

Submission to the Consultation
on
*New Australian Government Data Sharing and Release
Legislation*



Introduction

Thank you for the invitation to make a submission to the consultation on the *New Australian Government Data Sharing and Release Legislation*. Future Wise notes the short consultation period on this consultation, and its timing, appearing rapidly after the myHealthRecord secondary use framework and the response to the Productivity Commission's *Data Use and Availability* report. We trust that submissions will be given due consideration in light of these short time frames.

About Future Wise

This submission is authored by Future Wise. We are a group of Australian professionals of varied backgrounds who seek to promote ideas which improve the long-term direction of Australia, particularly in the areas of technology, health and education. More information about Future Wise is available on [our website](https://futurewise.org.au/).¹ We are happy to provide further clarification of any of the points in the submission, or for one of the authors to attend any hearings in person if required. Questions can be directed to the primary author, A/Prof Kate Galloway via email: kate@futurewise.org.au

¹ <https://futurewise.org.au/>

Summary of Submission

Future Wise is broadly supportive of improving use of Government data. It is noted, however, that the premise on which the Issues Paper is based is insufficiently broad to capture the real issue with enhanced data sharing.

The Paper states: 'Greater use and sharing of public data facilitates increased economic activity and improves productivity.' This assertion fails to recognise that Australia is more than an economy. It is a society and civil society depends upon effective boundaries of the exercise of government power over citizens.

This submission responds to the questions posed in the Issues Paper upon the premise of the importance of enhancing the rule of law, and the necessary balance between governmental power and citizen autonomy.

This submission is concerned with any data relating to a person, whether or not that person is specifically named in that data, and responses to the questions relate to this data unless indicated otherwise.

Future Wise submits:

- Current protections for citizens are inadequate and this would best be managed with a Bill of Rights
- Failing this, a broad-based data protection regime similar to the European Union's General Data Protection Regulation is required as a minimum
- The sharing and/or release of any public data must only proceed under a principle of "privacy by design"
- Data Custodians and end-users of shared data must take responsibility for the use and misuse of datasets to which they have access
- Penalties for misuse of shared data are - by themselves - insufficient protection of citizens' privacy: in economic terms in particular, this simply becomes the cost of doing business
- Agreements covering the use of shared data, and any research outputs from these data must be publicly available by default
- The sharing of data for enforcement or compliance purposes is not an acceptable use of a data sharing framework as we believe it is incompatible with the Government's responsibility to citizens, and may have unintended secondary effects on the creation of the datasets
- The role of Data Commissioner must include oversight and enforcement responsibilities to act as a safeguard for the use of this data in the public interest
- The Office of the Australian Information Commissioner should be strengthened, including additional resources, as it is likely that a data sharing regime as proposed will result in additional investigations
- An accessible public complaints mechanism is an essential part of any scheme making use of public data.

Responses to Discussion Questions

Key Principles and Data Sharing

1. Are these the correct factors to taken into account and to guide the legislative development?

Broadly speaking, these factors are appropriate per se. We note, however, that the explanation of each factor fails to grapple with core questions about data, for example:

- an individual data point may not of itself be 'private or sensitive' - it is the aggregation of multiple data points that can become private or sensitive.
- building trust in the use of public sector data implies that this may be shared with 'trusted users' - presumably non-government third parties. The framework is insufficient to deal with factors of trust in those third parties. That is a significant weakness.
- Establishing institutional arrangements relies on the Australian Bureau of Statistics. With respect, the outcomes of the 2016 Census reveal that the ABS is currently unlikely to be well-placed to be at the forefront of trusted data management projects. The same might be said for many parts of government - a significant brake on the Issues Paper's suggested framework which presupposes both government IT capacity and the capacity to hold the trust of the citizen.
- The tenor of the framework is that the data in question belongs to the Australian government 'a valuable national resource'. The data held is generated by individuals, both with and without their consent. The assumption that this data belongs to the government and is therefore its to share, is a flaw in the suggested framework.

2. What else should the Government take into consideration when designing the legislation?

Any legislative framework must account for the exponentially different character of aggregated data from that of its component parts. Any one agency, or even

multiple agencies, cannot necessarily foresee the implications of aggregation in terms of privacy or sensitivity. Thus the 'consistent and appropriate' safeguarding of data is not of itself a useful framework.

The question of 'ownership' of data must be addressed. Future Wise submits that the suggestion that citizens' data belongs to government is a misstep that fails to recognise data sovereignty in the citizen whose life is under scrutiny.

