# Comments on Draft Findings and Recommendations of the Statutory Review of the Data Availability and Transparency Act

**Peter Leonard**[1]

The draft findings and recommendations in the July 2025 *Draft Findings and Recommendations of the Statutory Review of the Data Availability and Transparency Act* 2022 (**DAT Act**) are welcome and generally supported by this writer.

The following comments should be read in that context: they address suggested improvements, and do not state the many other areas of agreement.

1. The DAT Act is an enabling framework, constructed to facilitate controlled and safeguarded data sharing between a willing data custodian and data recipient. This enabling framework is useful, but does not currently address and ameliorate cultural and other barriers that lead many decisionmakers in data custodians to be unwilling to share data. We discuss these cultural and other barriers later in these comments.

2. Controlled and safeguarded use of many public sector data sets, and particularly where Federal data sets are joined with (deep and potentially insightful) State and Territory agency-controlled datasets (i.e., public health services, educational and community services data), could assist national productivity. Current provisions of the DAT Act do not stimulate willingness of government agencies to share data. The DAT Act requires revisions to better align its operation with the Australian government's national productivity agenda.

3. Public sector data is a collective community asset and should be used to the benefit of the Australian community. Government agencies are stewards of that community asset, not 'owners' of data. However, that comment should not be read as a call to mandate data sharing by government agencies, or a suggestion that a public interest in data sharing overrides legitimate concerns as to excessive or inappropriate uses of data about Australians. For example, there will be instances (data contexts) where risk of harms to individuals[2] is greater than low or remote, or where data is not of sufficiently assured

[1] Peter Leonard is a data and technology business consultant and lawyer. He serves on the National Data Advisory Council. However, these comments are his personal views. His business consultancy Data Synergies assists businesses and other organisations with AI and data governance, assurance and legal compliance. He is an Adjunct Professor of UNSW Law and Justice.

[2] Adverse consequences and harms to some individuals are often (but not always) greater when outputs from analysis of data are applied to determine differential treatment of particular individuals or granular segments of inferred like individuals, for example, individuals grouped by inferred individual-level 'attributes' (characteristics, traits, vulnerabilities, preferences, activities or behaviours). Adverse consequences may be severe, sometimes life threatening. Individuals took their own lives as a direct consequence of erroneous insights that led to, in Australia, sending of Robodebt letters of demand, and in the United Kingdom, the Post Office scandal. The list of possible 'data-enabled harms' is extensive. The risk of some harms are greater when data trains large language models, given heightened possibility of incorrect inferences derived from LLMs. However, these harms are still within the broad category of data-enabled harms, whether or not also a recognised 'AI harm'. Examples of data-enabled harms include a negative outcome or decision with respect to an individual's eligibility for a right, privilege, or benefit; offer of less favourable terms, or cancellation or an unfavourable change in terms; online abuse; discrimination, stigmatisation or reputational injury; inconvenience or expenditure of time; disruption and intrusion from unwanted communications or contacts; and other detrimental or negative consequences that affect an individual's private life or family matters. Of course, harmful outcomes may also be non-human, such as damage to the environment (including other species) caused by reliance upon incorrect data, or group or societal and not individual, such as loss of social cohesion. The higher the assessed risks of harms, the greater the magnitude of possible consequences, and any limits in ability to mitigate those risks of harmful consequences through design and implementation of verifiably reliable, the less likely that the use of data for a particular use is safe and responsible. See further Peter Leonard, Privacy Harms: A research paper for the Office of the Australian Information Commissioner, June 2020, available at

quality to be reasonably reliable for the reliance that may be placed upon outputs from analysis of that data, or where those outputs may be used to effect inappropriate outcomes. Accordingly, revisions of the DAT Act need to better effect the public interest in data sharing, while not mandating data sharing.

4. Revision of the DAT Act should include an express object of stimulating willingness of data custodians to facilitate safeguarded and controlled data sharing. The current first object (section 2(a)) of "to serve the public interest by promoting availability of public sector data" is not sufficiently clear[3], and in any event does not address facilitating availability and linkage and other uses of State and Territory controlled data sets.

5. An instructive comparator (albeit in a *disclosure*, not a controlled *use*, data context), is the *Government Information (Public Access) Act* 2009 (NSW), which expressly states a general (overriding) *public interest* in favour of the disclosure of government information (section 12(1)), while also enumerating specific public interest considerations against disclosure (sections 13, 14 and 15, and Schedules 1 (Information for which there is a conclusive presumption of overriding public interest against disclosure), and 2 (Excluded information of particular agencies).

