University of Melbourne Response

Data Availability and Transparency Bill – Exposure Draft and Accreditation Framework Discussion Paper

Department of Prime Minister and Cabinet

November 2020

Executive Summary

The University of Melbourne welcomes the opportunity to offer comment on the exposure draft of the Data Availability and Transparency Bill and the Accreditation Framework Discussion Paper. The Department of Prime Minister and Cabinet is to be commended for the highly collaborative approach it has taken to establishment of the data sharing framework. This approach is delivering a positive reform agenda that represents a step change on current arrangements, with a clear trajectory for further improvements.

In broad terms, the arrangements for sharing public sector data must include robust safeguards that ensure that data is shared only with trusted users and for appropriate purposes, while also ensuring that the public benefits of data sharing are realised. This demands processes for accessing data that are based on clear standards. The express intent in the proposed legislation and associated instruments for high degree of transparency in the accredited entities, data sharing and data sharing agreements is to be applauded, as this is important for building public trust in the arrangements and allowing reputation to act as an incentive to best practice conduct.

While commending the proposed legislative reforms, the comments below outline areas where we suggest that the legislation could be further strengthened. The draft legislation includes a set of accountability mechanisms designed to ensure that data is not shared inappropriately, but leaves data custodians with considerable discretion in assessing data requests. We have concerns that this may lead to data requests being rejected without sufficient reason and may lead to inconsistencies in data custodian decisions. While acknowledging the need to balance the compelling opportunities associated with enabling greater data sharing with the imperative for safeguards, we encourage further consideration of stronger accountability measures so that decisions to not share data come with a clear justification. These measures should include making rejected requests reviewable, and a post-enactment review to scrutinise the number of rejected requests. We also suggest consideration of the OECD Council's recommendation on data health governance as a model for assessing data requests.

This submission addresses other areas where the draft legislation could be refined. The University of Melbourne strongly supports Indigenous Data Governance and urges a separate scheme to ensure that control over relevant data is provided to Indigenous communities. We also propose strengthening the approach to security and privacy protection, to ensure that the concepts and understandings of data privacy always correspond with best technological practice, as this is another facet important to underpin consumer confidence in data sharing. Finally, we argue that the legislation, while principle based, could be improved by including more detail in the Bill itself, such as some commitments regarding the decision-making processes, rather than leaving so much to delegated legislation.

This submission also includes a brief response to the Accreditation Framework Discussion Paper. It is important that the accreditation framework is designed so that responses to applications are timely and so that the costs associated with securing and maintaining accreditation are minimised. The University also emphasises the importance of institutional capacity relating to ethics review and approval being a condition of accreditation.

For further information or to discuss this submission please contact Professor Liz Sonenberg, Pro Vice-Chancellor at l.sonenberg@unimelb.edu.au.

Recommendations

Response to the exposure draft of the Data Availability and Transparency Bill

The importance of data access

The University of Melbourne recommends that:

- The data sharing framework should ensure accountability for decisions made by data custodians not to share data, in addition to decisions to share data
- Decisions not to share data should be reviewable
- A post-enactment review of the Act should scrutinise the number of data sharing requests that have been rejected, and the reasons for those decisions
- Consideration should be given to using the OECD Recommendation relating the use of personal health data for research purposes as an exemplar set of standards for the assessment of data requests.

Indigenous data governance

The University of Melbourne recommends that a separate scheme for Indigenous data be established to ensure appropriate control is provided to Indigenous communities.

Digital Privacy

The University of Melbourne recommends that:

- The concept of digital privacy that is applied in the data sharing framework always corresponds to best technological practice
- The lack of robustness in current consent requirements for data collection under the Privacy Act should be taken into account in deciding whether consent for data sharing is necessary.

Level of detail in the legislation

The University of Melbourne recommends that:

- Important elements of the data sharing reforms should be included in the Act, rather than being left to delegated legislation
- Consideration be given to sunset clauses on any delegated legislation to ensure that it is subject to ongoing parliamentary scrutiny
- The legislation be strengthened by
    - making data custodian decisions reviewable
    - requiring timely decisions, and
    - including some detail on how the public interest is to be understood in the assessment of data requests
- That individuals and organisations other than data scheme entities be allowed to make a complaint to the Commissioner where they believe the Act has been breached.

