable input.

I Introduction

In September 2022, the Optus data breach exposed the personal data of 9.8 million customers.[1] The identity credentials of many of those customers were compromised, requiring them to obtain new credentials to prevent identity fraud.[2] The breach was triggered by an unidentified hacker accessing personal information through a system vulnerability. Clare O'Neil, the Australian Government Minister for Home Affairs, characterised it as a 'basic' attack where Optus 'effectively left the window open'.[3] A few weeks after the Optus data breach, health insurer Medibank experienced a similarly serious breach, resulting in the exposure of 9.7 million personal records including health information, some of which was published.[4] This was an intentional attack by a Russian cyber-crime gang, using stolen login information.[5] Due to the sensitivity of this data, Minister O'Neil described the Medibank breach as 'the single most devastating cyber-attack we have experienced as a nation'.[6] Victoria Police reported that at least 11,000 cybercrime incidents were linked to the Medibank breach.[7] A number of regulatory and civil actions have been brought against both Optus and Medibank, detailed further below in Part II.

These exposures of private sector data were truly damaging,[8] and it is not difficult to imagine a similar scenario playing out with sensitive public sector data maintained by Australian governments. As an example, the National Exchange of Vehicle and Driver Information System ('NEVDIS') has been used since 1998 to collect driver and vehicle information from every Australian state and territory with

---

1 Commonwealth, *Parliamentary Debates*, House of Representatives, 26 September 2022, 1500 (Clare O'Neil, Minister for Home Affairs and Minister for Cybersecurity). See also Ben Knight and staff, 'Optus Data Breach Class Action Launched for Millions of Australians Caught Up in Cyber Attack', *ABC News* (online, 21 April 2023) <https://www.abc.net.au/news/2023-04-21/optus-hack-class-action-customer-privacy-breach-data-leaked/102247638>.

2 Lucy Cormack, '"It's Almost a Fluke": Why NSW Drivers' Licences Have Largely Been Spared in Optus Hack', *The Sydney Morning Herald* (online, 1 October 2022) <https://www.smh.com.au/politics/nsw/it-s-almost-a-fluke-why-nsw-drivers-licences-have-largely-been-spared-in-optus-hack-20220929-p5bm1v.html>.

3 Clare O'Neil, Minister for Home Affairs (Cth), 'Interview with ABC 7:30' (transcript, 26 September 2022) <https://minister.homeaffairs.gov.au/ClareONeil/Pages/interview-abc-730-26092022.aspx>; Jake Evans, 'Home Affairs Minister Clare O'Neil says Optus "Left the Window Open" for Cyber Criminals to Conduct Simple Hack', *ABC News* (online, 28 September 2022) <https://www.abc.net.au/news/2022-09-26/home-affairs-minister-blames-optus-for-cyber-attack-hack/101474636>.

4 Clare O'Neil, Minister for Home Affairs (Cth), 'Cyber Sanctions in Response to Medibank Private Cyber Attack' (Joint Media Release with Richard Marles and Penny Wong, 23 January 2024) <https://minister.homeaffairs.gov.au/ClareONeil/Pages/cyber-sanctions-in-response-to-medibank-private-cyber-attack.aspx>. See also Tiffanie Turnbull, 'Medibank Hack: Russian Sanctioned over Australia's Worst Data Breach', *BBC News* (online, 23 January 2024) <https://www.bbc.com/news/world-australia-68064850>.

5 O'Neil, 'Cyber Sanctions in Response to Medibank Private Cyber Attack' (n 4); Turnbull (n 4).

6 O'Neil, 'Cyber Sanctions in Response to Medibank Private Cyber Attack' (n 4); Turnbull (n 4).

7 Victoria Police, Submission No 34 to Joint Committee on Law Enforcement, Parliament of Australia, *Inquiry into the Capability of Law Enforcement to Respond to Cybercrime* (December 2023) 19.

8 Note also the July 2025 Qantas data breach, which exposed the personal information of 5.7 million individuals: see, eg, Qantas, 'Update On Qantas Cyber Incident: Wednesday 9 July 2025' (Media Release, 9 July 2025) <https://www.qantasnewsroom.com.au/media-releases/update-on-qantas-cyber-incident-wednesday-9-july-2025/>; Maurice Blackburn Lawyers, 'Compensation Sought on behalf of Nearly Six Million Aussies Caught Up in Massive Qantas Data Breach' (Media Release, 18 July 2025) <https://www.mauriceblackburn.com.au/media-centre/media-statements/2025/compensation-sought-on-behalf-of-aussies-caught-up-in-qantas-data-breach/>.

the combined database managed by Austroads, the association of Australian and New Zealand transport agencies.[9] Jurisdictions share data with NEVDIS daily; it holds millions of sensitive records of driver licence details, representing every current Australian driver. Should NEVDIS data sharing pathways or databases be compromised, the damage — including the need to replace driver licences — would far exceed the Optus and Medibank breaches. While NEVDIS contains personal information, risks also exist with public sector data sharing initiatives involving de-identified data. An example is the National Disability Data Asset ('NDDA'), which will bring together de-identified data on people with disability from all states and territories to boost research, policy development and service delivery around disability issues.[10] Its privacy impact assessment highlighted re-identification of the data as an ongoing risk requiring monitoring[11] given that the NDDA will contain sensitive information about vulnerable people, such as disability level/type, medical and treatment data, offender and victim records, housing status and welfare payments.[12]

Much has been written on the Optus and Medibank breaches and the threat they pose to customers' security and company reputations. Malicious attacks such as these are data breaches of great concern, but the term 'data breach' encompasses broader actions and consequences. The Office of the Australian Information Commissioner ('OAIC') defines a data breach as 'an unauthorised access or disclosure of personal information, or loss of personal information'.[13] A data breach can occur without malicious intent, simply through human error or failures of process or technology.[14] It can arise in relation to any activity involving personal information: collecting and holding customer information, as Optus and Medibank did; data use; data destruction; and most relevantly to this article, data sharing (where data is transferred from one data holder to another for a specific purpose).

In this article I focus on the legal obligations of organisations handling personal information to protect against data breaches, with a particular focus on public sector data holders and sharers. Government data holders are often required to manage large volumes of personal customer data, and public sector data sharing

---

9 'NEVDIS', *Austroads* (Web Page) <https://austroads.com.au/drivers-and-vehicles/nevdis>.

10 Amanda Rishworth MP, 'Governments Come Together to Deliver National Disability Data Asset' (Media Release, 9 June 2023) <https://ministers.dss.gov.au/media-releases/11431>. See also 'National Disability Data Asset Factsheet', *National Disability Data Asset* (Web Page) <https://www.ndda.gov.au/ndda-factsheet>.

11 National Disability Data Asset ('NDDA'), *Summary of the 2023 Privacy Impact Assessment* (Report) <https://www.ndda.gov.au/summary-pia-report>.

12 NDDA, *Interim Learnings from Test Case Analyses* (Report, September 2021) <https://www.ndda.gov.au/research-projects/pilot-phase-and-findings>.

13 Office of the Australian Information Commissioner (Cth) ('OAIC'), *Data Breach Preparation and Response: A Guide to Managing Data Breaches in accordance with the Privacy Act 1988 (Cth)*, (Guidance Material, June 2024) 8 <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>. See also the narrower definition of 'eligible data breach' in *Privacy Act 1988* (Cth) s 26WE ('*Privacy Act*'), which triggers mandatory notification to the OAIC under s 26WL of the *Privacy Act*.

14 See, eg, the OAIC data breach notification form, which requires the organisation to advise whether the incident was caused by malicious or criminal attack; system fault; or human error: OAIC, 'Notifiable Data Breach Form' <https://www.oaic.gov.au/__data/assets/pdf_file/0008/2240/oaic-ndb-form-for-training-purposes-only.pdf>.

(such as for NEVDIS, the NDDA and other purposes including law enforcement) is indispensable to meet legislative obligations and public expectations. However, the act of sharing information may increase the risk of a data breach. Personal information may be more vulnerable during the transfer itself,[15] and its security after transfer depends on the data recipient's conduct and security environment. Data recipients may also on-share the data with third parties, adding additional risk.

In Part II of this article I analyse the relevant legal obligations, starting with the OAIC's documented approach to assessing whether an Australian government or private sector organisation impacted by a data breach discharged its obligations under the *Privacy Act 1988* (Cth) ('*Privacy Act*'), specifically by reference to data security obligations imposed under that Act by Australian Privacy Principle ('APP') 11.[16] I also consider the various legal actions and grounds asserted against Optus and Medibank to illustrate the standard a data holder is expected to apply to prevent data breaches.

In the public sector context, an additional source of legal obligations is data sharing legislation such as the *Data Availability and Transparency Act 2022* (Cth) ('*DAT Act*').[17] The *DAT Act* encourages public sector data sharing — there is no equivalent legislation applicable to the private sector. Although it is intended to operate consistently with the *Privacy Act* and APP 11, I explore how the *DAT Act* overlay adds complexity and operational weaknesses to the task of protecting public sector data, potentially undermining *Privacy Act* protections and confusing public servants involved in data sharing management. I highlight why this is cause for concern, given the significance and sensitivity of such data.

To explore these issues, in Part III I focus on data sharing, describing the legislative framework applicable to public sector data sharing in Australia, and identifying gaps arising from the more recent overlay of the *DAT Act* provisions on the existing *Privacy Act* protective framework. In particular, I highlight the role of state and federal data sharing legislation such as the *DAT Act* in the widespread adoption and application of the Five Safes framework ('Five Safes') as the de facto standard for sharing public sector data in Australia. Unfortunately, the Five Safes is deeply flawed and regrettable in its application to personal information, introducing areas of weakness in protecting such data.

In Part IV I look at the additional protection offered by Data Sharing Agreements ('DSA's) required by data sharing legislation. I analyse four public sector DSA templates, together with relevant guidance, to assess whether the DSAs commonly used by the Australian public sector assist in redressing the weaknesses introduced by application of the Five Safes. Overall, I conclude that the DSAs add value, but tend to be overly vague in their application, perpetuating areas of weakness.

---

15 Ahmed Albugmi, Madini O Alassafi, Robert Walters and Gary Wills, 'Data Security in Cloud Computing' (2016) *2016 Fifth International Conference on Future Generation Communication Technologies (FGCT)* 55, 56.

16 *Privacy Act* (n 13) sch 1 ('*Australian Privacy Principles*') APP 11.

17 *Data Availability and Transparency Act 2022* (Cth) ('*DAT Act*').

What can be done about these gaps in protection introduced by data sharing legislation? Absent amendments to that legislation, in Part V of this article I propose additional protections that government data holders should include in their DSAs to assist in both protecting data subjects and mitigating these risks. In Part VI I conclude that following major data breaches such as Optus and Medibank, public sector agencies would be well advised to apply a higher level of data protection. At its most simple, this can be achieved by putting stronger DSAs in place and monitoring compliance with them, and performing a security risk assessment for each data share.

II The Reasonable Steps Standard under Information Privacy Legislation

A *Australian Information Privacy Frameworks: The Privacy Act 1988 (Cth) and State Counterparts*

The *Privacy Act* establishes the legislative framework for information privacy at the federal level, covering the data activities of 'APP entities' — federal public sector agencies as well as organisations with annual turnover exceeding $3 million (including Optus and Medibank).[18] Section 13 of the *Privacy Act* provides that an APP entity interferes with the privacy of an individual if it fails to comply with an APP in relation to that individual's personal information, and s 15 requires APP entities to comply with the *Australian Privacy Principles*. Similar provisions can be found in state and territory information privacy laws covering public sector agencies,[19] with most containing at least one privacy principle focused on information security, paralleling APP 11:

> 11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:
>
> (a) from misuse, interference and loss; and
>
> (b) from unauthorised access, modification or disclosure.
>
> 11.2 If:
>
> (a) an APP entity holds personal information about an individual; and
>
> [(b)–(d) [that information is no longer needed or required to be retained and is not contained in a Commonwealth record];]
>
> the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.[20]

---

18 *Privacy Act* (n 13) ss 6(1) (definitions of 'APP entity', 'agency' and 'organisation'), 6C.