6. The use cases and data contexts within which multiparty data sharing for data joining and advanced analytics have changed dramatically in the last decade. In the business sector (and in particular in relation to health applications), there is now generally understood best practice (by no means universally applied – there is also plenty of bad practice) as to:

   (1) design and implementation of reliably and verifiably safeguarded and controlled clean data environments, and

   (2) assessment of outputs from those environments for reliability for likely reliance to be placed upon those outputs in ways that affect outcomes for affected individuals, in order to:

      (a) prevent disclosure or further sharing of confidential or business sensitive information that may have been analysed within the clean room,

      (b) ensure outputs are effectively anonymised and therefore protected against reidentification risk and in full compliance with both privacy law and legitimate expectations of individuals to whom unit level data relates, and

      (c) assure reliability of outputs for likely reliance placed upon them to effect or influence outcomes experienced by affected individuals.

7. As a result of greater data maturity (understanding within businesses) as to how to manage data sharing of sensitive business data and of advanced data analytics, there is much more controlled and safeguarded data linkage across business entities than there was a decade ago.

---

https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/research-publications-on-the-privacy-act; Danielle Keats Citron & Daniel J. Solove, Privacy Harms, (2022) 102 Boston Uni Law Rev. 793; M. Ryan Calo, The Boundaries of Privacy Harm, (2011) 86 Indiana Law Journal 1131.

[3] This object is likely to be read as directed only at the DAT Act addressing the lack of authorisation barrier, and not consistent with an objective of stimulating appropriate uses of public sector data.

8. Many government entities are now significantly behind business sector entities as to understanding within and across those government entities (as compared to the business sector) as to appropriate safeguards and assurance controls for data linkage for advanced data analytics and AI applications.

9. As per the draft recommendations, the authorisation framework provided by the DAT Act could be made easier to navigate and more facilitative, without significantly increasing risks of harms to individuals to whom unit level data relates. However, the barriers impeding willingness of government entities to make more productive uses of public sector data are not only, or principally, the challenges identified on page 7 of the Draft Report.

10. The barriers impeding willingness of government entities to make available public sector data for other productive uses may be increasing, not decreasing. Robodebt, the UK Post Office, and other well publicised data and analytics related problems within public sector entities globally have increased concerns of decision makers as to risks of harms to affected individuals from use of outputs from inferential outputs, now including LLMs and genAI. Many decisionmakers are rightly concerned that LLMs and genAI may lead to data linkage outputs being used by downstream entities to effect harms upon individuals that have not been anticipated (foreseen) and appropriately risk mitigated.

11. Government departments and agencies are custodians of many potentially useful datasets. The keepers of those datasets are rightly concerned to continue to be seen by Australian citizens as trustworthy custodians of sensitive and confidential information about citizens. Decisionmakers may also consider that provision of their curated and controlled data sets to a downstream entity may (however unfairly) implicate the providing party in any issues created by downstream entities even where those issues could not reasonably be foreseen by a diligent providing party. Trustworthiness requires no surprises that may lead to adverse consequences. Adverse consequences may include that data collected for a stated particular purpose is repurposed for a purpose that Australian citizens consider harmful to their rights or interests, or that is unacceptably 'spooky' or overly intrusive. To cite one example, the Australian Bureau of Statistics demonstrates how a body that mandates provision by Australian citizens of sensitive and confidential information about them may maintain a high trustworthiness rating while facilitating data sharing and weathering the odd media crisis (such as the unfairly named 'Censusfail' media storm).

12. The barriers impeding willingness of government entities are multifaceted and therefore not always readily foreseen and risk mitigated. Barriers include concerns about public perceptions of trustworthiness of a data custodian, as to emerging (but not yet fully clear or stable) standards for safe, fair and responsible use of linked data and AI, or as to legal compliance. Other barriers are:
    - that data sharing is perceived to be hard to manage and to risk mitigate,

- that there is insufficient incentive for a decisionmaker within a data custodian to engage with a process that might not directly benefit that custodian agency, or which is perceived to be 'risky',
- that the data custodian is concerned as to whether data is of appropriate data quality to enable its safe or responsible use by downstream party, particularly where the data custodian does not have the financial and human resources to actively curate the data and further improve data quality, or to assess limitations of the data and then state those limitations to any recipient entity. Or more simply, the data custodian may have insufficient incentive to do these things.

13. In short, there are many barriers currently impeding data sharing by Australian government agencies. The challenges identified on page 7 of the Draft Report may not be the most impactful barriers. The listing of challenges should be expanded to better reflect the current range of barriers.