Response to the Accreditation Framework Discussion Paper

The University of Melbourne recommends that:

- The accreditation framework should be designed to ensure that responses to applications are timely and the administrative costs associated with securing accreditation are minimised
- The renewal process should be streamlined as much as possible with a focus on managing risk without unnecessarily repeating the initial application process
- Capability around ethics review should reach similar standards as that used for research projects, and processes should align, where possible, with established ARC and NHMRC requirements
- Unique frameworks for the handling and use of Indigenous data are developed in consultation with the Indigenous peoples to whom that data relates and applies
- High expectations around ethics and data privacy expertise are conditions of gaining and maintaining accreditation.

Response to draft Data Availability and Transparency Bill

Importance of data access

The *Draft Data Availability and Transparency Bill Consultation Paper* rightly acknowledges the benefits that a "rigorously safe, streamlined, transparent and accountable framework for data sharing" has for the Australian community.[1] Controlled access to quality public sector data for trusted users is critical in supporting properly informed public policy and leading research and development. This has become particularly clear in the context of the response to the COVID-19 crisis. Managing the public health and the economic impact of the pandemic depends upon high quality data revealing how particular cohorts are affected. More generally, improving access to public sector data for researchers will drive improvements in research performance and the public value that it delivers. Australians make a sizeable investment in our research system: the proposed legislative reforms represent an opportunity to increase the outcomes generated by that investment.

In broad terms, the reforms set out in the draft Bill will improve the extent to which data is made available to trusted users. Notwithstanding the improvements, there are areas where it can be strengthened to better ensure that accredited entities and individuals are able to access data where this is appropriate. As proposed, the legislation may result in an overly restricted sharing framework where data requests are rejected despite having a sound justification. We encourage further consideration on the matters of review, transparency, and public interest.

Section 23 of the Bill explicitly states that data custodians are required only to consider requests for sharing data; there is no duty for custodians to actually share data. Nor are decisions to not share data reviewable: as noted in the Explanatory Memorandum, "Data sharing decisions by data custodians will not be reviewable on their merits under this scheme. Such decisions are best made by data custodians as they have a full understanding of the risks of and public interest in sharing their data."[2] Decisions to accept or to reject sharing requests – and the reasoning behind those decisions – will be included in the Commissioner's annual report, but as the Commissioner has no power to compel custodians to share[3], other checks and balances should be clear in the framework. We note also that as part of their annual reporting, the Commissioner might seek to identify reasons for such denials and improve guidance to resolve any uncertainty leading to those decisions. We support such investigation and guidance and recommend that it extend to assessing compliance with internationally recognised good practice regarding review and approval procedures including, but not limited to, such procedures being robust, objective and fair; operating in a timely manner and promoting consistency of outcome; operating transparently while protecting legitimate interests in confidentiality.

The discretion allowed to data custodians when assessing requests is accompanied by high thresholds for ensuring that data is not shared inappropriately.

> "The data sharing scheme contains robust safeguards to ensure sharing occurs in a consistent and transparent manner, in accordance with community expectations. The Bill authorises data custodians to share public sector data with accredited users, directly or through an ADSP, where:

[1] Office of the National Data Commissioner, *Data Availability and Transparency Bill 2020, Consultation Paper*, p.iii.
[2] Explanatory Memorandum, Draft Bill, p.10.
[3] See Ibid., p.32.

- sharing is for a permitted purpose – government service delivery, informing government policy and programs, or research and development;
- the data sharing principles have been applied to manage the risks of sharing; and
- the terms of the arrangement are recorded in a data sharing agreement."[4]

While the need for a robust set of safeguards is clear, it is important that the threshold for data sharing is not set so high that sharing rarely occurs. There is a danger that the principles are interpreted very stringently and that reasonable data requests from researchers are denied. A further potential barrier to researchers accessing data relates to cases where the data custodian has a particular interest in access being limited. In some cases, there may be a conflict between the public interest that provides a justification for sharing the data and the custodian's own interest in limiting access.

The accountability mechanisms built into the data sharing framework are geared towards ensuring that data is not shared inappropriately: it is important that accountability and oversight also apply to decisions to *not* share data. We note that under S116 the Commissioner maintains a public register of names of parties to each data sharing agreement and mandatory terms (S18), but this only requires the agreement to identify which of the purposes set out in S15(1) is met and these are cast in very general terms (e.g., research and development);more granular transparency regarding purpose could be appropriate and advantageous on the public register. Beyond this, the number of sharing requests from accredited entities that have been rejected, along with the reasons for those decisions, should be scrutinised as part of a post-enactment review of the Act. As well as assessing the extent to which useful data sharing has been facilitated, the review could address any concerns about inappropriate or over-sharing.

