Business Council of Australia

SUBMISSION

Response to Data Sharing and Release Legislation Issues Paper

August 2018

Business Council of Australia ABN 75 008 483 216

CONTENTS

The Business Council of Australia draws on the expertise of Australia's leading companies to develop and promote solutions to the nation's most pressing economic and social policy challenges.

ABOUT THIS SUBMISSION

The Business Council welcomes the opportunity to respond to the Australian Government's *Data Sharing and Release Legislation Issues Paper for Consultation*.

EXECUTIVE SUMMARY

Greater availability and use of public sector data has the potential to bring significant benefits to the community, such as improved government policy and service delivery, more transparency, and improved accountability.

While the Business Council supports greater use and availability of public sector data, it must be accompanied by proportionate controls to manage the risk of inappropriate collection, sharing or use of data.

The development of *Data Sharing and Release Legislation* provides an opportunity to address barriers to greater use and availability of public sector data, including complex secrecy provisions, a lack of common protocols for data sharing, and a risk-averse culture.

Data sharing and release raise many complex issues, and discussions about best practice use of data are still evolving. The Business Council is willing to work closely with government and other interested parties to work through these issues.

The government's issues paper proposes establishing a one-size-fits-all regime that could be used to share or release any public sector data (including personal data). It would also co-exist with existing regimes for sharing and releasing data.

While the Business Council agrees with many of the proposals in the issues paper, we believe the proposed regime may not be the best model for all types of public sector data:

- The proposed regime appears well suited for de-identified data that should be subject to controlled sharing with researchers or other parts of government, subject to some amendments to make the process easier for users.
- However, we believe identified personal data (or readily identifiable datasets) will require stricter protocols prior to sharing, for example, the granting of consent, notification of use, or compliance with ethical guidelines.

  Government should act as the custodian of individuals' personal data, with the highest levels of integrity and ethics. How identified personal data will be used by government should be made as transparent as possible (acknowledging that this will vary depending on the nature of the use).

  Additional measures could be considered to grant consumers greater access and control over their identified personal data held by the public sector, including better identity management or the application of the Consumer Data Right to government agencies.
- Furthermore, there should be simpler treatment of low-risk datasets (that is, de-identified and aggregated datasets) that are suitable for public release.

KEY RECOMMENDATIONS

1. The legislation should establish a framework that establishes different approaches for the three primary categories of datasets:
    - datasets for public availability and release (de-identified, aggregated datasets)
    - datasets for controlled sharing within government and with researchers in some circumstances (de-identified but potentially identifiable datasets)
    - identified personal datasets (or readily identifiable datasets) for controlled sharing within government.
2. The legislation should establish a dedicated and simple pathway that encourages the publication and release of aggregated and de-identified datasets.
3. The regime proposed in the paper should be limited to those de-identified but potentially identifiable datasets to be shared within government and with researchers (and other organisations as necessary for government service delivery and public policy). The regime should be streamlined and made easier for users.
4. The legislation should include stricter protocols for sharing of identified personal data (and readily identifiable data) within government including, for example, the granting of consent, notification of use, or compliance with ethical guidelines.
5. Additional measures should be considered to grant consumers greater access and control over their identified personal data held in the public sector, including better identity management or the application of the Consumer Data Right to government agencies.

DISCUSSION

Rationale for data sharing and release

The Business Council supports greater use and availability of public sector data, accompanied by proportionate controls to manage the risk of inappropriate collection, sharing or use of data.

The potential benefits to consumers from greater availability and use of public sector data include:

- improved government service delivery, from reducing costs through better targeting, personalising services, and increasing convenience by enabling more integrated service delivery models
- improved transparency and accountability about the operations of government and the impact of policy decisions over time
- better capability for research, analysis and evaluation of government activities
- potential to trigger private sector innovation and investment on the basis of data previously held within government.

It is generally agreed that there are substantial data held by the Australian Government that are not available or used. Many datasets are siloed, not connected with relevant datasets in other parts of government, not available in a useable format, or not reliable.

Barriers to greater availability and use of public sector data include:

- limited interoperability
- a lack of protocols and standards to share data
- the cost of maintaining data sets and making data available in suitable formats
- a lack of clarity about when data is safe to share or release
- insufficient capability among the workforce, and
- a public service culture of risk aversion and disjointedness that stymies collaboration.

In its report, the Productivity Commission suggested that *Data Sharing and Release Legislation* would address some of these barriers, including unclear authority that impedes data sharing and encourage a risk averse mindset, and a lack of protocols for sharing data.

