Joshua Badge
Lecturer in Philosophy
School of Humanities and Social Sciences
Faculty of Arts and Education
Deakin University

29 July 2018

Data Sharing and Release Bill Feedback
Department of the Prime Minister and Cabinet
PO Box 6500
Canberra ACT 2600

RE: Australian Government Data Sharing and Release Legislation: Issues Paper for Consultation

Thank you for the opportunity to submit comments and requests for clarification on the *Data Sharing and Release Legislation Issues Paper* and the proposed changes to the regulatory framework for data sharing and release between Commonwealth bodies.

Allowing for consistent legislative requirements across government has the potential to produce convenient and systematic data sharing arrangements. Improved data sharing would promote the efficient delivery of government services as well as offering valuable new sources of information for evidence-based policy and research.

However, it is important to note that risk-aversion can be warranted, especially in cases involving sensitive personal data. Therefore, it is necessary to balance the potential benefits of data sharing while acknowledging the possible risks and danger of misuse.

2. Key Principles of the Data Sharing and Release Bill

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

The Issues Paper declares the overall aim of the *Data Sharing and Release Bill* will be to safeguard data sharing and release in a consistent and appropriate way; enhance the integrity of the data system; build trust in the use of public data; establish institutional arrangements, and; promote better sharing of public sector data.

Other aims of the Bill should include maintaining the appropriate level of privacy and security for sensitive or personal data, educating the public, and ensuring appropriate consumer protections.

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

Additionally, it is essential to recognise that the stated aims of the Bill have the potential to come into conflict. For instance, a *de facto* promotion of data sharing may diverge from the aim of promoting public trust in the use of public data in particular contexts.

While much of the data the Government holds may not be personal or sensitive, it should maintain appropriate safeguards for such data. Health data is more sensitive than preferred transport data, emphasising the need for clearly defined safety measures for different categories of information.

Acknowledging that risk aversion may be a barrier to sharing, the desire to avoid potential problems is well-intentioned. It is crucial to carefully consider public concerns relating to the privacy and security of data.

The paper notes that lack of authority often limits data sharing. However, limitations on the authority of government to share data are warranted in some contexts.

I request clarification on the following points raised by the paper in this section:

i. Precisely what legislative measures will be enacted to promote transparency and accountability?

ii. Precisely what safeguards will be put into practice by the *DS&R Bill* and how will they support and interact with the protections in the *Privacy Act 1988* and the *Privacy Amendment Act 2017*?

3. Scope of the Data Sharing and Release Legislation

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

At least three categories of data require special consideration: Census data, health data, and metadata.

The Australian Bureau of Statistics collects Census data on the understanding that it is anonymous. However, there is the possibility that Census data can be collated or aggregated with other datasets with the effect of identifying this information. To ensure the privacy of consumers in relation to Census data, there must be limits on other kinds of sensitive data it can be combined with.

Health data is highly sensitive and potentially identifying data. The government should maintain the principle that health data should be utilised for health purposes only. This would include the utilisation of health data to inform policy or for research purposes but would exclude *de facto* access by national security and law enforcement bodies in the absence of a subpoena, warrant or court order.

Metadata is a privileged category of data. The public understands that it is collected as an anti-terrorism measure, and it should be utilised in this context to the exclusion of others. While researchers and policy makers may desire to have access to this rich body of data for a number of reasons, this would jeopardise public trust in the integrity of data security and their personal privacy. National security and law enforcement bodies should retain exclusive access to metadata in appropriate contexts.

It is essential that any rules or regulations concerning contextual access to data, especially health data and metadata, is explicitly supported by legislation.

I request clarification on the following points raised by the paper in this section:

iii. The scope of the *DS&R Bill* includes all data collected by all Commonwealth entities. Does this include data collected, stored, or managed by third parties including commercial entities contracted or otherwise delegated functions by Commonwealth entities?

iv. The paper declares that there will be 'exclusions' for national security and law enforcement bodies. Does this imply that such bodies will be excluded from employing the *DS&R Bill* or that they will be permitted to bypass the necessary conditions and safeguards?

v. The paper asserts that 'many' of the data secrecy and confidentiality provisions are no longer 'fit for purpose'. This is a legitimate concern and government bodies should review legislation periodically. What are some examples of provisions which are no longer fit for purpose?

4. Streamlining Data Sharing and Release

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

The Five-Safes framework is a generally sensible approach to determining the appropriate control measures for the release of information. However, it may still permit the disclosure of identifying information in some contexts. It is plausible that conventionally de-identified health information shared or released for medical research could identify an individual.

Imagine a circumstance where health data concerning the geographic distribution of medical conditions is released to researchers or made public. An individual with an atypical medical condition or even a common medical condition in a rural or remote area could be identified from this data.

For instance, an individual may be the only person living with HIV in a particular postcode, electorate or other sample areas. This is similarly true of HIV acquisition notifications: due to the relatively low number of new HIV diagnoses an individual becomes more recognisable.

This issue is true of several medical conditions, though HIV is a special case in light of stigma and the risk of prosecution.

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

This is a useful proposal. Making data sharing agreements readily available would increase public confidence in the integrity of data sharing arrangements and would likely improve compliance.

25. What else should a data sharing agreement contain?

Data sharing agreements should demonstrate that the parties involved can satisfy their responsibilities to consumers and achieve the stated purpose justifying the release of information.