Finally, we note that the OECD Recommendation on Health Data Governance includes an item on 'review and approval' of the use of personal data which identifies the principles that should guide responses to sharing requests:

> Review and approval procedures, as appropriate, for the use of personal health data for research and other health-related public interest purposes. Such review and approval procedures should:
>
> i. Involve an evidence-based assessment of whether the proposed use is in the public interest;
> ii. Be robust, objective and fair;
> iii. Operate in a manner that is timely and promotes consistency of outcomes;
> iv. Operate transparently whilst protecting legitimate interests; and
> v. Be supported by an independent multi-disciplinary review conducted by those with the expertise necessary to evaluate the benefits and risks for individuals and society of the processing, and risk mitigation.[5]

Consideration should be given to using this as a model for articulating clear standards for the assessment of data requests.

Recommendations

The University of Melbourne recommends that:

- The data sharing framework should ensure accountability for decisions made by data custodians not to share data, in addition to decisions to share data

[4] Ibid., p.5.

[5] OECD (2017), *Recommendation on Health Data Governance*. https://www.oecd.org/health/health-systems/health-data-governance.htm

- Decisions not to share data should be reviewable
- A post-enactment review of the Act should scrutinise the number of data sharing requests that have been rejected, and the reasons for those decisions
- Consideration should be given to using the OECD Recommendation relating the use of personal health data for research purposes as an exemplar set of standards for the assessment of data requests.

Indigenous data governance

Issues relating to Indigenous data governance represent a key set of challenges for the legislative settings relating to data sharing. The Indigenous Data Network,[6] administered through the University of Melbourne, assists Indigenous communities in developing the technical capability and resources to enable them to manage their data for community advancement. The Network's activities include:

- Identifying best practice in community data collection, management and access
- Assisting Indigenous communities to apply best practice in data management by providing technical and educational resources
- Developing specific strategies and approaches to make better use of data over which Aboriginal and Torres Strait Islander people have ownership
- Creating a directory of databases to increase awareness of existing data sets and how to access them
- Integrating and archiving Indigenous datasets and preventing the orphaning of important datasets which would be detrimental to communities
- Negotiating with government and non-government organisations to ensure data activities are aligned with Indigenous priorities, and that data collected is available for sharing under appropriate conditions
- Working with the Indigenous Research Exchange to develop guidelines and best-practice case studies for research and data analysis in evaluation to improve Indigenous outcomes
- Coordinating educational programs to ensure the development of a critical mass of Aboriginal and Torres Strait Islander people with expertise in the data sciences.

Given its expertise in the issues that are raised for Indigenous communities concerning the use of data, the University of Melbourne endorses the contributions made by the Indigenous Data Network to the discussion around data availability and transparency. We draw particular attention to the work of Network members on a National Framework for Indigenous Data Governance[7] that identifies six key features of existing data governance frameworks, legislation, guidelines and principles relevant to the interests of indigenous Australian individuals and communities in data as an asset.

We support a cautious approach to the sharing of data relating to Indigenous Australians, given the particular risks entailed where this data is shared inappropriately. We note, for example, that Indigenous communities are especially vulnerable to privacy-related risks that come with the collection and storage of data. The risk of individuals being re-identified (see below) through anonymised data is heightened when dealing with minority groupings and with sparsely distributed populations.

[6] https://mspgh.unimelb.edu.au/centres-institutes/centre-for-health-equity/research-group/indigenous-data-network

[7] Rose, J., Langton, M., Smith, K, and Clinch, D. ``Indigenous Data Governance in Australia: Towards a National Framework.'' (23pp). Requests for copies should be directed to james.rose@unimelb.edu.au

One of the dangers in the proposed data sharing framework is that public interest assessments are couched in broadly utilitarian terms such that the interests of Indigenous communities are potentially outweighed by some other set of interests in decisions on whether data should be shared. The way to address this risk is to ensure that Indigenous communities have control over the relevant data through involvement in public interest assessments, such that what counts as the public good is determined by (rather than *for*) Indigenous communities. The University of Melbourne suggests a separate scheme for Indigenous data to ensure appropriate control is provided to relevant Indigenous communities.