19 *Information Privacy Act 2014* (ACT) ('*ACT IPA*'); *Privacy and Personal Information Protection Act 1998* (NSW) ('*NSW PPIPA*'); *Information Act 2002* (NT) ('*NT IA*'); *Information Privacy Act 2009* (Qld) ('*Qld IPA*'); *Privacy and Data Protection Act 2014* (Vic) ('*Vic PDPA*');); *Personal Information Protection Act 2004* (Tas) ('*Tas PIPA*'); *Privacy and Responsible Information Sharing Act 2024* (WA) ('*WA PRISA*'). South Australia has a relevant Cabinet Administrative Instruction, which does not offer equivalent protection: see *Information Privacy Principles (IPPS) Instruction* (Premier and Cabinet Circular PC012). Note that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) amends the *Qld IPA* from 1 July 2025, and the *WA PRISA* is yet to fully commence.

20 *Australian Privacy* Principles (n 16) APP 11. See also the equivalent information/territory protection provisions ('IPP/TPP') under state and territory legislation, which have some drafting differences but

This clause is considered the 'most operative and directly relevant protection of personal data obligation in Australian law',[21] and is identified by the OAIC as 'key to minimising the risk of a data breach'.[22] While the new *Cyber Security Act 2024* (Cth) requires APP entities to report to the Australian Signals Directorate any ransomware payments to hackers and facilitates voluntary data breach notifications by any Australian organisation (including with limited use protections around information shared), it does not change the central role of APP 11 in setting the standard for preparedness.[23]

APP 11 raises some important concepts. First, it references a central concept in privacy regulation: 'personal information', defined as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable'.[24] My references in this article to personal information point back to that key underlying definition. Second, APP 11 indicates that obligations are triggered if the entity 'holds' that information, defined to mean that the entity 'has possession or control of a record that contains the personal information'.[25] The personal information does not need to be in the entity's possession for APP 11 to apply, provided the entity 'has the right or power to deal with the personal information'.[26] This is often interpreted to mean that a public sector data holder continues to 'hold' personal information it collects and maintains even after it has shared it, because it retains control through legal means (such as under a DSA).[27]

Third, APP 11 imposes a reasonableness standard on organisations in managing the security of personal information they hold ('the reasonable steps standard').[28] The OAIC guidance on APP 11 indicates that reasonable steps will depend on a variety of factors, all as assessed by the OAIC, including: the organisation's size and resources; the amount and sensitivity of personal information held; the potential harms; and the feasibility of security measures.[29] The reasonable

---

a similar effect: *NSW PPIPA* (n 19) cl 12 (IPP 12); *Vic PDPA* (n 19) sch 1 IPP 4; *Qld IPA* (n 19) sch 3 IPP 4; *ACT IPA* (n 19) sch 1 pt 1.4 TPP 11; *Tas PIPA* (n 19) cl 4 (IPP 4); *NT IA* (n 19) sch 2 IPP 4; *WA PRISA* (n 19) sch 1 (IPP 4) (not yet in effect).

21 Joel Lisk, 'Data Security in Australia: The Obligation to Protect' (2023) 97(10) *Australian Law Journal* 749, 757.

22 OAIC, *Data Breach Preparation and Response* (n 13) 9.

23 *Cyber Security Act 2024* (Cth) pts 3–4. See also Australian Signals Directorate (Cth), 'Ransomware Payment and Cyber Extortion Payment Reporting', *Australian Cyber Security Centre* (Web Page) <https://www.cyber.gov.au/report-and-recover/report/ransomware-payment-and-cyber-extortion-payment-reporting>.

24 *Privacy Act* (n 13) s 6(1) (definition of 'personal information').

25 Ibid s 6(1) (definition of 'holds').

26 See, eg, OAIC, *Australian Privacy Principles Guidelines* (December 2022) 19 [B.84] <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines>.

27 See, eg, Office of the Victorian Information Commissioner ('OVIC'), *Guidelines to the Information Privacy Principles* (online, 4th ed, 2019) [4.59]–[4.62] <https://ovic.vic.gov.au/privacy/guidelines-to-the-information-privacy-principles/>.

28 This is not a narrow *Wednesbury* standard of reasonableness as applied under judicial review: *Associated Provincial Picture Houses Ltd v Wednesbury Corporation* [1948] 1 KB 223. The OAIC guidance indicates that the APP entity must take positive steps to protect the data: OAIC, *Australian Privacy Principles Guidelines* (n 26) 4 [11.7]–[11.8].

29 OAIC, *Australian Privacy Principles Guidelines* (n 26) 4 [11.7]–[11.8]; OAIC, *Guide to Securing Personal Information: 'Reasonable Steps' to Protect Personal Information* (2018) <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information?external-uuid=2bc65cdd-f52f-4981-9f16-f4ec8716b507>.

steps standard is applied by the OAIC in its own discretion and has not yet received 'substantial judicial consideration'.[30] But the OAIC's approach is evident in a number of documented investigations of data breaches, particularly breaches affecting Sony Playstation Network ('Sony') in 2011,[31] Epsilon in 2011,[32] Adobe in 2013,[33] Avid Life Media ('Ashley Madison') in 2015,[34] Australian Recoveries & Collections ('ARC') in 2015,[35] and Marriott International ('Marriott') in 2015–18.[36]

The OAIC's investigations show that while the reasonable steps standard is demanding, it does not require a data holder to 'design impenetrable systems'.[37] But it is helpful if the data holder can demonstrate compliance with independent information security standards. Technology companies Epsilon and Sony were found by the Commissioner (in separate matters) to have met the reasonable steps standard, at least partially because they were operating in compliance with an independent security standard, ISO 27001[38].[39]

The investigations also demonstrate that security measures are inadequate if they are not effectively implemented. In a joint report with the Canadian Privacy Commissioner into the Ashley Madison breach, the OAIC found that even though security safeguards existed, the reasonable steps standard was not met because the safeguards were not coherently implemented with an appropriate governance framework including a security policy, a risk management process and adequate staff training in privacy and security.[40] Such a security framework needs to include adequate monitoring, as noted by the OAIC in relation to Marriott, which was found to have fallen short of reasonable steps largely due to deficiencies in security monitoring.[41]

Appropriate contractual protections are key if the data is in the hands of a third party. The Blood Service breach involved the inadvertent internet publication

---

30 Lisk (n 21) 757. This may change with the Optus and Medibank cases.

31 *Sony PlayStation Network/Qriocity: Own Motion Investigation Report* [2011] AICmrCN 16 (29 September 2011) ('*Sony Report*').

32 *Dell Australia and Epsilon: Own Motion Investigation Report* [2012] AICmrCN 2 (1 June 2012) ('*Epsilon Report*').

33 *Adobe Systems Software Ireland Ltd: Own Motion Investigation Report* [2015] AICmrCN 1 (1 June 2015).

34 OAIC, *Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner and Acting Australian Information Commissioner* (Investigation Report, 24 August 2016) ('*Ashley Madison Investigation Report*') <https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-decisions/investigation-reports/ashley-madison-joint-investigation>.

35 OAIC, *Australian Recoveries & Collections: Enforceable Undertaking* (Decision, 31 August 2016) ('*ARC Enforceable Undertaking*') <https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-decisions/enforceable-undertakings/australian-recoveries-and-collections-enforceable-undertaking>.

36 OAIC, *Marriott International: Enforceable Undertaking* (Decision, 7 February 2023) <https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-decisions/enforceable-undertakings/marriott-international-enforceable-undertaking>.

37 *Adobe Systems Software Ireland: Own Motion Investigation Report* (n 33).

38 International Organization for Standardization, *ISO/IEC 27001: Information Security, Cybersecurity And Privacy Protection — Information Security Management Systems — Requirements* (3rd ed, 2022).

39 Sony had implemented 'internal information technology security standards that are based on the international information security standard ISO/IEC 27001': *Sony Report* (n 31). See also *Epsilon Report* (n 32).

40 *Ashley Madison Investigation Report* (n 34) 4 [8]–[10].

41 *Marriott International: Enforceable Undertaking* (n 36) [18].

of personal information by a contractor. The OAIC identified a failure to satisfy the reasonable steps standard — despite the Blood Service's security framework with adequate safeguards — because the security requirements in the outsourcing contract 'were not clearly articulated or proportional to the scale and sensitivity of the information held'.[42]

Other missing protections identified by the OAIC were appropriate data retention practices, staff training in privacy and security, and auditing. The Blood Service and Ashley Madison were both criticised for retaining personal information longer than needed.[43] A lack of staff training contributed to both the ARC breach and Ashley Madison breach.[44] Auditing was raised as an issue in relation to the Blood Service, which had no reporting or assurance mechanisms in its outsourcing contract.[45]

These investigations highlight that the reasonable steps standard of data protection as applied by the OAIC is relatively demanding. The OAIC's investigations and guidance indicate that for an organisation to achieve and maintain the standard, considerable focused action is required, including:

- implemented security and risk management policies (covering system monitoring);
- appropriate contractual obligations on third parties and contractors;
- relevant data retention practices;
- staff training in privacy and security; and
- auditing or reporting on contract compliance.

Demonstrated compliance with independent security standards, such as the Australian Government's Protective Security Policy Framework,[46] ISO 27001 or the Australian Cyber Security Centre's Essential Eight security framework ('Essential Eight'),[47] will assist.

The 2022 *Privacy Act Review Report* recommended changes to strengthen APP 11, of which the following were accepted by the Government:

(a) Amending APP 11.1 to indicate that 'reasonable steps' includes both technical and organisational measures. This amendment is included in s 34 of the *Privacy and Other Legislation Amendment Act 2024* (Cth)

---

42 OAIC, *DonateBlood.com.au Data Breach (Australian Red Cross Blood Service)* (Decision, 7 August 2017) <https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-decisions/investigation-reports/donateblood.com.au-data-breach-australian-red-cross-blood-service>.

43 Ibid; *Ashley Madison Investigation Report* (n 34) 24 [114]–[116].

44 *Ashley Madison Investigation Report* (n 34) 18 [78]; *ARC Enforceable Undertaking* (n 35) [5.6].

45 OAIC, *DonateBlood.com.au Data Breach* (n 42).

46 'Applying the Protective Security Policy Framework', *Department of Home Affairs (Cth)* (Web Page) <https://www.protectivesecurity.gov.au/about/applying-protective-security-policy-framework>.

47 Australian Signals Directorate (Cth), 'Essential Eight', *Australian Cyber Security Centre* (Web Page) <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight>. Essential Eight assesses an organisation's cybersecurity maturity (ie, the extent to which security controls are developed and ingrained in that organisation) at levels 0–3, with a target maturity level of at least 2 appropriate for handling personal information.

('*2024 Amendment Act*'), requiring organisations to incorporate both types of measure in security protections.[48]

(b) Enhancing the OAIC's guidance on what constitutes 'reasonable steps'.[49]

These changes are likely to assist in clarifying and applying the reasonable steps standard in practice, without substantially amending APP 11's operational effect.

If an APP entity fails to meet this standard and a data breach ensues, it may be subject to enforcement mechanisms under the *Privacy Act*. This includes injunctive relief,[50] a complaints process,[51] and substantial fines for serious or repeated interferences.[52] The *2024 Amendment Act* added a suite of new enforcement mechanisms (most commencing in December 2024) such as:

- more flexible civil penalties for privacy infringement;[53]
- expansion of the orders available to the Federal Court of Australia to address privacy offences;[54]
- conferral on the Information Commissioner of increased powers around public inquiries, determinations and monitoring;[55]
- inclusion of a statutory cause of action for serious privacy invasions;[56] and
- the criminalisation of doxxing behaviours.[57]

The practical impact of these new enforcement mechanisms will soon emerge. But in the meantime, it is instructive to look at the legal avenues pursued, and claims made in the Optus and Medibank cases, outlined in the next section.