The framework fails to recognise why government departments do not share data. There is a sound reason for this, recognised from even a pre-digital time: citizens are at risk from function creep where their data is aggregated across government departments. While the Issues Paper purports to recognise 'risk', nowhere does it articulate this previously recognised risk of State overstep with accompanying citizen disempowerment.

Scope of the Bill

3. Should the scope be broader or narrower?

The scope of the legislation appears designed to avoid what is described as a 'risk-averse culture' towards data sharing. Future Wise submits that this is an inappropriate framing of the scope, given that the question central to data sharing is the avoidance of risk: risk for the individual concerned, and thereby risk for the government agency. Risk-aversion is not an obstacle to be overcome by the legislation. Rather it is a disposition that must be encouraged; the principle of 'Do no harm' should apply to government use of data about citizens.

The Bill will not 'by default compel all data to be shared'. Future Wise submits that the Bill must not compel any data to be shared. To the extent that the Bill will facilitate data sharing, this must be provided for according to principles applied to both the donor agency and the donee.

4. Are there entities that should be included or excluded from scope? How would this be justified?

With the increasing tendency for government to outsource its functions, data collected by third party contractors undertaking government business should be covered by the same data principles as government departments.

5. Should any specific categories of data be specifically out of scope? How would this be justified?

Provision should be made for whistleblower protection where it relates to government data.

6. Should exemptions, for example for national security and law enforcement, occur at the organisational level or for specific data categories?

While Future Wise believes that there is an argument to be made for some data to be exempt from release on the basis of national security, we feel it would be appropriate that any exemptions under these areas be made available for review (for example, by the Inspector-General of Intelligence and Security). This would increase public trust that data is not being censored by the government under the banner of national security, where it is not truly justified; see our response to the following question for further detail.

7. Are there instances where existing secrecy provisions should prevail?

It is noted that 'secrecy' provisions relate to 'government data'. Current prohibitions, however, relate to 'secrecy and confidentiality'. If the Issues Paper is suggesting that only government data (such as military secrets) would prevail but not confidentiality of individuals' data, then Future Wise rejects this position.

The Issues Paper identifies that the 500 existing secrecy and confidentiality provisions are 'rarely reviewed or modified'. Certainly, the proposal for a standardised system is simpler, and arguably more reliable than the existing

patchwork of provisions. Future Wise therefore supports a standardised system, subject to an overarching principle of risk-aversion in terms of the desirability of protecting the confidentiality of individuals' information in particular when it is aggregated in novel ways.

Future Wise notes that recently, government has seen fit to disclose individual information into the public domain. Further, this has been found [not to breach](#) the individual's privacy.² Questions arise therefore about the proposed balance between secrecy (that appears to benefit government) and confidentiality (that benefits the citizen). In protecting government data as 'secret' but permitting government to disclose individual data skews the balance of power as between state and citizen.

This incident, including the findings of the OAIC, tests the credibility of government data sharing proposals. It calls into question why secrecy is privileged - as it is framed in this question - while confidentiality is omitted.

Future Wise recommends that the proposed data sharing structure reinforces the obligation on government, including ministers, to maintain confidentiality of individuals' information in all circumstances. This is an iteration of data sovereignty, the rule of law, and respect for the citizen in the face of government power.

The purpose test

8. Do you agree with the stated purposes for sharing data?

Broadly speaking, Future Wise accepts the stated purposes for sharing data.

However, the purpose test is also implicitly expansive. While data may be shared according to the purpose test, the resultant data processing itself may generate further data. Once that data is shared, the original data point has been integrated

² Christopher Knaus, 'Government cleared of privacy breach in robodebt row' (29 May 2019) *The Guardian* ([online](https://www.theguardian.com/australia-news/2018/may/29/government-cleared-of-privacy-breach-in-robodebt-row) - <https://www.theguardian.com/australia-news/2018/may/29/government-cleared-of-privacy-breach-in-robodebt-row>).

in a number of ways. This leaves the individual the subject of that data without control over its ultimate deployment. This poses a risk for that individual that is not contemplated within the purpose test: namely that the scope of a purpose will continue to expand.

The overarching purpose in this case may continue to be in prosecution of government purposes, but the ultimate purpose may be far removed from the original point of data sharing. In this way, government usurps individuals' data sovereignty without any balance between government and citizens' rights.