Recommendation

The University of Melbourne recommends that a separate scheme for Indigenous data be established to ensure appropriate control is provided to Indigenous communities.

Digital privacy

The University of Melbourne suggests that the protections of individual privacy could be strengthened. The Explanatory Memorandum states:

> "The Bill takes a principles-based approach in establishing the data sharing principles. This will ensure the principles remain applicable as technology, data management practices, and community expectations evolve over time. The Commissioner may make data codes and guidelines to provide further detail on how to apply the data sharing principles"[8].

These guidelines and processes should not be so prescriptive as to undermine the purpose of principles-based regulation and should be subject to sunsetting or review at regular intervals. This will ensure that the understanding of digital privacy applied in the data sharing framework is robust and corresponds with best technological practice.

We have concerns that the Five Safes approach for managing risks associated with data sharing may not provide adequate protection. Differential privacy is a relatively new framework for guaranteeing the privacy of individuals in a sensitive dataset when releasing aggregate statistics or machine-learned models on such data andshould be part of an approach to privacy-by-design in data sharing systems. Researchers at the University of Melbourne are currently working with the ABS on differential privacy as a more robust approach to guaranteeing individual privacy, and we note it was in use for the 2020 United States Census.

With regard to potential concerns of individuals about the use of personal information, the Explanatory Memorandum states:

> Where the data being shared includes personal information, subclause (1)(b) requires consent for sharing to be sought from the individuals concerned unless it is unreasonable or impracticable for the data scheme entities to do so. The standard of consent required is that set by the Privacy Act. The 'unreasonable or impracticable' language is drawn from section 16A of that Act, and should be interpreted using relevant guidance on consent made by the Australian Information Commissioner.[9]

In many circumstances the Privacy Act does not require consent or consent may be inferred. This is not considered best practice (see for example the ACCC Digital Platform Inquiry[10]). The lack of robustness in current consent requirements for data collection under the Privacy Act should be taken into account in deciding whether consent for data sharing is necessary.

[8] Explanatory Memorandum, p.23.
[9] Ibid., p.24.
[10] ACCC Digital Platform Inquiry https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platforms-inquiry

Recommendation

The University of Melbourne recommends that:

- The concept of digital privacy that is applied in the data sharing framework always corresponds to best technological practice
- The lack of robustness in current consent requirements for data collection under the Privacy Act should be taken into account in deciding whether consent for data sharing is necessary.

Level of detail in the legislation

The draft Bill proposes to include only general principles on a number of key issues, leaving much of the detail to delegated legislation. The main drawback of this approach is that delegated legislation is subject to a much lower level of scrutiny than Acts of Parliament. In many cases, delegated legislation remains unchanged for a number of years, and can work to subvert the intent of the legislation itself.

Given this, the University of Melbourne argues that additional elements of the data sharing reforms should be included in the Act rather than left to legislative instruments. This is consistent with a 'soft law' approach to regulation, which involves the Data Commissioner issuing Guidelines. Where delegated legislation is to be used, the Explanatory Memorandum should provide a clear justification as to why this approach is being taken. Consideration should also be given to sunset clauses on legislative instruments to ensure that they are subject to ongoing parliamentary scrutiny.

Specific issues where the proposed reforms would be strengthened by detail being included in the Bill include:

- **Review of decisions on data sharing:** As noted above, a review of decisions by data custodians around data sharing supports accountability around these decisions. The legislation should provide a basis for reviewing these decisions.
- **Timeliness:** The time it takes for researchers to gain accreditation and to access data is critical to the public benefit that the data sharing framework generates. Delays in either providing accreditation or in making data available can inhibit the utility of public data. The legislation should require timeliness in decisions relating to accreditation and to applications for data access.
- **Public interest:** The concept of 'the public interest' has a central place in the sharing framework in that it is one of the key considerations that supports data being made available to trusted users. The Bill should provide some detail on how the public interest is to be understood in the assessment of data requests. As discussed, we recommend that a utilitarian assessment of public interest, which does not adequately respect the interests of those whose data is used, is not permitted under the scheme. Guidance on public interest assessment currently indicates that different risks and benefits must be "weighed against each other" but does not indicate that those whose interests are 'outweighed' need have good reason to expect or accept the trade-off. We welcome reference to community expectations and norms and suggest that it should be possible to challenge a public interest determination through the National Data Commissioner.