B *The Application of the Reasonable Steps Standard to the Optus and Medicare Claims*

The Optus breach arose from a vulnerability with an Application Programming Interface ('API'), effectively a gateway for data access. A coding error in 2018

---

48 Explanatory Memorandum, Privacy and Other Legislation Amendment Bill 2024 (Cth) 4 [12], 43 [99]–[102].

49 Attorney-General's Department (Cth), *Privacy Act Review Report* (2022) 224–6 <https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report>; Attorney-General's Department (Cth), *Government Response: Privacy Act Review Report* (2023) 33–4 <https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report> ('*Government Response*').

50 *Privacy Act* (n 13) s 80W.

51 Ibid ss 36, 52.

52 Ibid s 13G.

53 *Privacy and Other Legislation Amendment Act 2024* (Cth) sch 1 pt 8 ('*2024 Amendment Act*') amending *Privacy Act* (n 13) s 13G, inserting *Privacy Act* (n 13) ss 13H, 13J–13K. 'Doxxing' is the malicious publication of personal data for harassment: see *2024 Amendment Act* sch 3 inserting *Criminal Code Act 1995* (Cth) sch 1 (*Criminal Code*) ss 474.17C–474.17D.

54 *2024 Amendment Act* (n 53) sch 1 pt 9 inserting *Privacy Act* (n 13) s 80UA.

55 See, eg, *2024 Amendment Act* (n 53) sch 1 pt 10 inserting *Privacy Act* (n 13) pt IV div 3B; sch 1 pt 14 amending *Privacy Act* (n 13) pt VIB.

56 *2024 Amendment Act* (n 53) sch 2 adding *Privacy Act* (n 13) sch 2 (in force from 10 June 2025).

57 *2024 Amendment Act* (n 53) sch 3 inserting *Criminal Code* (n 53) ss 474.17C–474.17D. 'Doxxing' is the malicious publication of personal data for harassment.

weakened the protection of two Optus domains containing APIs. This coding error was detected by Optus and fixed in 2021 for one domain but not for the second, which was exploited by the hacker.[58] The weakness existed for four years prior to the breach and Optus had many opportunities to detect and correct it.[59] Submissions by the OAIC suggest that '[t]he cyberattack was not highly sophisticated … [i]t was carried out through a simple process of trial and error'.[60] The Medibank breach was caused by compromised login credentials. A contractor had saved Medibank passwords to his personal browser, allowing the hacker to steal the passwords and undertake multiple accesses to Medibank systems that were unprotected by multi-factor authentication and so poorly monitored that Medibank did not uncover the ongoing breach for almost two months.[61]

What options were open to the many Optus and Medibank victims? At the time, it was commonly accepted that enforcement avenues for individuals under the *Privacy Act* were inadequate.[62] The *2024 Amendment Act* includes mechanisms that may have benefited those victims. One is a tort for serious invasions of privacy, allowing natural persons to sue if they experience an intentional or reckless intrusion of a serious nature.[63] While this cause of action is not broadly relevant to data breaches, it may have utility in the most egregious cases of reckless behaviour.[64] As already noted, the *2024 Amendment Act* also increases civil penalties and extends the range of orders available to courts.[65] A more targeted solution recommended by the 2022 *Privacy Act Review Report* (which the Government accepted in principle but has not yet legislated) was the inclusion in the *Privacy Act* of a direct right of action to allow data breach victims to bring action against APP entities in respect of a breach of the Act and *Australian Privacy Principles*, seeking compensation for economic and non-economic loss and aggravated damages.[66] In agreeing 'in-principle' to this new enforcement mechanism, the Government noted that damages should be unlimited, but required a complainant to first undertake a complaints process to prevent court overload.[67] Such a right of action will assist in data breach cases should it be legislated.

Given there was no direct right of action under the *Privacy Act*, Optus and Medibank victims pursued other avenues: namely, representative complaints to the

---

58 Australian Communications and Media Authority ('ACMA'), 'Concise Statement', Submission in *Australian Communications and Media Authority v Optus Mobile Pty Ltd*, Federal Court of Australia, VID429/2024, 19 June 2024, 2–3 [8]–[14].

59 Ibid 2 [12]–[13].

60 Ibid 3 [15].

61 Australian Information Commissioner, 'Concise Statement', Submission in *Australian Information Commissioner v Medibank Private Ltd*, Federal Court of Australia, VID497/2024, 19 June 2024, [8]–[18] ('OAIC Concise Statement').

62 See, eg, Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final Report* (June 2019) 23–4 <https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report>.

63 *Privacy Act* (n 13) sch 2. The tort came into effect on 10 June 2025.

64 The tort is informed by the Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Report No 123, June 2014) ('*2014 ALRC Report*'): Explanatory Memorandum, Privacy and Other Legislation Amendment Bill (n 48) 8 [3]. The *2014 ALRC Report* specifically recommended that the tort not apply to data breaches because other available remedies were more appropriate: *2014 ALRC Report* (n 64) 122 [7.61]–[7.62].

65 See above nn 53–4.

66 Attorney-General's Department (Cth), *Government Response* (n 49) 19.

67 Ibid.

OAIC under s 36 of the *Privacy Act*, and class actions in the Federal Court of Australia.[68] The OAIC also brought a civil penalty action against Medibank under s 13G of the *Privacy Act*.[69] To what extent do these avenues of redress involve consideration of the reasonable steps standard?

Representative complaints under the *Privacy Act* concern an interference with privacy, so an investigation of data breach complaints can be expected to focus on the reasonable steps standard under APP 11. Such a process is low-cost to initiate and allows each class member's circumstances to be considered individually, with compensation available for loss and damage including non-economic loss.[70] The process is essentially inquisitorial, with the OAIC empowered to secure evidence and investigate the claim without application of the rules of evidence.[71] These complaints can be time consuming to resolve,[72] and the determination is non-binding, potentially requiring court action for enforcement, which will increase the time and cost before a complainant receives recompense.[73] The OAIC's approach to 'reasonable steps' is likely to be consistent with that detailed above in Part II(A).

The second avenue pursued is class actions in the Federal Court of Australia. The legal claims in such actions vary, but may include a negligence ground, as in the Optus class action.[74] Class actions are expensive and can take considerable time to reach a conclusion, often with litigation funders taking a significant portion of any damages awarded.[75] Despite strong interest from lawyers and litigation funders there

---

68 'Representative Complaints Update', *Office of the Australian Information Commissioner* (Web Page, 13 December 2023) <https://www.oaic.gov.au/newsroom/representative-complaints>; Knight and staff (n 1); Colin Kruger, 'Compensation for Medibank Hack Victims Could Be Fast-Tracked', *The Age* (online, 8 April 2024) <https://www.theage.com.au/business/companies/compensation-for-medibank-hack-victims-could-be-fast-tracked-20240405-p5fhrl.html?btis=>; Melissa Brown, 'Law Firm Launches Class Action on behalf of Millions of Customers Caught Up in Medibank Data Hack', *ABC News* (online, 5 May 2023) <https://www.abc.net.au/news/2023-05-05/medibank-data-breach-class-action-slater-gordon/102307106>.

69 *Australian Information Commissioner v Medibank Private Ltd* (Federal Court of Australia, VID497/2024, commenced 5 June 2024); 'OAIC Takes Civil Penalty Action against Medibank', *Office of the Australian Information Commissioner* (Web Page, 5 June 2024) <https://www.oaic.gov.au/newsroom/oaic-takes-civil-penalty-action-against-medibank>. The telecommunications regulator (ACMA) also brought action against Optus under the *Telecommunications (Interception and Access) Act 1979* (Cth), but the legal basis is beyond scope here due to its lack of general application to data breach defendants: *Australian Communications and Media Authority v Optus Mobile Pty Ltd* (Federal Court of Australia, VID429/2024, commenced 20 May 2024); see also Ry Crozier, 'Optus to Face ACMA-Filed Court Case over Data Breach', *IT News* (online, 23 May 2024) <https://www.itnews.com.au/news/optus-to-face-acma-filed-court-case-over-data-breach-608235>. Further, the Federal Government has applied cyber sanctions to the Russian hackers in the Medibank case: Penny Wong, 'Further Cyber Sanctions in Response to Medibank Private Cyberattack', (Joint media release with Richard Marles and Tony Burke, 12 February 2025) <https://www.foreignminister.gov.au/minister/penny-wong/media-release/further-cyber-sanctions-response-medibank-private-cyberattack>.

70 'Representative Complaints Update' (n 68).

71 See, eg, *Medibank Private Ltd v Australian Information Commissioner* (2024) 301 FCR 517, 540 [108]–[109].

72 Rose Dlougatch, 'Cyber-Insecurity: Data Breaches, Remedies and the Enforcement of the Right to Privacy' (2018) 25(4) *Australian Journal of Administrative Law* 219, 224.

73 *Privacy Act* (n 13) s 52(1B); Aiden Lerch and Sophie Whittaker, 'More Valuable Than Oil: The Application of Tort Law and Equity to Data Breach Cases' (2019) 27(2) *Tort Law Review* 100, 105.

74 *Robertson v Singtel Optus Pty Ltd* (Federal Court of Australia, VID256/2023, commenced 20 April 2023); Knight and staff (n 1).

75 Kruger (n 68).

has not yet been a successful data breach class action in Australia.[76] This contrasts with the United States, where negligence actions based on a failure to discharge a duty of care have been successful in class actions around data breaches.[77] A successful negligence action in Australia would require the court to identify a common law duty of care towards data subjects, which has not yet been established here as a legal basis for data breach compensation.[78] A class action might reference the reasonable steps standard[79] as part of the standard of care expected of a data holder in a negligence claim. Given that Australian courts have not yet recognised the duty of care, the relevant standard of care has not yet been considered or established by an Australian court.[80] Lerch and Whittaker refer to the approach taken by US courts, where the standard of care was assessed by considering the duties imposed on defendants by privacy legislation,[81] and conclude that '[i]t would therefore be reasonable for the [*Australian Privacy Principles*] to be the standard of care applicable in [Australian] data breach cases'.[82] But it is yet to be seen in practice, including whether a court's approach to applying the reasonable steps standard would align with the OAIC approach. Future decisions in data breach class actions (like Optus) may further develop our understanding of the standard.

Finally, as noted earlier, the OAIC is pursuing a civil penalty action against Medibank under s 13G of the *Privacy Act* for serious or repeated privacy interferences, focusing on whether Medibank met the reasonable steps standard under APP 11.[83] Medibank is only the third defendant faced with such an action.[84] An OAIC submission in this matter helpfully includes an Annexure listing expected security protections aligned with independent standards like the Essential Eight, consistent with the reasonable steps considerations detailed above.[85] Significant penalties apply for contraventions of s 13G — even though new higher s 13G penalties were introduced after the Medibank breach, applicable penalties in the Medibank case are up to $2.22 million for each contravention.[86] This civil penalty

---

76 Gavin Smith and Valeska Bloch, 'Where Are All the Data Breach Class Actions in Australia?', *Allens* (Blog Post, 17 October 2018) <https://www.allens.com.au/insights-news/insights/2018/10/pulse-where-are-all-the-data-breach-class-actions-in>.

77 Lerch and Whittaker (n 73) 109; Smith and Bloch (n 76). In 2017, 95% of US federal data breach class actions included negligence, with 65% listing it as the primary cause of action: Daniel M Filler, David M Haendler and Jordan L Fischer, 'Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data' (2022) 54(1) *Connecticut Law Review* 105, 117.

78 Amanda Beattie, Kieran Doyle and Nicole Gabryk, 'The Rise of Data Breach Class Actions: Legal Trends and Implications', *Wotton Kearney* (Blog Post, 26 October 2023) <https://www.wottonkearney.com.au/the-rise-of-data-breach-class-actions-legal-trends-and-implications/>.

79 See, eg, the Medibank claims: Brown (n 68).

80 Lerch and Whittaker (n 73) 113.

81 Ibid 110–1.

82 Ibid 114.

83 *Australian Information Commissioner v Medibank Private Ltd* (n 69).

84 Elizabeth Knight, 'Medibank on the Hook for Trillions But There's More at Stake than Money', *The Sydney Morning Herald* (online, 5 June 2024) <https://www.smh.com.au/business/companies/medibank-on-the-hook-for-trillions-but-there-s-more-at-stake-than-money-20240604-p5jj62.html>.