14. Draft recommendation 4 is therefore welcome: each of the key points on page 18 of the draft Report are endorsed: in particular, "The general responsibility on data custodians to consider data sharing requests should be reframed as a positive obligation to share data for the authorised purposes, except where there are strong grounds for refusal. For example, where the requestor is accredited to the highest possible level, or where the request would have a clear public benefit, the grounds for refusal should be highly limited." It is also important that there is clarity as to the role and identity of the person within a data custodian who has authority and accountability for decisions to share or not share data. Contrast, and perhaps consider, the role of Public Service Data Champion, or the role of Privacy Champion under the Privacy (Australian Government Agencies – Governance) APP Code 2017.

15. Draft recommendation 4 does not fully address the 'legitimately concerned data custodian' problem: that is, the data custodian is concerned as to data quality appropriate to enable safe or responsible use by a downstream party. Indeed, the current heavy reliance upon 'data sharing agreements' implicates the providing party in evaluation of activities of the downstream party that the providing party may have little ability or incentive to assess and manage. It may be appropriate to consider a limited 'safe harbour' for a providing party that exercises reasonable diligence in relation to a particular stated data use and relies upon a higher level accreditation of a downstream entity. A pivot away from reliance upon data sharing agreements, and towards an appropriate allocation of organisational accountability, may significantly lift the range of data sharing across government agencies.

16. The DAT Act is also built for specific data sharing projects directed at achieving known, predetermined insights and outputs. This is not a problem unique to the DAT Act: existing processes for human research ethics committee (HREC) review and oversight have a similar focus, and do not readily adapt to non-episodic data sharing. Universities and research bodies have well established and generally understood framework and systems for evaluation, initiation and ongoing management and control of projects for joining and analysis of unit level data for human research. However, many valuable and potentially

productive applications of advanced analytics and AI require ongoing ingestion of data and/or use of AI for discovery of possible (that is, not granularly specified in advance) insights and applications: these applications do not readily fall within project specific control frameworks.

17. The DAT Act should more readily facilitate ongoing data sharing, and discovery data linkage, in each case subject to safeguards and assurance controls of equivalent standard of robustness and reliability as apply to the DAT Act principles for one-off, specific outputs-and-outcome-focussed, projects. The business sector has demonstrated ways to evaluate and risk manage ongoing data linkage and/or discovery orientated data analytics and AI training, in some cases using highly business sensitive data sets that require very robust and highly reliable risk assessment and management.

18. A Ministerial power to permit data sharing not otherwise permitted where the Minister considers it to be 'in the national interest' should be re-considered, regardless of whether that power could only be exercised through a disallowable instrument: draft recommendation 5 refers. Concepts of *national interest* (as distinct from *national security*) are politically elastic and dynamic and contestable: what may be considered in Canberra to be 'in the national interest' may also undermine citizen perceptions of trustworthiness of government handling of unit level data about citizens. In any event, an exercise of such power (noting again that we are considering national interest, and not national security) should be subject to prior public consultation and publication of a cost-benefit analysis.

19. The Attorney-General's Department February 2023 Privacy Act Review Report included, as chapter 14, a detailed review of the research 'exceptions' (in the form of conditioned qualifications to the requirement of user consent) within the Privacy Act. These recommendations (14.1, 14.2 and 14.3: broadened scope of research permitted across broadened types of research, including social research, to be governed by a single (uniform) set of guidelines), were accepted by the Federal Government in the Government's September 2023 Response to the February 2023 Review Report. The DAT Act should facilitate a similar broad range of research activities, whether through cross-referencing and 'calling up' revised research provisions in the Privacy Act or otherwise. By contrast to draft recommendation 5, this broad research facilitation should not require Ministerial review or approval.

20. The range of participants within coverage of the DAT Act framework should be expanded. Recipients of sharing remain almost exclusively government agencies and universities (while noting the proposed addition of some not-for-profits and – curiously - personal health networks, but not other key health intermediaries. As per the draft recommendations, private sector data analytics services providers would remain outside the scheme, apparently (only?) because those entities are in the business sector. (By contrast, government agencies use business sector consultants in relation to many and varied government assignments that include exposure to much more sensitive government data, including for enforcement related purposes).

21. Draft recommendations 10 and 11 should be revisited. The restriction as to private sector entities should be removed (but without changing safeguards and assurance control standards and related accreditation criteria). The National Data Commissioner, not the Minister, should administer accreditation criteria, including as to determination of accreditation eligibility categories. The Minister might be empowered to issue directions (as a disallowable instrument) to the Commissioner as to as to determination of accreditation eligibility categories.