Perhaps outside the scope of the legislation, we question why only "data scheme entities" can make a complaint to the Commissioner if they have reason to believe a party to be in breach of responsibilities under the Act. Given there will be public registers, it is desirable there are clear mechanisms entitling a wider range of people to raise complaints or issues to the attention of the Commissioner that might result in investigation.

Recommendations

The University of Melbourne recommends that:

- Important elements of the data sharing reforms should be included in the Act, rather than being left to delegated legislation
- Consideration be given to sunset clauses on any delegated legislation to ensure that it is subject to ongoing parliamentary scrutiny
- The legislation be strengthened by
    - making data custodian decisions reviewable
    - requiring timely decisions
    - including some detail on how the public interest is to be understood in the assessment of data requests
- That individuals and organisations other than data scheme entities be allowed to make a complaint to the Commissioner where they believe the Act has been breached.

Response to Discussion Paper on Accreditation Framework

The following comments offer a specific response to consultation question 5, relating to data capability and how it should be assessed in the accreditation process. The University of Melbourne's general position on the accreditation framework is that its design should ensure timely responses to applications and should minimise the administrative costs associated with securing and maintaining accreditation. While some level of administrative impost is unavoidable, an overly onerous application process and unnecessary delays in securing accreditation will result in bottlenecks in the research pipeline as well as drawing resources away from research activity. We also have some concerns that the processes associated with accredited users (section 2.2.1) may be overly onerous and should be reviewed to ensure an appropriate balance between safeguards and practicality. The Office of the National Data Commissioner should be resourced at a level that it is able to process applications in a timely fashion as well as performing its other compliance and oversight functions.

Accreditation renewal is an area where the administrative impost may be higher than necessary if not designed sensibly. The Discussion Paper indicates that Accredited Users will be required to renew their accreditation every three years, and Accredited Data Service Providers every five years. While those timeframes are appropriate, the renewal process should be streamlined as much as possible with a focus on managing risk without unnecessarily repeating the initial application process.

5. Are there elements of data capability that should be given more or less weight in the accreditation process, i.e. making elements mandatory or optional?

Institutional capacity around ethics assessment and approval and sophisticated understanding of security and privacy should be seen as important considerations in the accreditation. Since in many cases the data is to be accessed for research and development purposes, ethics review should reach similar standards as that used for research projects. These processes should align with established ARC and NHMRC requirements, where appropriate. Entities with limited experience in these areas could be encouraged to partner with research organisations for the purposes of building capability.

There are two specific areas that we emphasise when it comes to data awareness and training: one relating to the use of Indigenous data, and the other relating to privacy.

Indigenous data

The comments above noted the need for Indigenous data governance to be reflected in the Data Availability and Transparency legislation, such that input into data sharing decisions is afforded to Indigenous communities. Considerations on data governance should also be a feature of the accreditation framework. Given the historical misuse of data relating to Indigenous people, unique frameworks for the handling and use of Indigenous data should be developed in consultation with the Indigenous peoples to whom that data relates and applies.

Privacy

There is currently a review of the Privacy Act 1988 as part of the Government's response to the Australian Competition and Consumer Commission's Digital Platforms Inquiry. This has been initiated because there are concerns that the Privacy Act is not fit-for-purpose in responding to data privacy, including arising from the ACCC Digital Platform Inquiry. However, currently the Privacy Act does not represent best practice in collecting and handling personal data. While 'privacy coverage' is a relevant consideration in accreditation, robust training around data privacy is of critical importance.

Recommendations

The University of Melbourne recommends that:

- The accreditation framework should be designed to ensure that responses to applications are timely and the administrative costs associated with securing accreditation are minimised
- The renewal process should be streamlined as much as possible with a focus on managing risk without unnecessarily repeating the initial application process
- Capability around ethics review should reach similar standards as that used for research projects, and processes should align with established ARC and NHMRC requirements, where appropriate
- Unique frameworks for the handling and use Indigenous data are developed in consultation with the Indigenous peoples to whom that data relates and applies
- High expectations around ethics and data privacy expertise are conditions of gaining and maintaining accreditation.