85 'OAIC Concise Statement' (n 61) Annexure B.

86 The *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* (Cth) commenced in December 2022 and increased s 13G penalties for a body corporate from $2.22 million to the higher of $50 million, three times the value of benefit or 30% of adjusted turnover. The *2024 Amendment Act* retained these penalty amounts while clarifying what conduct meets the threshold

action is an important mechanism to encourage better corporate behaviour, but does not compensate victims.

A public sector data holder impacted by a significant data breach is less likely to face a class action or civil penalty action. Even if a duty of care to prevent data breaches were established in Australia, courts may be reluctant to extend it to public sector data holders, given well-established judicial concerns around imposing new liabilities relating to government's failure to act (typically in a resource-constrained environment), and where the duties and obligations of government may differ from those of other entities.[87] The existence in Australia of a statutory duty on public sector agencies (such as an obligation under APP 11) is not usually enough to found a new duty of care.[88] For a representative complaint, a public sector APP entity will be in the same position as a public company like Optus or Medibank, and the OAIC will apply the APP 11 reasonable steps standard. In Part III below, I focus solely on the public sector, assessing whether public sector data sharing frameworks assist government data holders to meet the reasonable steps standard.

III Public Sector Data Sharing Frameworks

I have noted that public sector data holders are often required to share personal information for policy development, law enforcement and other purposes — and that data sharing potentially increases the risks of a data breach. In this Part I outline the importance of such data sharing and assess the impact of legislated public sector data sharing frameworks.

The Australian public sector holds vast quantities of data. In 2017, the Productivity Commission's report from its inquiry into the use of public and private sector data ('*Productivity Commission Report*') estimated a potential boost to economic output of up to $64 billion per year if public sector data were made more widely available.[89] The Report found that this value is not currently being realised, observing that 'numerous hurdles to sharing and releasing data are choking the use and value of Australia's data'.[90] One such hurdle is that data is 'systematically siloed in the public sector with little sharing between agencies or beyond'.[91] While the notorious 'Robodebt' program highlighted Federal Government cross-agency data sharing and data matching for welfare debt recovery, such data sharing activities are not widespread.[92] The *Productivity Commission Report* considered that the lack of

for s 13G: Explanatory Memorandum, Privacy and Other Legislation Amendment Bill (n 48) 20 [81]–[82].

87 Janina Boughey, Ellen Rock and Greg Weeks, *Government Liability: Principles & Remedies* (Lexis Nexis Butterworths, 2019) 412–18. There is also the concern that liabilities would be funded from the public purse: at 412.

88 Mark Aronson, Matthew Groves and Greg Weeks, *Judicial Review of Administrative Action and Government Liability* (Lawbook Co, 7th ed, 2022) 1237 [21.440].

89 Productivity Commission, *Data Availability and Use* (Inquiry Report No 82, 31 March 2017) 117–8 <https://www.pc.gov.au/inquiries/completed/data-access/report> ('*Productivity Commission Report*').

90 Ibid 2.

91 Ibid 145.

92 The Robodebt Scheme's cross-agency data activity relied on specific legislation — the *Data-matching Program (Assistance and Tax) Act 1990 (Cth)*, which regulates the use of tax file numbers across multiple agencies to detect incorrect payments: *Royal Commission into the Robodebt Scheme*

coordinated data sharing among public sector entities was contributing to 'fragmentation and duplication of data collection activities' and waste.[93] In this context, the types of data sharing exemplified by the NDDA and NEVDIS are encouraging. The Victorian test case undertaken as part of the NDDA pilot involved linking disability service data and mental health service data to study the population impacted by *both* disability and mental health and to assess which supports are most effective in improving outcomes.[94] This is the type of valuable data activity that is likely to attract community approval. Data sharing is also highly beneficial for law enforcement, including in fields such as child protection or domestic violence prevention where it may allow patterns of bad behaviour to be detected and addressed, ideally preventing harm.[95] NEVDIS falls in the law enforcement category, allowing the tracking of stolen vehicles across state borders and helping prevent vehicle cloning.[96] Safe, trusted and effective public sector data sharing is needed to allow such important initiatives to continue and increase. While the *Productivity Commission Report* displayed frustration with current data sharing practices and a strong desire to drive change, it recognised the importance of building social licence around data sharing, because otherwise such initiatives will be widely rejected and fail.[97] Importantly, one of the most critical components of social licence identified in the Report was trust, as achieved through '[e]mbedding genuine safeguards into Australia's data framework to assure people their data is being used safely'.[98] A key conclusion of the *Productivity Commission Report* was the need to free up government data using a legislated data sharing framework.[99] In evaluating this approach below, it is pertinent to keep the concepts of social licence and genuine safeguards in mind.

A *Data Sharing Frameworks: The* DAT Act *and State Counterparts*

The *Productivity Commission Report* recommendation led to the passage and 1 April 2022 commencement of the *DAT Act*, establishing a scheme under which Federal Government agencies may share public sector data with accredited users from the federal or state public sectors or Australian universities in specified circumstances,[100] with such sharing to be regulated by a new Office of the National Data Commissioner ('ONDC').[101] The *DAT Act* was pre-dated by some public sector data sharing Acts in the States all designed to facilitate public sector data sharing, such as the *Data Sharing (Government Sector) Act 2015* (NSW), the *Victorian Data*

(Final Report, July 2023) 11–13. This is the only data matching legislation at the federal level: 'Government Data Matching', *Office of the Australian Information Commissioner* (Web Page) <https://www.oaic.gov.au/privacy/privacy-legislation/related-legislation/government-data-matching>.

93 *Productivity Commission Report* (n 89) 153.

94 NDDA, *Interim Learnings from Test Case Analyses* (n 12) 18–25.

95 *Productivity Commission Report* (n 89) 147 (Box 3.4).

96 'NEVDIS' (n 9). Vehicle cloning is where a registered vehicle is used to hide the identity of a stolen vehicle.

97 *Productivity Commission Report* (n 89) 177.

98 Ibid 178.

99 Ibid 14.

100 *DAT Act* (n 17) s 13.

101 Ibid s 45.

Sharing Act 2017 (Vic) and the *Public Sector (Data Sharing) Act 2016* (SA).[102] Of these, the *Public Sector (Data Sharing) Act* 2016 (SA) is considered the broadest, because it covers law enforcement data and overrides all other state legislation.[103] The *DAT Act*, applying as it does to all public sector data in the hands of the Commonwealth, may have an even greater impact.[104] It is not mandatory for Federal Government agencies to conduct their data sharing under the auspices of the *DAT Act*; they may choose instead to conduct their sharing under a DSA or memorandum of understanding ('MOU')[105] provided they have identified an adequate legal basis for that sharing.[106] But because the *DAT Act* simplifies some sharing considerations, including by providing a clear legal basis for sharing for certain allowed purposes, it is likely that many organisations will employ it. For example, while NEVDIS does not rely on the *DAT Act*, it is possible that the NDDA will.

Chapter 2 of the *DAT Act* sets out specific 'authorisations', allowing sharing and handling of public sector data if specified conditions are met. Importantly, if the sharing is so authorised, s 23 provides that it may override all other laws (federal, state or territory).[107] This allows authorised data sharing to take precedence over secrecy provisions, which creates new risks for data protection. For example, both the *Child Care Act 1972* (Cth) s 12J and the *Age Discrimination Act 2004* (Cth) s 60 strictly restrict the use of personal or protected information held under those Acts, but such information could potentially be shared under the *DAT Act*. The *DAT Act* requires the sharing to be for one of three allowed purposes in s 15: the delivery of government services; informing government policy and programs; or research and development — not data sharing for law enforcement.[108] There are numerous other conditions in s 13, including that the sharing must be:

- consistent with constitutional requirements, including to an appropriate recipient (s 13(4));
- consistent with specified 'data sharing principles' set out in s 16 (s 13(1)(e));
- covered by and consistent with a valid DSA as defined in ss 18–19 (s 13(1)(c)–(d));

---

[102] The legislation is summarised in a NSW review of its Act: Department of Customer Service (NSW), *Review of the Data Sharing (Government Sector) Act 2015* (August 2021) 10–13 <https://www.parliament.nsw.gov.au/tp/files/80507/Statutory%20Review%20of%20the%20Data%20Sharing%20Government%20Sector%20Act%202015.pdf> ('*NSW Review*'). Western Australia now has new data sharing legislation, not yet in effect: *WA PRISA* (n 19).

[103] *NSW Review* (n 102) 12.

[104] *DAT Act* (n 17) s 9 (definition of 'public sector data'). This could include data collected by the Commonwealth from states and the private sector.

[105] A data sharing MOU is a non-binding DSA, often used between government parties because emanations of the same Crown cannot enter binding arrangements. In this article I treat a data sharing MOU as a DSA and refer to it as such.

[106] Revised Explanatory Memorandum, Data Availability and Transparency Bill 2022 (Cth) 5 [30]–[31]. Legal basis generally consists of an allowed head of sharing under privacy legislation, such as under *Australian Privacy Principles* (n 16) APP 6, together with a legislative power allowing the data holder to share data for that purpose.

[107] This implements the *Productivity Commission Report* recommendation regarding legal override: *Productivity Commission Report* (n 89) 333.

[108] *DAT Act* (n 17) s 15(1). Data sharing for law enforcement relies on *Australian Privacy Principles* (n 16) APP 6.2(e).

- subject to appropriate privacy protection in accordance with s 16E (ss 13(1)(g), (i)); and
- not otherwise prohibited under s 17 (s 13(2)(c)).

Civil penalties apply if data is nominally shared under a *DAT Act* authorisation but fails to comply with s 13.[109]

How might the *DAT Act's* legislative override impact the *Privacy Act*? While the override applies to any Australian legislation prohibiting sharing (including laws enacted after it), the *Privacy Act* is an exception.[110] The *DAT Act*'s legislative history indicates a strong intent for it to operate consistently with the *Privacy Act*.[111] The Revised Explanatory Memorandum for the DAT Bill specified that it was 'not intended to override the *Privacy Act*' and demonstrated an expectation that s 17(5) of the *DAT Act* would prohibit any data handling inconsistent with the *Privacy Act*.[112] Further, DSAs under the *DAT Act* must include terms binding the parties to comply with all *Australian Privacy Principles*.[113] Accordingly, the legislative override will not limit the *Australian Privacy Principles*, and the APP 11 reasonable steps standard will apply to all *DAT Act* sharing. But, in practice, the *DAT Act* contains weaknesses in protection, and its complexity raises the practical risk that public servants will view it as exhaustive and fail to meaningfully apply APP 11. The main weakness comes from its reliance on data sharing principles. The *Productivity Commission Report* evidenced suspicion towards the use of DSAs and MOUs in public sector data sharing, describing the MOUs as 'unnecessarily complicated and time consuming',[114] and recommending reliance instead on data sharing principles based on the Five Safes.[115] Ultimately, the *DAT Act* retained DSAs but required them to implement data sharing principles.[116] In Parts III(B)–(C) I assess these data sharing principles, a critical component of the *DAT Act* framework.

B *Data Sharing Principles Based on the Five Safes*

A feature of the *DAT Act* and other Australian legislative data sharing frameworks is the application of data sharing principles based on the Five Safes. The Five Safes is a framework for planning, designing and evaluating data access solutions.[117] It was devised at the United Kingdom ('UK') Office for National Statistics in the early 2000s to enable the sharing of confidential business survey data for research

---

109 *DAT Act* (n 17) s 14(1).

110 Revised Explanatory Memorandum (n 106) 39 [233]–[236].

111 See, eg, *DAT Act* (n 17) ss 3(b), 16E, 16F; Supplementary Explanatory Memorandum, Data Availability and Transparency Bill 2020 (Cth) 1 [3], 5 [11], 6 [20].

112 Revised Explanatory Memorandum (n 106) 39 [236]; see also at 29 [168]. The *DAT Act* (n 17) s 17(5)(a) bars sharing that would contravene a Commonwealth Act giving effect to international law, which the *Privacy Act* (n 13) does.