9. Are there any gaps in the purpose test that would limit the benefits of public sector data use and reuse?

The purpose test includes a crucial gap that limits benefits. This gap is that the purpose must not be inconsistent with human rights. The purpose must not be discriminatory or breach civil liberties. As Australia does not have a bill of rights but relies on tenuous anti-discrimination legislation, it is imperative that the legislative framework embed civil liberties and human rights into its framework.

Future Wise further recommends the establishment of a bill of rights that would uphold civil liberties and non-discrimination in all government data dealings. This would preclude the erosion of civil liberties through legislative change over time.

10. What further detail could be included in the purpose test?

The purpose test should incorporate civil liberties and non-discrimination at its heart.

11. Should data be shared for other purposes? If so, what are those purposes?

Public benefit, in light of civil liberties and non-discrimination, is the only appropriate purpose for data sharing.

12. Should there be scope to share data for broader, system-wide purposes?

Future Wise considers that a broader data sharing scope is fraught with risk for individuals. This relates to the inability to understand all possible outcomes of aggregated data for individuals who are inevitably identified within such a process. This submission therefore considers that there should not be broader, system-wide purposes of data sharing.

13. Should the purpose test allow the sharing of data to administer or enforce compliance requirements?

Future Wise is strongly opposed to these measures. Such a provision may compromise the way in which individuals, in particular, share their data. This will have implications for data quality - an issue for government - but also for individuals. For example, if an individual knows that their health data may be used for compliance, they may be reluctant to disclose information about their health.

Data safeguards

14. Is the Five-Safes framework the appropriate mechanism to ensure data is safeguarded?

Future Wise acknowledges that Five-Safes framework is widely adopted in data sharing contexts. It has been described, however, as a 'structure and an ethos'. Desai et al identify that even with the framework, organisations 'need to address psychological and institutional factors in data access'.³ Therefore, the Five-Safes framework cannot be seen as a definitive answer to questions of data security.

³ Tanvi Desai, Felix Ritchie and Richard Welpton, 'Five Safes: designing data access for research' *Economics Working Paper Series 1601*. – (online: <https://pdfs.semanticscholar.org/1b81/11c8acb9862bf9a07f27afe604ed75224beb.pdf>)

Any data security framework implemented as part of this sharing regime requires frequent review by data security experts to ensure that it remains best-practice in ensuring the safe sharing of public data.

Public sector data sharing arrangements

21. Would this arrangement overcome existing barriers to data sharing and release?

Note comments above concerning 'barriers'. This question fails to grapple with the foundational issue of the benefits for the individual in establishing barriers to data sharing and release. Such data sharing arrangements must incorporate checks and balances to compensate for enhancement of government power at the expense of citizen rights. This is in accordance with the overarching principle of the rule of law, notably in the absence of a bill of rights or entrenched protections of civil liberties.

22. Would streamlined and template agreements improve the process?

While Future Wise is generally in-favour of standardised methodology, we reiterate our points above re: the heterogeneity of public data. Streamlined tools run the risk of oversimplification and failing to take into account the very different nature of these disparate public datasets.

23. Do you agree that data sharing agreements should be made public by default?

Yes. It is imperative that these agreements regarding access to public data are themselves in the public domain, to build public trust in the safety and transparency of the use of their data.

24. What level of detail should be published?

Future Wise believes that the default position should be for the agreements to be fully published on a publicly-accessible webpage and that there should be cautious application of commercial-in-confidence redaction of the agreements.

25. What else should a data sharing agreement contain?

Data sharing agreements must contain protections for those whose data is involved. These protections should not only consist of sanctions in the event of misuse, as, while these may act as a deterrent, are - by themselves - insufficient disincentive to misuse.

26. What other transparency mechanisms could be mandated?

Given the data used is public data, and the Government's stated commitment to the principles of the Open Government Partnership, Future Wise strongly supports a requirement that any publications resulting from the use of public data be under Creative Commons licensing.

Accreditation

27. How long should accreditation as an ADA or Trusted user last?

Accreditation of third parties for access to individuals' data adheres to the overarching tenor of the proposals to enhance the economy, but fails to engage with the need to protect the citizen. Permitting data to move beyond government and the framework of administrative law and constitutional control of government power, introduces a new relationship between the individual and the corporation as the guardian of that individual's data.