I request clarification on the following points raised by the paper in this section:

vi. Will the Five-Safes framework have legislative force or will it be an operational policy?

vii. In either case, what purview will the National Data Commissioner have in the interpretation, modification or application of the framework?

viii. What are the proposed limits on the release of data for research and development purposes? For instance, is research for commercial gain permissible if it has nominal benefits?

6. National Data Commissioner

The creation of a National Data Commissioner supported by a National Data Advisory Council represents a positive and practical step towards securing appropriate oversight, promoting public trust and protecting consumer's interests.

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

The paper insists that the NDC will 'champion greater data sharing', however, this is a disadvantageous conceptualisation of the nature of the NDC from a privacy and security perspective.

The role of the NDC should be to carefully maintain and enforce the consistent and appropriate use of data held by the government. The beneficial use of data held by the government does not testify to a *de facto* position on the relative increase or decrease of data sharing.

Indeed, many of the outlined functions relate to the capacities of the Commissioner as an office of administrative oversight, which may be incongruous with the role of an advocate in a variety of situations. As a consequence, 'good news stories' should not take precedence over regular and accurate reporting on privacy and security issues.

Additionally, it would be beneficial to make the advice provided by the Advisory Council publicly available. This would promote transparency and public trust in the NDC and is consistent with the suggestion that data sharing agreements be made publicly available.

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

To perform the role outlined in the paper, the NDC will need to be vested with the authority to investigate, prevent, manage and respond to misconduct and breaches.

This should include the authority to investigate and, if necessary, invalidate data sharing arrangements when they are found to contravene best practice, the Five-Safes framework, or legislation or are otherwise susceptible to misuse.

Additionally, the NDC should be vested with the authority to invalidate Data Authority and Trusted User accreditation in similar contexts. The NDC must be permitted to administer and moderate such entities to ensure that they employ the data for the purposes it was released.

39. Should penalties be strict liabilities?

The paper suggests that a 'strict criminal liability culture' would de-incentivise data sharing and discourage openness about breaches or misconduct. The reasoning for this conclusion

needs to be stated with greater clarity to assess its validity. As it stands the conclusion is questionable.

Criminal liability is an effective method to ensure accountability and de-incentivise the inappropriate or malicious use of confidential, personal or sensitive data. The omission of criminal liability would critically undermine public trust in Commonwealth bodies sharing information.

Liability would only de-incentivise the sharing of data where a) the legislation was ambiguous, b) there was generally poor understanding of the provisions or c) the data should not be shared. The solution to this difficulty is clear, unambiguous legislation and a substantive education campaign for public servants, not the weakening or removal of criminal liability.

Further, leaving decisions about the appropriate penalties for intentional misuse at the discretion of the NDC is an opaque and capricious approach to the management of misconduct. This would further serve to undermine public trust. There should be standards that are clear in their application and purpose.

It is crucial to recognise that criminal liability does not necessitate a strict or impermissible data sharing culture, and there is no reason why a 'good faith' immunity could not be additionally legislated.

I request clarification on the following points raised by the paper in this section:

ix. What is the proposed selection process and criteria for the Advisory Council?

x. Specifically, what industries and areas of government will have representation on the Advisory Council?

Summary of Position

The public must be provided with clear rules which outline how data can and cannot be used prior to enacting legislation. Intelligible examples should be supplied to facilitate public comprehension of the system, including: how different categories of data can be utilised, what kinds of safety measures are included and the limitations on the use of data.

The *DS&R Bill* must acknowledge the need for privacy and security for sensitive data and ensure robust consumer protections. Communicating the issues arising from data sharing arrangements to the public about is critical. It should also recognise that limitations on data sharing authority may be valid in some circumstances.

The creation of a National Data Commissioner supported by an Advisory Council is an advantageous proposal. However, unambiguous legislation, civil sector education and rigorous consumer protections are required to create a comfortable but legitimate sharing culture within government while ensuring that public trust is not eroded.

Recommendations

- Census data, health data, and metadata are exceptional categories of data which require significant attention: measures should be taken to ensure Census data remains anonymous; health data should only be utilised for health reasons in the absence of

judicial authorisation, and; metadata should only be exploited for the purposes that it was collected i.e. for anti-terrorism measures.

- The Five-Safes framework must include a nuanced understanding of whether data can identify an individual. Conventional de-identification may not be suitable in all contexts.
- Data sharing agreements should be made public by default and should contain a reasonable demonstration that the parties can fulfil their legislative obligations, especially to consumers.
- The purpose of the National Data Commissioner should be to carefully maintain and enforce the appropriate use of data held by the government, not merely to advocate for the greater sharing of data.
- The advice provided by the National Data Advisory Council to the National Data Commissioner should also be made publicly available to encourage transparency and accountability.
- The NDC should be authorised to invalidate data sharing agreements as well as Data Authority and Trusted User accreditations.
- It is critically important to include criminal liability in the legislation to ensure accountability and de-incentivise the inappropriate or malicious use of sensitive data. A 'good faith' release clause can also be included.

It is crucial that the changes proposed in the *Data Sharing and Release Bill* do not undermine public trust in the privacy and security of intimate or identifiable information, nor public confidence in government bodies in general. Educating public servants and communication with the public is paramount to successful legislative change in this sphere.

Regards,

Joshua Badge
Deakin University