Different requirements for different classes of data

The issues paper proposes what could be described as an overarching, moderately prescriptive control regime for sharing and releasing public sector data. Data would only be shared if they meet a ‘purpose test’. The management and use of the data would be subject to the ‘Five Safes’ risk framework used by the Australian Bureau of Statistics (ABS), and all users of the data would need to be accredited and willing to access data through a secure environment.

This regime appears well suited for de-identified but potentially identifiable datasets that are suitable for controlled sharing within government and with selected researchers (and other organisations necessary for government service delivery or public policy).

However, we believe different treatments are required for: (1) identified personal data (or readily identifiable data); and (2) de-identified, aggregated datasets suitable for release.

1. The currently proposed regime would allow government departments to share identified personal data (or readily identifiable data).

   While individuals may receive benefits from governments sharing personal data to deliver better quality services, it is equally the case that this could be viewed with suspicion by the community, particularly if it is unclear by whom and how the data will be used.

   Given the sensitivity of personal identified data records, the Business Council proposes additional controls, such as the need to obtain express consent, to inform individuals about potential access and use of their data, or to comply with ethical standards.

   We also note that certain data types – such as health data and financial data – will carry additional duties and obligations, including when used by government. Any regime for sharing of those datasets by agencies should not erode the existing protections.

2. On the other hand, in relation to datasets suitable for public release, the regime appears to be overly prescriptive:

   - Not all aspects of the 'Five Safes' framework are relevant for publicly released data: for example, it is not possible to regulate data use or intention after a dataset has been publicly released.
   - The 'purpose test' does not capture all legitimate uses of publicly available government data, such as commercial purposes (for example, the use of geological data for mining).

The Business Council supports a principles-based approach to the legislation. However, the principles should recognise and account for differences across datasets, and focus on the degrees of protection appropriate for different types of data. An overly broad or one-size-fits-all approach that tries to deal with all types of data is likely to introduce unnecessary ambiguity and risk.

We suggest a principles-based framework that recognises the differences between the different types of data and provides an additional level of clarity. A possible suggested framework is below:

Type of dataset		**Objective**	**Suggested role of the Data Sharing & Release Legislation**
Data that should be **publicly released**		Public sector datasets should be made publicly available if they are: • aggregated, • de-identified and not re-identifiable, and • not subject to any of the exceptions outlined below. These data should be made available in their raw form, in useable formats, in a central repository. They should be complete and current. Datasets to be released should be prioritised on the basis of the estimated economic and social benefits from making datasets publicly available, taking into account the costs of making them available and maintaining them.	Encouraging agencies to make these classes of data publicly available.
Data that should be subject to **controlled sharing** (made available to some parties in some circumstances)	De-identified (but potentially re-identifiable) data	Some de-identified but potentially identifiable data should be available, subject to controls such as: • making data available in a controlled environment that restricts users from identifying individuals. • limiting users to government agencies and public policy researchers (and other organisations necessary for the purposes of government service delivery and public policy) • prohibiting any uses beyond public policy or research.	Establishing a control scheme (like the one in the consultation paper). Requiring the development of a set of guidance and governance arrangements that outlines expectations for the ethical use of this data.
	Identified personal (or readily identifiable) data	Consumers should have greater control and access over their identified personal data. In order to share such data within and across government, the legislation should: • require express consent from the data subject, for that particular use; and/or • require notification about access and use of their data; and/or • require compliance with legal constraints (for example, the need to seek a warrant before access) and ethical guidelines (including for the purposes of compliance, national security or law enforcement.)	Upholding requirement to seek express consents / notify individuals / comply with ethical guidelines Establishing a requirement for government-wide ethical guidelines to be developed.

Data for public availability and release

Some aggregated, de-identified datasets are already made available under a range of different regulatory requirements, including the *Public Data Policy Statement* that encourages the public service to make datasets publicly available by default.

The consultation paper proposes making public availability of aggregated, de-identified data contingent on meeting a 'purpose test' and the 'Five Safes' risk framework.

Instead, the legislation should establish a dedicated and simple pathway that encourages the publication and release of aggregated and de-identified datasets.

Identification of priority datasets for release should be undertaken by the National Data Commissioner and prioritised on the basis of the net economic and social benefits from making datasets publicly available.

If the government proceeds with applying a purpose test for datasets to be publicly available, it is essential that the purpose test is expanded to establish "initiation of private sector innovation and investment in new business models, products and services" as a legitimate purpose.

Data that should be subject to controlled sharing

De-identified but potentially identifiable datasets

The regime proposed in the consultation paper is broadly suitable for classes of data that should be subject to controlled sharing (de-identified but potentially identifiable).