Although the government imperative is to maximise the economic benefit of its data, the profit motive of corporations diverges from the role of government and attendant protections of the citizen. It raises questions about the downstream deployment of data and its monetization. The Productivity Commission Report

identified economic benefits, but the deployment of individuals' data in downstream applications for commercial benefit exist beyond the scope of the public purpose.

Once data is released to a third party user, even where accredited, it becomes feral and effectively beyond government control: certainly beyond the control of the person or community to whom it relates. Used, for example, in insurance will have implications for individuals not contemplated within the public purpose of the proposed legislation.

Because of the risks attendant upon such release, Future Wise submits that accreditation should be undertaken with great caution and for a minimum period. It should relate to specific purposes and not beyond.

National Data Commissioner

32. Are these the right functions for the National Data Commissioner?

The National Data Commissioner role is slated to 'champion greater data sharing' including by disseminating good news stories about data sharing. There is no mention of upholding the data sovereignty of individuals, or their rights. This is a fundamental omission and represents the skewed nature of the proposal.

Future Wise recommends a more temperate position description that seeks to manage the balance between the benefits of this exercise of expanded government power, the responsibilities attendant on the exercise of this power and upholding clearly articulated rights of the individuals whose data is at stake.

33. What review powers should the National Data Commissioner have?

See response above; the Data Commissioner should have the ability to review data sharing arrangements and, where required the ability to require parties to these agreements to comply with the requirements of the agreements, the framework and the Privacy Act, or other legislation as appropriate.

Where shared data is being put to use that is clearly not in the public interest, the data commissioner should have the authority to suspend or terminate agreements relating to the data misuse.

34. Should the NDC have the power to conduct an investigation into system wide issues?

Yes.

35. What other actions could the NDC be able to take?

Given the broad nature of the Legislation, and the potential privacy implications of misuse of public data, Future Wise supports broad oversight authority for the Commissioner. It would be reasonable to share some of these roles with the Office of the Australian Information Commissioner, as there will be some overlap, however we note that OAIC has been under significant resource constraint and would require additional financial support to be able to take on additional responsibilities brought about from this Legislation.

36. Are there other ways community values and expectations can be captured and addressed?

Future Wise supports not only the creation of a consumer data right, but also broad based protections to citizen information sovereignty. We believe that this is best achieved with the creation of a Bill of Rights, including the right to privacy and autonomy of control of personal information. If this is not considered feasible, then at a minimum, Future Wise would call for the introduction of measures similar to the European Union's General Data Protection Regulation.

37. What aspects should be taken into consideration when considering consequences for non-compliance with the DS&R Bill?

In line with our previous submissions, Future Wise emphasises that sanctions or penalties for misuse alone are insufficient protection for citizen privacy, and that this is particularly important with as broad a based sharing regime as is proposed by the Legislation.

We encourage the Government to develop the Data Sharing and Release regime with privacy-by-design principles and a strong focus on citizen data privacy.

38. Should the consequences differ depending on the type of data involved or the type of misuse, eg harsher penalties for intentional misuse?

As discussed earlier in the submission, the value of a subset of data does not necessarily lie in the nature of the data itself, but more in its ability to be combined with other available data. It is therefore difficult to stratify data into lower or higher risk, and it therefore follows that there should be some consequences for misuse of any shared data.

Future Wise does not support exemptions for 'good faith' or unintentional misuse; we believe that the risks to privacy from these data are sufficient to justify a deterrent to unintentional misuse such that the agencies making use of shared data will be mindful of the risks and of good data management practices.

39. Should penalties be strict liabilities?

Yes.

40. What would be an appropriate penalty for intentional misuse of data?

Immediate termination of data sharing agreements, and a period of exclusion from further access to shared datasets. For data which relates to individuals, significant financial penalties should also apply.

41. How would responsibility for misuse of data be shared across the data system?

While the end-users of shared data should bear the primary responsibility for the use to which they put the datasets, Future Wise believes it is imperative that the data custodians give due consideration to the scenarios in which their data may be used. Making a dataset accessible where there is the risk (for example) of re-identification of individuals should also carry consequences to the data custodian sufficient to ensure that due diligence is carried out to minimise the risk.

42. To what extent should there be a complaints mechanism and how should it work?

As a system sharing and making use of public data, it is imperative that there be an open, transparent and responsive complaints process, including the scope for members of the public (or civil society organisations) to make complaints about the sharing, release and use or misuse of public data. This would logically be a role of the Data Commissioner, or as discussed above, of the OAIC.

43. Should a complaints mechanism provide for complaints by the public?

Yes.