113 *DAT Act* (n 17) ss 16E(2), 16F. See also Supplementary Explanatory Memorandum (n 111) 101 [8].

114 *Productivity Commission Report* (n 89) 449.

115 Ibid 318.

116 *DAT Act* (n 17) ss 13(d), 16, 19(7).

117 Felix Ritchie, 'The "Five Safes": A Framework for Planning, Designing and Evaluating Data Access Solutions' (Conference Paper, Data for Policy 2017: Government by Algorithm?, September 2017) <https://uwe-repository.worktribe.com/output/880713> ('The "Five Safes"').

purposes.[118] This confidential data was not personal information— it related to businesses and not individuals. Subsequently, the Five Safes was used to disseminate detailed but anonymised census data.[119] In short, the Five Safes was designed to allow confidential (but not personal) data to be made available to academic researchers in a controlled way.[120] In recent years, the Five Safes' designer Felix Ritchie has increasingly publicised the Five Safes as an appropriate model for public sector data sharing,[121] representing a significant departure from the original use case.

Under the Five Safes, the prospective discloser must assess five dimensions of a data request, namely: the project, people, settings, data and outputs (see Table 1 summary below).[122] Each dimension requires certain controls to be imposed to ensure a 'safe' outcome: safe projects, safe people, and so on. The controls can be shifted and combined to produce appropriate sharing controls overall, and all five dimensions need to be assessed together to determine whether an adequate solution has been reached.[123]

Table 1: Elements of the Five Safes framework[124]

Dimension	Assessment scope
Safe projects	Legal, moral and ethical considerations, public benefit, valid statistical purpose
Safe people	Data user knowledge, skills and incentives
Safe settings	Practical controls on data access, including physical environment and compliance processes.
Safe data	Potential for re-identification of individuals in the data.
Safe outputs	Analysis of outputs to remove identifiable information.

The Five Safes is not prescriptive; 'it is a framework for thinking, but does not explicitly state a solution'.[125] It is not designed to identify the best solution, but rather a range of possible solutions in which the term 'safe' is regarded as a continuous measure, rather than as a binary 'safe' or 'unsafe'.[126]

[118] Felix Ritchie, 'Secure Access to Confidential Microdata: Four Years of the Virtual Microdata Laboratory' (2008) 2(5) *Economic & Labour Market Review* 29, 30.
[119] Ibid 31.
[120] Ibid 30.
[121] Ritchie, 'The "Five Safes"' (n 117) 3–4.
[122] Tanvi Desai, Felix Ritchie and Richard Welpton, 'Five Safes: Designing Data Access for Research' (Working Paper No 1601, Economics Working Paper Series, UWE Bristol Faculty of Business and Law, January 2016) 5 <https://uwe-repository.worktribe.com/output/914745>.
[123] Ibid 5–6.
[124] Ibid 8–16.
[125] Felix Ritchie and Elizabeth Green, 'Frameworks, Principles and Accreditation in Modern Data Management' (Working Paper, UWE Bristol Business School Working Papers in Economics, 2020) 2 <https://uwe-repository.worktribe.com/output/6790882>.
[126] Desai, Ritchie and Welpton (n 122) 15–16.

In 2015, the Australian Bureau of Statistics started using the Five Safes to share a wide variety of data.[127] The Five Safes was then adopted in Australian legislation, starting with the *Public Sector (Data Sharing) Act 2016* (SA).[128] The original 2020 Explanatory Memorandum for the *DAT Act* refers to the data sharing principles as 'a key safeguard to manage risks of sharing public sector data based on the internationally recognised five safes framework'.[129] A major Commonwealth data sharing agreement preceding the *DAT Act*, the 2021 *Intergovernmental Agreement on Data Sharing between Commonwealth and State and Territory Governments*, reflected this approach, including data sharing principles based on the Five Safes.[130] The Five Safes is now represented in a wide variety of Australian legislation and policy materials.[131] Unfortunately, this uncritical reliance on the Five Safes has introduced a significant area of weakness into Australian public sector data sharing.[132] The Five Safes is used in the UK, Canada and other countries, but it has achieved significantly greater purchase in Australia, with Ritchie and Green identifying Australia's public sector adoption of the framework both as 'a substantial leap beyond current practices in other countries' and also 'more of a risk than a piecemeal approach'.[133]

While the data sharing principles in s 16 of the *DAT Act* and further detailed in Part 2 of the *Data Availability and Transparency Code 2022* (Cth) ('*DAT Code*')[134] are openly based on the Five Safes, they are slightly modified, as outlined in Table 2 below.

Notice the differences between Tables 1 and 2: while the *DAT Act* purports to lean on an 'internationally recognised' framework,[135] the Five Safes is an academic framework rather than a legislative code, so its implementation unavoidably leads to potentially significant changes.[136]

---

127 Ibid 17; 'Five Safes Framework', *Australian Bureau of Statistics* (Web Page) <https://www.abs.gov.au/about/data-services/data-confidentiality-guide/five-safes-framework>.

128 'Sharing Public Sector Data', *Department of Treasury and Finance (SA)* (Web Page) <https://www.treasury.sa.gov.au/Our-services/information-sharing-data-analytics/information-sharing-in-south-australia/sharing-public-sector-data>.

129 Explanatory Memorandum, Data Availability and Transparency Bill 2020 (Cth) 23 [114].

130 *Intergovernmental Agreement on Data Sharing between Commonwealth and State and Territory Governments* (signed and entered into force July 2021) cls 5(b), 12.

131 See, eg, *NSW Review* (n 102) 28.

132 See, eg, Shiri Krebs and Lyria Bennett Moses, 'Data Sharing Agreements: Contracting Personal Information in the Digital Age' (2024) 48(1) *Melbourne University Law Review* 95, 107.

133 Ritchie and Green (n 125) 13.

134 The *Data Availability and Transparency Code 2022* (Cth) ('*DAT Code*') is made under the *DAT Act* s 126. The *DAT Code* s 5 requires a data sharing arrangement to be consistent with the data sharing principles.

135 See above n 129 and accompanying quote.

136 Further, several amendments were made to the data sharing principles through the legislative process: 'Data Availability and Transparency Bill 2022', *Parliament of Australia* <https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6649>.

Table 2: Five Safes framework, as reflected in the *DAT Act* and *DAT Code*

	DAT Act **Principle (s 16)**	***DAT Code*** **Data sharer must satisfy itself that project is consistent with this principle by:**
Safe Projects	Project is appropriate	Applying a public interest assessment (s 6) and ethics assessment (s 7).
Safe People	Data is only provided to appropriate persons	Addressing any conflict of interest (ss 8–10). Considering the attributes, qualifications, affiliations, expertise and experience of data recipients (ss 11–2).
Safe Settings	Data is handled in an appropriate environment	Considering whether reasonable and proportionate security standards are in place (s 13).
Safe Data	Only data reasonably necessary for purpose is handled, with appropriate protections	Considering whether data is reasonably necessary and whether it should be treated prior to sharing (s 14).
Safe Outputs	The only output is final and necessary	Considering the nature and use of the output (s 15).

C *Why Use of the Five Safes Framework Falls Short of the Reasonable Steps Standard*

Given its wide use throughout the Australian public sector, the Five Safes framework has received remarkably little formal scrutiny.[137] It was critiqued by 14 Australian privacy experts in their submission to a Senate Committee on the *DAT Act* who noted:

> Even in the field of de-identification, the Five Safes has been criticised as not fit for purpose. It is even less fit as a replacement for current legal and ethical criteria for sharing, because it was not designed to create an authority to share personal information in the first place.[138]

A community submission to a Western Australian privacy consultation ('Brennan et al WA Submission') expressed doubt whether the Five Safes was an effective methodology, noting incisively that the submission authors had 'been unable to locate any material produced by any privacy regulator in the world that endorses

[137] Chris Culnane, Benjamin IP Rubinstein and David Watts, 'Not Fit for Purpose: A Critical Analysis of the "Five Safes"' (Working Paper, 4 November 2020) 2 <https://doi.org/10.48550/arXiv.2011.02142>.

[138] Melanie Marks, Anna Johnston et al, Submission No 2 to the Senate Committee on the Data Availability & Transparency Bill, *Inquiry into the Data Availability and Transparency Bill 2020 and the Data Availability and Transparency (Consequential Amendments) Bill 2020* (17 February 2021) 8, citing Culnane, Rubinstein and Watts (n 137) <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Finance_and_Public_Administration/DataTransparency/Submissions>.

it',[139] and strongly recommending that it not be adopted in that State.[140] The most scathing assessment to date was a 2020 working paper by Culnane, Rubinstein and Watts, which asserted that the Five Safes framework is 'fundamentally flawed' and 'appropriates notions of safety without being anchored in any objective standard by which to assess or measure what is and is not safe'.[141] When these critiques are considered in the context of public sector data, it becomes clear that there are significant risks in relying on the Five Safes, as discussed below in Parts III(C)(1)–(4).

1 *The Five Safes Framework Has Critical Design Weaknesses*

Five critical design weaknesses identified in the Culnane, Rubinstein and Watts working paper and Brennan et al WA Submission are as follows.

(a) *The Five Safes Disregards Legal Considerations*

Because of its statistical origins, the framework appears oriented towards quantitative data,[142] which may explain why it appears to bypass legal protections and privacy rights.[143] Applicable laws, legal basis and privacy and security requirements are inadequately expressed — other than a passing mention of legal compliance under 'Safe projects'.[144] The Brennan et al WA Submission states that the Five Safes must only be used once the legal authority to share personal information has been identified.[145] Otherwise, non-compliance with law is likely; the UK Department of Education considered that it was fully complying with the Five Safes while sharing children's personal information with the private sector in contravention of applicable privacy laws.[146]

(b) *The Five Safes Uses an Unrealistic Concept of Safety*

The Framework relies on a theoretical concept of safety, unattached to real risks.[147] Further, the framework evaluates 'safety' rather than risk, a more familiar concept in most workplaces.[148] The Culnane, Rubinstein and Watts working paper describes

---

139 Pip Brennan, Mark Fitzpatrick, Juan Larranaga, Vicki O'Donnell, Maria Osman, Carol Petterson, Julia Powles, Chris Twomey and Ross Wortham, Independent Submission to the *Privacy and Responsible Information Sharing for the Western Australia Public Sector* Discussion Paper (2019), 13 <https://www.wa.gov.au/government/document-collections/what-we-heard-privacy-and-responsible-information-sharing>.

140 Ibid 14. In fact, the new WA legislation includes 'responsible sharing principles' modelled on the Five Safes, with which DSAs must comply: *WA PRISA* (n 19) s 175, sch 2.

141 Culnane, Rubinstein and Watts (n 137) 1–2.

142 Desai, Ritchie and Welpton (n 122) 4.

143 Culnane, Rubinstein and Watts (n 137) 2–3.

144 Desai, Ritchie and Welpton (n 122) 8.

145 Brennan et al (n 139) 13.

146 Emma Day, Kruakae Pothong, Ayça Atabey and Sonia Livingstone, 'Who Controls Children's Education Data? A Socio-Legal Analysis of the UK Governance Regimes for Schools and EdTech' (2024) 49(3) *Learning, Media and Technology* 356, 362: 'Only (deidentified) 'safe data' is meant to be shared by [government], but of the 84 … shares with commercial entities, 18 (23%) shares included either Level 1 "instant identifier" (e.g., full names, addresses, email addresses) or Level 2 "meaningful identifiers"'.