As datasets become increasingly disaggregated, there is an increasing risk that de-identified data can be re-identified. Often even the best de-identification efforts cannot entirely eliminate the risk. For this reason, in the absence of express consent, de-identified datasets that are potentially re-identifiable are best shared within a controlled environment where potential re-identification or data misuse can be monitored and prevented.

We understand the preference for this approach to the controlled sharing of data. However, this approach is at odds with the Productivity Commission's recommendation, which was to consolidate all legislative authorities for sharing data under a single regime.

Instead, the paper proposes no change to the existing legislative authorities for sharing data or the secrecy provisions. The proposed scheme is an alternative pathway for data sharing that public service agencies can voluntarily choose to use, in order to override data sharing regimes in other pieces of legislation.

Because this regime is voluntary, it will only be used by the public service if it is simple, convenient and genuinely value adding, beyond existing arrangements. Members of the public service have advised us that the current ABS processes for accrediting users can be lengthy and difficult. This should be improved, if the same processes are used for government-wide controlled data sharing.

Additionally, if government is merely the custodian of data provided by a private sector entity (for example, a regulator holding commercial information), these datasets should not be available for sharing, unless the business has expressly consented to it.

Invariably, greater data sharing increases the risk of data breaches. Although it is not appropriate for this legislation, it should go without saying that government departments sharing additional data must observe the highest levels of cyber security and data protection.

Identified personal data

Rightly, consumers expect that government will take steps to reduce the risk of inappropriate collection, sharing or use of data that are commensurate with the private sector – if not stronger. Governments should not act as if they are entitled to individuals' data (except for compliance and law enforcement purposes). Instead, governments should behave as custodians of individuals' personal data, treating it with the highest levels of integrity and protection.

Stricter controls should be established around sharing of identified personal data (or data that is readily identifiable). The Business Council's initial thinking is that the legislation could:

- require express consent from the data subject, for the specific proposed use, and/or
- require data subjects to be notified about potential access and use of their data, and/or
- require compliance with ethical guidelines and legal constraints (including data shared for the purposes of compliance, national security and law enforcement).

There could be potential benefits for the individual in sharing their identified personal data: for example, the government may be able to improve the personalisation and targeting of its service delivery so an individual receives a vastly more effective service.

However, the decision on whether to share data for that purpose should be made by the individual through the granting of consent. This need not be onerous: agencies could consider creative ways of collecting and managing consent, or providing opt-out options.

We recognise that data sharing is essential for some compliance, national security and law enforcement purposes. This should be undertaken within the boundaries established by a government-wide set of ethical guidelines and the law.

Additional measures for promoting consumers' control and access

As the Business Council has argued on many occasions[1], consumers should have greater access and control over data where they are the subject, including data held by government. This could be one way to alleviate community concerns about government use of personal data, by providing more transparency of data use and giving consumers a greater share of the value generated by data use.

[1] Business Council of Australia, *Submission to the Productivity Commission's inquiry into data availability and use*, August 2016, http://www.bca.com.au/publications/submission-to-the-productivity-commissions-inquiry-into-data-availability-and-use.

Consumers could be given greater access and control through a number of possible avenues:

- The government is proceeding with the establishment of a Consumer Data Right, which will provide consumers greater access and control over their own data held by businesses. The Right will commence first in banking, energy and telecommunications.

  There is no reason, in principle, why identified personal data held by governments should not be subject to the Consumer Data Right as well. The Productivity Commission recommended establishing the Consumer Data Right to "provide greater insight and control for individuals over how data that is collected on them is used." If this is true for businesses, it is also true for governments. The Australian Government holds a range of personal data on its citizens that could greatly enhance convenience for consumers, if it is shared with an individual's consent.

  For this reason, the Commission explicitly recommended that the Consumer Data Right should apply to personal data held by government agencies (excluding security-related data).

- The government could consider possible measures to ensure better management and integrity of individuals' identity.

  Inconsistent treatment of identity across government results in poor quality datasets, inconvenience to individuals, and an erosion of trust in how governments use identified personal data.

  Efficient identity solutions can offer possible benefits including greater convenience, the ability to offer behavioural insights or the opportunity to ensure greater integrity. In fact, identity solutions that are simpler, clearer and more convenient could enhance trust in governments' use of identified personal data, as long as they are carefully designed to manage privacy and security.

  Currently, the most innovative approaches are found in the private sector, and many of these identity solutions offer the highest levels of security. For that reason, governments could incorporate greater private sector expertise in relation to identity solutions.

BUSINESS COUNCIL OF AUSTRALIA
42/120 Collins Street Melbourne 3000 T 03 8664 2664 F 03 8664 2666 www.bca.com.au