22. Recommendation 13 revisits the service delivery purpose and its interaction with the prohibition on enforcement related purposes. Associated Finding 8 states that "the service delivery purpose is currently impeded by extensive privacy protections in the DAT Act and interactions with the prohibition on enforcement related purposes. While permitting enforcement related purposes would likely require and introduce substantial additional protections and complexity, some flexibility to enable the DAT Act to assist in service delivery would improve its utility." Recommendation 13 is high level: "Amendments are required to ensure that data sharing with the primary purpose of delivering government services is not unduly precluded. What constitutes an enforcement purpose should also be reconsidered, and particularly whether inadvertent detection of misconduct should be prohibited." We suggest particular caution as to this proposed reform. The so-called "extensive privacy protections" are there for purposes beyond ensuring equivalence with Privacy Act protections. In particular, those protections are a key plank in ensuring citizen trustworthiness while authorising freer unit level data flows across government agencies and potentially beyond to other data recipients. Moreover, data AI and advanced data analytics enable algorithmically determined differential (and potentially automated) treatment (singling out, whether individually or as a member of a class or segment) of affected individuals, regardless of whether those individuals are identified or identifiable throughout that process. Narrowing of the prohibition on application for enforcement related purposes risks undermining the citizen trustworthiness underpinning of the DAT Act. Overly broad drafting of any relaxed prohibition on enforcement related purposes would risk achievement of other reforms needed to the DAT Act.

23. As per the draft recommendations, State and territory government agencies are not more readily integrated into the data sharing framework, although they are custodians of many key data assets which could yield insights and potential outcomes beneficial for social policy and decision-making affecting Australian society. Of course, constitutional limitations have the result that State and Territory legislatures would still need to enact enabling statutes to facilitate these data sets being brought into the DAT Act framework. However, the DAT Act could better facilitate their joining and use of State and Territory agency-controlled data sets, and Commonwealth controlled data sets, and potentially also private sector-controlled data sets. Recommendations 15 and 16 are welcome.

18 August 2025

## Appendix

There is a curious contrast in ambition between the Productivity Commission's August 2025 'Pillar 3' interim report *Harnessing data and digital technology* and the July 2025 *Draft Findings and Recommendations of the Statutory Review of the Data Availability and Transparency Act 2022*.

The PC *Harnessing data* interim report commences:

> Data and digital technologies are the modern engines of economic growth. Emerging technologies like artificial intelligence (AI), which can extract useful insights from massive datasets in a fraction of a second, could transform the global economy and speed up productivity growth.
>
> Australia needs to harness the consumer and productivity benefits of data and digital technology while managing and mitigating the downside risks. There is a role for government in setting the rules of the game to foster innovation and ensure that Australians reap the benefits of the data and digital opportunity.
>
> .....
>
> Australian governments should take an outcomes based approach to AI regulation – one that uses our existing laws and regulatory structures to minimise harms and introduces technology specific regulations as a last resort.
>
> Data access and use can fuel productivity growth: insights from data can help reduce costs, increase the quality of products and services and lead to the creation of entirely new products. But some requirements in the Privacy Act, the main piece of legislation for protecting privacy, are constraining innovation without providing meaningful protection to individuals.

The PC *Harnessing data* interim report then proposes:

- "new pathways to allow individuals and businesses to access and share data that relates to them" (the proposal appears to be private sector wide, but does not appear to include data custodians that are not government agencies), and

- for the Privacy Act, an alternative, highly simplified, "compliance pathway" based upon data custodian self-assessment of "best interests" of affected individuals "that enables regulated entities to fulfil their privacy obligations by meeting criteria that are targeted at outcomes, rather than controls-based rules".

The July 2025 DAT Act Draft Findings and Recommendations proposes some streamlining of the DAT Act's complexities, but not fundamental reforms that (applying the *Harnessing data* reasoning) could fuel productivity growth.

The DAT Act Review largely assesses the DAT Act against its objectives as set nearly a decade ago by the Productivity Commission's 2017 review into improving data availability and use. That 2017 review found Australia was not making the most of its valuable public data, and that as a result, widespread community and productivity benefits were being missed. The review called for a regulatory framework to support safe and widespread sharing of Australian Government

data for public benefit by enabling necessary permissions and shifting attitudes to 'treating data as an asset'. The PC's 2017 Report called for an overarching enabling framework to facilitate sharing of Australian Government data. The DAT Act provided that enabling framework, and expressed a laudably broad and current object to "serve the public interest by promoting better availability of public sector data": section 4(a). However, the mechanisms then enacted were in the context of limited, project specific, specified purpose, sharing of government data sets between Government agencies, facilitated and conducted by agencies and not businesses, and subject to constraints that largely mirrored requirements of the Privacy Act 1988 and without any broader research permissions.

The July 2025 DAT Act Draft Findings and Recommendations should be revisited as to alignment with the Productivity Commission's August 2025 'Pillar 3' interim report (Harnessing data and digital technology): national productivity should be brought into this discussion.