147 Culnane, Rubinstein and Watts (n 137) 4–6.

148 Ibid 6.

the use of 'safe' as 'emotive' and 'overly optimistic'.[149] In fact, the 'use of "safe" was a deliberate attempt to dismantle the binary meaning of safe/unsafe, and make it explicitly a relative concept'[150] — which may be poorly understood by the public servants applying it. The Brennan et al WA Submission denies that the Five Safes is a risk management framework at all.[151]

(c) *The Five Safes Relies on the Five Dimensions Being Independent When They Are Not*

The framework assumes that the safes are independent of one another.[152] But in practice they appear to depend on one another: 'if one safe fails it can bring down all or some of the rest', leading to comparisons with a 'house of cards'.[153]

(d) *The Five Safes Focuses on a Point in Time When Risks Extend across a Lifecycle*

The framework requires a point-in-time analysis, when the risks associated with personal information apply to its whole lifecycle.[154] The Brennan et al WA Submission notes that this base assumption of the Five Safes that risks are static is wrong; the risks of disclosure are dynamic and vary across the lifecycle.[155]

(e) *The Five Safes Does Not Apply Any Independent Standard of Data Security*

The Five Safes does not require compliance with any independent security standard, such as the Protective Security Policy Framework, ISO 27001 or Essential Eight: '[i]t appropriates notions of safety without being anchored in any objective standard'.[156]

2 *The Framework Does Not Adequately Address Personal Information*

Descriptions of the framework imply that it applies to de-identified data (many of the controls are intended to prevent identification of the data), but the framework does not make this explicit.[157] However, the Five Safes is now applied to the sharing of personal information under the *DAT Act* by Australian public sector agencies, without clear awareness that this contradicts its intent.[158]

---

149 Ibid 7.
150 Desai, Ritchie and Welpton (n 122) 15.
151 Brennan et al (n 139) 13.
152 Desai, Ritchie and Welpton (n 122) 6.
153 Culnane, Rubinstein and Watts (n 137) 8.
154 Ibid 2.
155 Brennan et al (n 139) 13.
156 Culnane, Rubinstein and Watts (n 137) 2.
157 See, eg, Desai, Ritchie and Welpton (n 122) 11. In their 2020 co-authored working paper, Ritchie and Green state that '[i]t could be argued that the common measure across all dimensions is "what is the risk of re-identification?"': Ritchie and Green (n 125) 9. But the framework is now being widely used in Australia for the sharing of personal information, where the likelihood of identification is 100%.
158 The Senate Standing Committee sought unsuccessfully to limit the *DAT Act* to de-identified information, which would have been appropriate: Senate Standing Committee for the Scrutiny of

3 *The Framework Demands a High Degree of User Sophistication*

The framework is described by Ritchie and others as 'explicitly relativistic, subjective and empirical',[159] where 'the use of the framework itself is no guarantee of good practice'.[160] In considering the framework as part of a Technical White Paper, the Australian Computer Society ('ACS') notes that 'several of the dimensions are highly dependent on judgement'.[161] These are concerning descriptors of a framework intended to be used by mid-level public servants to protect sensitive data. Such decision-making does not fall within an established professional skillset, and the subjectivity makes consistency of outcomes unlikely.

The ACS recommended the inclusion of additional dimensions, and also proposed quantified risk thresholds for each dimension.[162] Under the ACS' quantified approach, any data sharing project 'using personal information' would be assessed at 'Safe Level 1 – Not safe project', and would not proceed.[163] This means that the ACS has concluded that the Five Safes is not suitable for sharing personal information in *any* circumstances — and yet it remains the Australian public sector standard for the sharing of personal information.

4 *The Framework Is Poorly Suited for Adoption into Legislation*

How did Australian legislatures adopt the Five Safes as legislative principles that may be inconsistent with, and undermine, their existing laws? Especially when faced with fast-moving technologies, it is not unusual for legislatures to provide regulatory flexibility by recognising rules and guidelines developed by non-legislative bodies. Examples include industry codes and standards under both the *Telecommunications Act 1997* (Cth)[164] and the *Online Safety Act 2021* (Cth).[165] But in those contexts, the external document is reviewed and confirmed by the relevant regulator before being implemented. What is unusual here is for external principles to be included in a Bill, modified through the legislative process and adopted into legislation with minimal formal review and no rigorous assessment of the modifications. The roots of this development are the *Productivity Commission*

Bills, Parliament of Australia, *Scrutiny Digest* (Digest 1 of 2021, 29 January 2021) 5 [1.10] <https://www.aph.gov.au/-/media/Committees/Senate/committee/scrutiny/scrutiny_digest/2021/PDF/d01_21.pdf>.

159 Desai, Ritchie and Welpton (n 122) 21.

160 Ritchie and Green (n 125) 5.

161 Australian Computer Society ('ACS'), *Data Sharing Frameworks: Technical White Paper* (September 2017) 69 <https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Data-Sharing-Frameworks_FINAL_FA_SINGLE_LR.pdf>.

162 ACS, *Privacy in Data Sharing: A Guide for Business and Government* (November 2018) 18–19, 55–65 <https://www.acs.org.au/content/dam/acs/acs-publications/Privacy%20in%20Data%20Sharing%20-%20final%20version.pdf>. Notably, such thresholds are explicitly rejected by Ritchie and Green, who describe the lack of quantitative measures as a strength of the framework: Ritchie and Green (n 125) 11.

163 Ibid 57.

164 'About Industry Codes and Standards', *Australian Communications and Media Authority* (Web Page, 10 October 2023) <https://www.acma.gov.au/about-industry-codes-and-standards>. The page indicates that industry codes and standards are approved by the ACMA as the regulator.

165 'Industry Codes and Standards', *eSafety Commissioner* (Web Page, 23 May 2025) <https://www.esafety.gov.au/industry/codes>. The page indicates that codes are developed by industry and submitted as drafts to the eSafety Commissioner for review and publication.

Report's evident frustration with status quo data sharing and its recommendation to adopt a principles-based legislative framework weighted towards data openness.[166] A principles-based approach requires principles, so the *Productivity Commission Report* identified the Five Safes as the preferred approach — seemingly in reliance on the Australian Bureau of Statistics' prior adoption and an article co-authored by Ritchie, and in the absence of any independent evaluation of effectiveness.[167] Parliamentary scrutiny identified valid issues about the use of the data sharing principles — their potential to undermine consent; the failure to restrict sharing to de-identified data; the vagueness of the 'public interest' test; and the use of the *DAT Code* (a legislative instrument not subject to Parliamentary scrutiny) to flesh out the principles — but did not secure major changes to address these issues.[168] The impact is heightened by the *DAT Act*'s legislative override, which allows authorised data sharing in compliance with the data sharing principles to proceed despite other laws.[169] As Witzleb noted in 2023, it remains to be seen whether the *DAT Act* achieves the appropriate balance between protection and enabling appropriate use of government data.[170]

In a recent article, Green and Ritchie assessed critiques of the Five Safes including the Culnane, Rubinstein and Watts working paper and the Brennan et al WA Submission. Green and Ritchie dismissed them as 'misinterpretations' of the model, asserting without analysis that 'the problem is not the framework, but the implementation'.[171] The Green and Ritchie article did not tackle the critiques in any detail, focusing instead on promoting the Five Safes.[172] In relation to concerns that the Five Safes does not adequately recognise legal requirements, Green and Ritchie stated that 'modern data protection laws are explicitly multi-dimensional and recognise the impossibility of prescribing absolute standards',[173] seemingly misrepresenting the requirements of such laws.[174] The approach to defending the Five Safes in the Green and Ritchie article lacks academic rigour and should give pause to governments relying on it. In this light, recent comments by Ritchie and Whittard that 'in general [the Five Safes'] use as a framework is uncontroversial' seem deliberately misleading.[175]

---

166 *Productivity Commission Report* (n 89) 96–7.

167 Ibid 185, 418–19 (citing Desai, Ritchie and Welpton (n 122)).

168 Senate Standing Committee for the Scrutiny of Bills (n 158) 4–7 [1.9]–[1.17]. The scrutiny resulted in changes to the Explanatory Memorandum, but did not substantially resolve the identified issues: Senate Standing Committee for the Scrutiny of Bills, Parliament of Australia, *Scrutiny Digest* (Digest 5 of 2021, 17 March 2021) 37–8, [2.4]–[2.10].

169 *DAT Act* (n 17) s 23.

170 Normann Witzleb, 'Responding to Global Trends? Privacy Law Reform in Australia' in Moritz Hennemann, Kai von Lewinski, Daniela Wawra and Thomas Widjaja (eds), *Data Disclosure: Global Developments and Perspectives* (De Gruyter, 2023) 147, 166.

171 Elizabeth Green and Felix Ritchie, 'The Present and Future of the Five Safes Framework' (2023) 13(2) *Journal of Privacy and Confidentiality* jpc.831, 6–7.

172 Ibid 14–16.

173 Ibid 10.

174 While information privacy laws may avoid absolutes in relation to the *means* of data protection, they tend to be very clear around permitted *purposes* for the use of personal information: see, eg, *Australian Privacy Principles* (n 16) APP 6.

175 Felix Ritchie and Damian Whittard, 'Using the Five Safes to Structure Economic Evaluations of Data Governance' (2024) 6 *Data & Policy* e16, e16-4.

In Part II above, I detailed that the applicable legal standard for data holders in defending against a data breach is the taking of reasonable steps to protect the data, in compliance with APP 11. Given the significant weaknesses in its data sharing principles based on the Five Safes, application of the *DAT Act* may result in data sharing conduct that does not meet this standard. The Five Safes' lack of focus on legal compliance, its omission of defined risk or information security standards, its inherently subjective approach and its lack of alerts around dangerous practice may result in public sector data holders unwittingly engaging in poor and risky data sharing practice that falls short of the reasonable steps standard. As an example, if the NDDA were to rely on the *DAT Act* for data sharing, the weaknesses in the model might result in the sharing of inadequately de-identified personal information without reasonable security protection. While the *DAT Act* prohibits a recipient from *intentionally* re-identifying de-identified data,[176] this would not protect data from re-identification if inadvertently disclosed — triggering a data breach of considerable concern given the vulnerability of the data subjects and sensitivity of the data.

It is important to note that the *DAT Act* requires the use of DSAs, which may apply an additional layer of protection. In Part IV below, I assess the ability of DSAs to remedy weaknesses introduced by the Five Safes. But at a minimum, the widespread use of the Five Safes in the Australian public sector requires critical evaluation.

IV Comparing Public Sector Data Sharing Agreement Templates

DSAs are an important tool in managing the ongoing conduct of data sharing involving personal information. A DSA allows the data holder to communicate expectations and legal requirements, undertake compliance monitoring and impose sanctions where necessary. Even where the recipient is bound by the same privacy laws as the data holder and is subject to legislative compliance mechanisms, a DSA provides a practical way for the data holder to enforce those obligations, such as by withholding data or terminating the DSA in the event of non-compliance. Unlike a 'point-in-time' data sharing decision, a DSA also imposes ongoing obligations and helps manage the data lifecycle, from the method of sharing through to data destruction.

While Australian data sharing legislation did not eliminate DSAs, in most cases it was closely followed by form-like DSA templates intended to streamline the DSA process, for completion by non-legal staff without significant legal oversight. Perhaps inadvertently, the templates risk focusing public servants on *DAT Act* obligations to the exclusion of reasonable steps requirements. In this section I review four standard public sector DSA templates from federal, state and territory jurisdictions, to identify the additional protection they offer.[177] Analysis by Krebs and

[176] *DAT Act* (n 17) s 16A(3).

[177] I have not included the *Intergovernmental Agreement on Data Sharing between Commonwealth and State and Territory Governments* because it does not contain its own DSA template, stating: 'A [separate] data sharing agreement can be used to ensure the arrangement is appropriately authorised and governed': *Intergovernmental Agreement on Data Sharing between Commonwealth and State and Territory Governments* (n 130) sch E.

Bennett Moses concluded that '[m]ost of the Australian data sharing agreements that we reviewed lacked both specificity and comprehensiveness, resorting to general principles and failing to include important obligations'.[178] My focus is to assess whether these templates contain adequate protections to overcome weaknesses in the Five Safes and to help ensure that the reasonable steps standard is met.

A *The Office of the National Data Commissioner DSA Template*

The recently superseded 2022 ONDC DSA template ('ONDC DSA') resembles a form and includes encouragement on the first page for parties to seek legal advice on whether it will be binding.[179] As a relatively generic template, it focuses on recording the parties' mutual intentions, rather than applying standards set by the data provider. The bulk of the template is devoted to the application of the data sharing principles (that is, the Five Safes). To the extent that there are obligations under the ONDC DSA, they generally flow from the data sharing principles and perpetuate any gaps or weaknesses in the application of those principles. For instance, under the principle 'Setting', cl 4.14 requires the parties to '[d]escribe in detail the physical and Information Technology (IT) environment that will be used to transmit, store and access the data'.[180] The parties could describe a completely unsuitable environment for personal information and there is no guidance that this must be rejected. Due to its reliance on the data sharing principles, the ONDC DSA template is lacking safeguards to ensure that an appropriate level of protection is applied. While this template has been superseded, it remains relevant due to its influence on other jurisdictions.

B *The Australian Capital Territory Public Sector DSA Template*

The Australian Capital Territory ('ACT') public sector DSA template ('ACT DSA') is a version of the ONDC DSA, tailored for use by the ACT Government.[181] It has a similar format and focus on the data sharing principles (that is, the Five Safes), and accordingly carries the same weaknesses as the ONDC DSA.

C *The South Australian Intra-Government DSA Template*

The South Australian intra-government DSA template ('SA DSA'), used for South Australian agencies sharing data with one another, is expressly described as a 'form' in its preamble.[182] Like the ONDC DSA, it focuses on recording the parties' mutual

---

178 Krebs and Bennett Moses (n 132) 136.

179 'Data Sharing Agreement Template', *Office of the National Data Commissioner* (Template, 2022) 1 <https://www.datacommissioner.gov.au/sites/default/files/2022-07/ONDC_Legislation_Agnostic_DSA_Template.doc> ('ONDC DSA'). This template was current until February 2025, when a new dynamically generated template was introduced in the Dataplace platform: 'Data Sharing Agreements', *Office of the National Data Commissioner* (Guidance Note, 2025:2) <https://www.datacommissioner.gov.au/data-sharing-agreements>.

180 Ibid 9.

181 ACT Government, 'External Data Sharing Agreement Template', *ACT Data Sharing Policy* (2 January 2025) <https://www.act.gov.au/open/act-data-sharing-policy> ('ACT DSA').

182 Department of the Premier and Cabinet (SA), 'South Australian Intra-Government Data Sharing Agreement', *Data Sharing Agreement Forms* <https://www.treasury.sa.gov.au/Our-services/data-sharing/data-sharing-forms-and-templates> ('SA DSA').

intentions, with a substantial section (part 6) to step through application of the data sharing principles (ie the Five Safes). Again, this approach leaves significant discretion to each individual assessment, failing to set an objective standard or indicating when sharing might be inappropriate. For instance, one of the Safe Settings questions is 'Based on these safeguards, is the likelihood of accidental disclosure or access low?' with a yes/no checkbox.[183] If the answer is 'no', there is no guidance that additional controls must be applied. It presumably assumes that the signatory will review these criteria carefully before signing, but in a busy public service agency that may leave too much room for error.

D *The DSA under the Victorian Government Data Sharing Heads of Agreement*

The Victorian Government's *Data Sharing Heads of Agreement* ('Heads of Agreement')[184] was intended to operationalise the *Victorian Public Sector Data Sharing Policy*.[185] The DSA ('Vic DSA'), contained in Annexure 1 under the Heads of Agreement, is non-binding and for use within Victorian Government departments who are signatories to the Heads of Agreement.[186] The annexure also has the appearance of a form, but does import certain obligations from the Heads of Agreement, such as the obligation to only use the data for a specified purpose (cl 8), and requirements for data handling, retention and security, including compliance with the Victorian Protective Data Security Standards[187] and completion of a security assessment (cl 12). Further, cl 4 of the Heads of Agreement requires the parties to comply with applicable privacy law and the Victorian Protective Data Security Standards, thereby upholding compliance with independent security standards. These elements make this DSA considerably stronger than the others reviewed. While the explanatory material indicates that the '[p]arties are free to replace all or any part of the annexures with the format/content that best suits their circumstances',[188] which may undermine such requirements, the best view is that

---

[183] Ibid 7. Below the check boxes, the form states 'Provide specific details below', but there is no suggestion that such details are required.

[184] Victorian Government, 'Victorian Public Sector (VPS) Data Sharing Heads of Agreement – as at 19 August 2022', *Victorian Public Sector Data Sharing Heads of Agreement* (19 December 2022) <https://www.vic.gov.au/victorian-public-sector-data-sharing-heads-agreement> ('Heads of Agreement'). Note that the application of data sharing principles to these Heads of Agreement is a little unclear due to an outdated definition of 'National Data Sharing Principles' as 'the principles set out in the Office of the National Data Commissioner's *Best Practice Guide to Applying Data Sharing Principles*': at 4. The Guide referred to principles based on the Five Safes but has since been archived and is no longer available on the ONDC website: Department of Prime Minister and Cabinet (Cth), *Best Practice Guide to Applying Data Sharing Principles* (15 March 2019) <https://nla.gov.au/nla.obj-1856777422/view>.

[185] 'Victorian Public Sector Data Sharing Policy', *Victorian Government* (Web Page, 1 May 2024) <https://www.vic.gov.au/victorian-public-sector-data-sharing-policy>.

[186] Victorian Government ,'VPS Data Sharing Heads of Agreement - Template Annexures - Version 3.1' (December 2022) <https://www.vic.gov.au/victorian-public-sector-data-sharing-heads-agreement> ('Vic DSA').

[187] OVIC, *Victorian Protective Data Security Standards Version 2.0 Implementation Guidance v 2.1* (January 2021) <https://ovic.vic.gov.au/wp-content/uploads/2021/02/20210216-VPDSS-V2.0-Implementation-Guidance-V2.1.pdf>. The Victorian Protective Data Security Standards are the Victorian equivalent of the Protective Security Policy Framework.

[188] Vic DSA (n 186) 1.

this flexibility was not intended to, and should, not override the requirements in the Heads of Agreement.

E *Key Elements of Public Sector DSAs*

Table 3 below provides a summary of the contents for the four DSAs (ONDC, SA, ACT, Vic), compared against one another and two additional frameworks:

(a) the requirements for a compliant DSA under the *DAT Act* s 19; and

(b) the Office of the Victorian Information Commissioner ('OVIC') publication *Information Sharing and Privacy: Guidance for Sharing Personal Information* ('*OVIC Guidance*'), which includes a section on the recommended contents of a DSA.[189]

The shading in Table 3 shows the provisions that are present in each document, with unshaded areas highlighting omissions.

Table 3 indicates that the following eight DSA elements are specified in all four DSAs, required by the *DAT Act* s 19 and recommended for inclusion by the *OVIC Guidance*.

1 *Parties*

The parties to the DSA should be clearly specified, generally including name, ABN, address, role under the agreement (discloser or recipient) and contact details.[190] Similarly, all four DSAs require that the agreement be appropriately executed (while execution is not mentioned in the *DAT Act* s 19 and the *OVIC Guidance*, it can be assumed as being necessary to finalise an agreement).

2 *Defined Purpose or Project*

A standard and characteristic element of DSAs is a statement of the intended purpose of data use.[191] If a DSA is entered for a specific project, it will generally include a description of the project and how the data will be used as part of that project, and sometimes the public benefits of the project.

3 *Defined Data*

It is usual to clearly specify what type of data is covered by the DSA, potentially at the level of databases or data fields.[192] This is often covered by a defined term, such as the 'Data' or 'Information', and referenced throughout the DSA.

---

[189] OVIC, *Information Sharing and Privacy: Guidance for Sharing Personal Information* (D20/8573, April 2021) 14–17 ('*OVIC Guidance*') <https://ovic.vic.gov.au/wp-content/uploads/2021/04/Information-Sharing-and-Privacy-Gudiance-on-Sharing-Personal-Information.docx>.

[190] *DAT Act* (n 17) s 19(1); ONDC DSA (n 179) 2–4; SA DSA (n 182) 1–2; ACT DSA (n 181) 4; Vic DSA (n 186) 1; *OVIC Guidance* (n 189) 15.

[191] See, eg, *DAT Act* (n 17) s 19(2); ONDC DSA (n 179) 5; SA DSA (n 182) 2; ACT DSA (n 181) 5; Vic DSA (n 186) 2; *OVIC Guidance* (n 189) 15.

[192] See, eg, *DAT Act* (n 17) s 19(3); ONDC DSA (n 179) 10; SA DSA (n 182) 4; ACT DSA (n 181) 9; Vic DSA (n 186) 1–2; *OVIC Guidance* (n 189) 15.

Table 3: Comparison of DSAs, the *OVIC Guidance* and the *DAT Act* s 19[†]

	ONDC DSA	**SA DSA**	**ACT DSA**	**Vic DSA**	***OVIC Guidance***	***DAT Act* s 19**
Parties	■	■	■	■	■	■
Defined purpose/project	■	■	■	■	■	■
Purpose limitation	■	■	■	■	■	■
Defined data	■	■	■	■	■	■
Data lifecycle, retention	■	■	■	■	■	■
Data quality		■	■	■		
Legislative basis	■				■	■
Matching, re-identification restrictions	■	■	■			■
Third party recipients, on-sharing	■		■	■		■
Users	■	■	■	■	■	*Addressed by data sharing principles*
Incident management	■		■		■	■
Security	■	■	■	■	■	*Addressed by data sharing principles*
Risk assessments	■	■	■	■	■	*Addressed by data sharing principles*
Non-compliance & enforcement		■			■	■
Assurance				■	■	
Duration	■		■	■	■	■
Variation	■		■			■
Termination			■	■	■	■
Execution	■	■	■	■		

[†] ■ denotes coverage
denotes no coverage

4 *Users*

All of the templates require some specification or definition of the relevant users (noting that for the *DAT Act* s 19, this is encompassed by the data sharing principles).[193]

These elements are arguably all necessary to establish an effective and meaningful DSA, but offer only a minimal contribution to satisfying the reasonable steps standard. The following elements, also present in all four agreements, begin to contribute to meeting that standard.

5 *Purpose Limitation*

Each DSA includes a requirement that data use be restricted to the specified purpose.[194] Some DSAs may allow uses incidental to the specified purpose (provided the incidental purpose(s) are specified),[195] and some may restrict the use to the specified purpose only, but there will generally be a purpose limitation in any public sector DSA.[196] This purpose limitation is important to the security of the data.

6 *Risk Assessments*

All templates consider whether other assessments are needed (for the *DAT Act* s 19 this is encompassed by the data sharing principles, which mention an ethics assessment), and most require that a separate Privacy Impact Assessment ('PIA') be performed.[197] A PIA will assess compliance with applicable privacy laws and identify any privacy risks that need to be controlled as part of the project. A PIA will ideally encourage *Privacy Act* compliance, but as it is commonly prepared by non-technical staff there is a high risk that the APP 11 'reasonable steps' analysis will be inadequate. A security risk assessment is prepared by technical staff and is generally more effective in this regard. The Vic DSA also requires performance of a security risk assessment (recommended in the *OVIC Guidance* also),[198] and the ONDC DSA, SA DSA and ACT DSA inquire whether ethics, finance or IT approval is relevant.[199]

7 *Security*

All templates require security controls to be considered and specified (again, in the case of the *DAT Act* s 19, this is encompassed by the data sharing principles).[200] In

---

193 ONDC DSA (n 179) 8–9; SA DSA (n 182) 5; ACT DSA (n 181) 7; Vic DSA (n 186) 1; *OVIC Guidance* (n 189) 16.

194 See, eg, *DAT Act* (n 17) s 19(6); ONDC DSA (n 179) 5; SA DSA (n 182) 4; ACT DSA (n 181) 6; Vic DSA (n 186) 2 (item 1); *OVIC Guidance* (n 189) 16.

195 *DAT Act* (n 17) s 19(6)(a)(ii).

196 The purpose restriction might also be imposed by legislation — see, eg, *Road Safety Act 1986* (Vic) s 90N(2), which requires the relevant agreement to include a binding undertaking that the recipient will only use the shared personal information for the specified purpose.

197 See, eg, ONDC DSA (n 179) 7; SA DSA (n 182) 3; ACT DSA (n 181) 6; Vic DSA (n 186) 3 (item 4), Annexures 2–3 (combined with Heads of Agreement (n 184) cl 12); *OVIC Guidance* (n 189) 16.

198 Vic DSA (n 186) 3 (item 3), Annexure 3 (combined with Heads of Agreement (n 184) cl 12); *OVIC Guidance* (n 189) 16.

199 ONDC DSA (n 179) 7; SA DSA (n 182) 3; ACT DSA (n 181) 6.

200 ONDC DSA (n 179) 9–10; SA DSA (n 182) 4, 6–7; ACT DSA (n 181) 8; Vic DSA (n 186) 3 (item 3); *OVIC Guidance* (n 189)16.

most cases, this is included as a response to the 'Safe Settings' element of the Five Safes, asking that the chosen security settings be documented but not setting any minimum standards or guardrails.[201] Some DSAs require more detail than others, with the ACT DSA asking whether the data recipient complies with ISO 27001,[202] without indicating how this information should be evaluated.[203] Only the Vic DSA requires a security risk assessment, which provides detail on applicable security settings and potential areas of weakness, and would usually require technical staff to assess the security settings and evaluate their effectiveness against an independent security standard, and presumably action any recommendations. A security risk assessment is a valuable component of any data sharing activity — this is a strength of the Vic DSA, which is also strong in requiring compliance with an independent information security standard, the Victorian Protective Data Security Standards. The other three DSAs do not require compliance with any independent standard.

8 *Data Lifecycle and Retention*

While all DSAs refer to data retention, only the Vic DSA applies appropriate data retention requirements, with the data recipient being required to agree to securely destroy the data once it is no longer needed.[204] All other DSAs just ask the parties to specify how they will treat the data at the end of the project or purpose, with no standard specified.[205]

Table 3 (above) also points to some components that are less universal but are specified in several of the DSAs. In Part V below, I discuss the elements that are lacking or should be more consistently applied to assist with meeting the reasonable steps standard.

V Improving Data Sharing Agreements to Meet the Reasonable Steps Standard

There are additional DSA elements that would go a long way towards addressing the deficiencies of the Five Safes and enabling a public sector data holder to ensure that it has taken reasonable steps to protect the shared data — as well as building the social licence around data sharing emphasised in the *Productivity Commission Report* by implementing genuine safeguards. The OAIC findings discussed in Part II above suggest that an adequate DSA should require the data recipient to implement: security and risk management policies (covering system monitoring); appropriate data retention policies; staff training in privacy and security; and effective contractual arrangements for any on-sharing to data recipient contractors. In addition, the DSA should include an assurance and audit framework for contract compliance and would ideally require the data recipient to operate in accordance with an independent security standard. Considering these OAIC expectations for the reasonable steps standard, it is notable that the DSAs analysed in Table 3 (above) largely lack those elements.

---

[201] See, eg, SA DSA (n 182) 6–7; ACT DSA (n 181) 8–9.
[202] International Organization for Standardization (n 38).
[203] ACT DSA (n 181) 8.
[204] Heads of Agreement (n 184) cl 13; Vic DSA (n 186) 4 (item 8).
[205] See, eg, ONDC DSA (n 179) 8; SA DSA (n 182) 7; ACT DSA (n 181) 7.

A *Appropriate Security Governance and Risk Management Policies*

None of the DSAs require the recipient organisation to have commonly implemented security governance in place (such as security policies and risk management policies). An enterprise security management policy would usually detail requirements for security threat monitoring and alerting, and such policies should also cover management of data incidents. The OAIC described such governance in the Ashley Madison joint investigation as 'a basic organizational security safeguard, particularly for an organization holding significant amounts of personal information'.[206] In that investigation, the OAIC identified 'critical gaps in security' that it attributed to the lack of an implemented security governance and monitoring framework.[207] Further, the lack of a documented risk management framework in the Ashley Madison case seemed to underpin a failure of appropriate risk assessment, potentially contributing to the loss of data.[208] There is a clear risk of non-compliance with the reasonable steps standard if appropriate security governance and risk management policies are not required by the relevant DSA.

B *Data Retention Requirements*

The DSAs should specify how long data may be kept, and how it should be disposed of, consistent with APP 11.2. Only the Vic DSA is adequate in this regard, with an overarching obligation to dispose of data in the Heads of Agreement,[209] and more detail on data retention, destruction and assurance in the Vic DSA itself.[210] The other DSAs merely allow the users to record data retention arrangements — but data holders using those DSAs should take that opportunity to be prescriptive, following the example of the Vic DSA. Applying the Blood Service findings around reasonable steps under APP 11.2, both the data holder and the data recipient should have systems and procedures in place 'to identify information the organisation no longer needs and destroy or de-identify this information'.[211]

C *Staff Training Requirements*

None of the DSAs is prescriptive in relation to staff training in privacy and security; only the *OVIC Guidance* makes any significant mention of this.[212] Some of the DSAs request details of the users' qualifications, but without setting a minimum standard or requiring any refresher training. By means of an enforceable undertaking, the OAIC required ARC to develop, finalise and conduct privacy training with its staff on a regular basis, including during onboarding and at regular intervals, and to maintain records of training compliance.[213] While this was considered necessary to implement the reasonable steps standard in the face of the employee conduct that

206 *Ashley Madison Investigation Report* (n 40) 15 [65].
207 Ibid 15 [67].
208 Ibid 16 [69]–[70].
209 Heads of Agreement (n 184) cl 13.
210 Vic DSA (n 186) 4 (items 8, 10).
211 OAIC, *DonateBlood.com.au Data Breach* (n 42).
212 *OVIC Guidance* (n 189) 16.
213 *ARC Enforceable Undertaking* (n 35) [5.6].

triggered the ARC breach, it would be good practice in any case. At a minimum, the DSA should require some type of staff compliance training in privacy and security, to ensure that employees understand their obligations under the DSA.[214]

D *Contracting Obligations*

None of the DSAs address the issue of whether subcontractors can be used to manage the data and the obligations that should apply to them. Given the OAIC's findings regarding contractual arrangements in the Blood Service breach, this is likely to be a weakness. Data recipients may engage subcontractors to undertake data hosting and data analytics, or to manage infringements or customer queries, among other things. A DSA should specifically require the data recipient to take responsibility for its subcontractors' compliance with the DSA, otherwise the protections of the DSA are likely to be significantly undermined by subcontractor use. A related issue is the offshoring of data by contractors to jurisdictions with a lower level of legislative privacy and security protection. This can expose the data to considerable risk, but was not addressed in any of the DSA templates.[215] The DSAs should specifically limit offshoring of the data.

E *Auditing for Compliance*

Another common deficit in the templates is a lack of ongoing compliance and assurance activity. Among the four DSAs, only the Vic DSA references this, suggesting that the parties document any assurance required for data destruction, and also any other assurance or audit processes — but without requiring such assurance.[216] A data holder cannot be confident of compliance in the absence of ongoing reporting or auditing.[217] In the case of shared personal information, it is appropriate to apply regular auditing to the data recipient (either self-assessment or some level of independent auditing) to ensure that agreed standards continue to be met. Resources permitting, it may be appropriate to specifically allow investigative access by the data holder or its agent (such as a security testing company) to the data recipient's environment and data use in order to confirm that appropriate standards are being upheld. None of the DSAs require the data recipient to allow investigative access by the data holder. Ideally, all of the DSAs should be reviewed and updated to add assurance requirements and (where feasible) allow for investigative access. Auditing and inspection activity often requires follow up and ongoing supervision to ensure that any identified issues are appropriately rectified and closed out — such activities will need to be adequately resourced by the data holder.

---

[214] The data holder may wish to prepare and supply relevant user training to data recipients, especially if there are complexities around appropriate use of the data.

[215] It may also point to non-compliance with APP 8, which covers the cross-border disclosure of personal information and requires an APP entity to 'take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the *Australian Privacy Principles* (other than Australian Privacy Principle 1)': *Australian Privacy Principles* (n 16) APP 8.

[216] Vic DSA (n 186) 4 (items 8, 10).

[217] See, eg, the OAIC Guide reference to auditing: OAIC, *Guide to Securing Personal Information* (n 29) 42.

F *Independent Standards*

With the exception of the Vic DSA, the DSAs do not require compliance with any independent security standards. This omission from the templates implies that *any* level of protection may be adequate provided it is documented and agreed. While the reasonable steps standard does not require compliance with an independent security standard, the OAIC's investigations into Sony and Epsilon indicate it can be beneficial in establishing that reasonable steps were taken.[218] Also, the OAIC referenced independent standards to establish the measures that Medibank should have implemented.[219] By requiring compliance with the Victorian Protective Data Security Standards and also a security risk assessment, the Vic DSA could assist data holders in demonstrating that reasonable steps were applied. The other three DSAs do not require this. Guidance should be developed for data holders using those DSAs, encouraging them to require that data recipients comply with an independent standard such as Protective Security Policy Framework, ISO 27001 or the Essential Eight, including a security risk assessment in each instance.

The existing public sector DSA templates would be improved by paying attention to the six elements discussed above in Part V(A)–(F), to help address the weakness of the Five Safes and ensure that reasonable steps have been taken. This is not a 'set and forget' exercise. To appropriately monitor and oversee each DSA, ongoing contract management will be required, including supervising annual assurance activities and determining on a risk basis whether additional controls (such as investigative access) should be actioned. Public sector data holders should ensure that they are adequately resourced to actively manage their data sharing arrangements throughout the data sharing lifespan.

VI Conclusions

As illustrated by the NDDA and NEVDIS examples, public sector data sharing is highly valuable — it underpins law enforcement, policy development and service delivery, and may unlock considerable economic value. But for such data sharing to grow and flourish, the *Productivity Commission Report* asserts that it needs strong trust and social licence, based on the public's confidence that their data will not be negatively impacted by a data breach or otherwise. In this article I considered the OAIC's application of the APP 11 reasonable steps standard to understand the standard of conduct applicable to public sector data holders to prevent a data breach. I also outlined the weakness introduced into public sector data management by the *DAT Act*, which overrides some legislative protection and may apply inadequate data protection due to reliance on unsuitable data sharing principles. Although the *DAT Act* is intended to operate alongside and in addition to the *Privacy Act* and APP 11, its complexity is such that public servants may apply it and corresponding DSA templates in a standalone manner, resulting in weak or inadequate efforts to comply with the reasonable steps standard.

I stepped through the unfortunate process by which the Five Safes were adopted as data sharing principles, and critiqued that framework, outlining its

[218] *Sony Report* (n 31); *Epsilon Report* (n 32).
[219] 'OAIC Concise Statement' (n 61) Annexure B.

weaknesses in respect of the sharing of personal information. A high-level principles-based approach like the Five Safes framework, while potentially suitable for research and statistics, raises too many risks and offers too little guidance in a public sector context. It is ill-equipped to satisfy the reasonable steps standard. I also assessed the role of DSAs in helping to fill that gap, highlighting six areas that could immediately be improved to assist in satisfying the reasonable steps standard. This would involve updating or using the DSAs to:

- require that the data recipient has appropriate security governance policies and a risk management framework in place;
- apply appropriate data retention policies; impose obligations in relation to staff training in privacy and security; include restrictions and obligations in relation to subcontracting;
- impose assurance and compliance activities on the data recipient; and
- require that a data recipient's environment comply with an independent standard where feasible.

Ideally, DSA templates would be amended accordingly, but they are sufficiently flexible to allow data holders to include these requirements in practice, starting immediately. In this regard, the stronger Vic DSA provides a helpful model. This is not just contractual amendment — appropriate ongoing management is needed throughout the data lifecycle.

Strengthened DSAs would ideally be combined with targeted guidance to public servants on the ongoing relevance of APP 11 to data handling under the *DAT Act*. This guidance should strongly encourage the undertaking of a security risk assessment as part of each *DAT Act* authorisation, together with the implementation of any ensuing recommendations. Should such improvements be made, it would allow Australian public sector agencies to ensure that they take reasonable steps in their data sharing activities to protect their customers' personal information, consistent with APP 11. Not incidentally, such action is likely to build social licence around data sharing by implementing genuine safeguards that reduce the likelihood of a data breach and protect important customer data.