lifecoursecentre

Data Sharing and Release Legislative Reforms – Response to Discussion Paper (September 2019)

15 October 2019

THE UNIVERSITY OF QUEENSLAND AUSTRALIA

THE UNIVERSITY OF WESTERN AUSTRALIA

THE UNIVERSITY OF MELBOURNE

THE UNIVERSITY OF SYDNEY

Australian Government
Australian Research Council

LIFE COURSE CENTRE

The Australian Research Council Centre of Excellence for Children and Families over the Life Course (the Life Course Centre) is a national research centre focused on investigating the drivers of deep and persistent disadvantage in Australia. We are also committed to leveraging our evidence-based research to develop new knowledge, technology and practices to benefit Australian children and families living in disadvantage.

The Life Course Centre is administered by The University of Queensland and is a collaboration with The University of Western Australia, the University of Sydney and the University of Melbourne. We also have a wide range of collaborative links to national and international academic, government and non-government partners.

In order to better understand the causes and life course consequences of disadvantage, and to develop effective interventions to address it, our research requires access to integrated public sector data about children and families experiencing disadvantage. Access to linked longitudinal administrative data enables us to investigate people's interactions with government services and institutions over time, and identify the critical time-points at which interventions can be most effective.

The Life Course Centre supports reforms to improve public sector data sharing and use, and we welcome the opportunity to respond to the **Data Sharing and Release Legislative Reforms Discussion Paper (September 2019)**, released by the Office of the National Data Commissioner within the Australian Government Department of Prime Minister and Cabinet.

For more information on the Life Course Centre visit: www.lifecoursecentre.org.au

Life Course Centre
Institute for Social Science Research, The University of Queensland
80 Meiers Road, Indooroopilly, Queensland 4068 Australia
Phone: (07) 3346 7477
Email: lcc@uq.edu.au

This Life Course Centre submission has been prepared by:

Professor Janeen Baxter, Life Course Centre Director, The University of Queensland
Mr Francis Mitrou, Life Course Centre Research Fellow, The University of Western Australia
Dr Sarah Johnson, Life Course Centre Research Fellow, The University of Western Australia

Life Course Centre Chief Investigators:

Professor Janeen Baxter, The University of Queensland
Professor Deborah Cobb-Clark, University of Sydney
Professor Lorraine Mazerolle, The University of Queensland
Professor David C. Ribar, University of Melbourne
Professor Cate Taylor, The University of Western Australia
Professor Karen Thorpe, The University of Queensland
Professor Matthew Sanders, The University of Queensland
Professor Mark Western, The University of Queensland
Professor Stephen Zubrick, The University of Western Australia

We have engaged with the Office of the National Data Commissioner in several ways since it was established in 2018, including a brief submission to the Data Sharing and Release Legislation: Issues Paper in 2018, invitations to Life Course Centre Data for Policy events and workshops, and attendance at several Data Sharing and Release roundtables.

The Life Course Centre commends the Office of the National Data Commissioner (ONDC) for its extensive consultation on the Data Sharing and Release Legislative Reforms. The process has been inclusive, fair, thoughtful, and comprehensive in its coverage.

The Discussion Paper is representative of the high-quality and thorough approach ONDC is undertaking with these reforms. Please take our responses as support, rather than criticism, of the Discussion Paper and the overall process of the legislative reforms.

Our submission has been guided by **the 14 points provided in Section 1.6 ‘Have your say’** in the Data Sharing and Release Legislative Reforms Discussion Paper.

1. **Do you think the distinction between data sharing and data release is clear? How could this distinction be clearer?**

Yes, the distinction is clear.

2. **What are the challenges for open release of public sector data?**

One challenge is the potential for different interpretations of the same data set when it is available for analysis, rather than available as a set of pre-populated tables. A data set needs to be released with a comprehensive description of the data and its limitations. A second challenge with the public release of multiple data sets, is increased risk for the potential re-identification of individuals. Deploying disclosure control tools that adequately protect against re-identification, while still providing enough granularity to be useful for policy and research, remains a challenge.

3. **Do you think the Data Sharing and Release legislative framework will achieve more streamlined and safer data sharing?**

We are very positive that the legislative framework will provide a more streamlined process for data sharing among public sector organisations, and also create cultural change that encourages safe data release. The proposed legislation will provide greater assurance and an overarching framework for data security. Although the ONDC will not be compelling organisations to share data, the intention to provide education and targeted assistance to those organisations that appear to be risk adverse and need additional support to achieve cultural change, is welcomed. The legislation will particularly assist those organisations that are less advanced in their data sharing. For some, there may be a need for funding and resources to prepare their data for sharing and integration, including bringing data sets together within a government agency. As discussed below in response to Question 8, there is an opportunity to further streamline data sharing, release and access processes via centralized processes for assessing data sharing requests (proposed ONDC-housed Data Sharing and Release Project Approval Panel), and enable the delivery of data to researchers in a timely and affordable way.

4. **What do you think about the name, Data Sharing and Release Act?**

The name is fine, as a large part of the legislation is about data sharing. However, the role of the Act relating to data release to the public is less clear in the name. Alternative names that could better convey the intent of the Act could include: ‘Data Sharing and Public Release Act’, or ‘Data Sharing, Integration and Release Act’.

5. **Do the purposes for sharing data meet your expectations? What about precluded purposes?**

Yes, these purposes meet expectations. However, it will be important to have mechanisms in place to avoid duplication and re-identification of individuals, including the duplication of single-agency and cross-agency data sets held in different locations. The transparency measures will be helpful in this respect. The preclusion of data sharing for compliance and assurance purposes is welcomed and should assist in building community trust, which has been impacted by high-profile cases such as Robo-debt. Developing strong public support for data sharing is critical, and highlighting how lives and services can be improved, and costs saved, can play an important role in this.

6. **What are your expectations for commercial uses? Do we need to preclude a purpose, or do the Data Sharing Principles and existing legislative protections work?**

This aspect is still unclear. While the main purpose for commercial users appears to be for research and development, it may be better if a specific purpose test is articulated. It is clear that commercial users could use “open data” for planning and research purposes in the same manner as any other Australian. However, it is less clear if commercial users could be “trusted users” with access to customised research data in the same way that accredited university and government researchers can via custodian-approved projects. Commercial users would need to pass the test of being “trusted users” and be subject to accreditation. Their access to shared data would also need to be approved by an ethics committee with evidence of stakeholder support. This process is likely to benefit larger companies with greater access to resources to train users and house data.

It is also important to note that there is a difference between having “trusted-user” accreditation and pursuing projects deemed to be in the public good. There will often be greater scrutiny of how public data is used by commercial enterprises, compared to academic and government researchers. The public know that profit is the ultimate goal of commercial enterprises, and will be sceptical of profits generated via public sector data, without a commensurate level of public return. The public will need a high level of assurance about sharing public data for commercial use. Ensuring the public good component outweighs any potential commercial benefit should be part of the purpose test for approved commercial sector projects.

7. **Do you think the Data Sharing Principles acknowledge and treat risks appropriately? When could they fall short?**

Yes, risks are acknowledged appropriately. However, where data custodians are defined as organisations, it is not clear who will be responsible within any given organisation for making decisions around the sharing and release of data. This becomes more complex in organisations that preside over multiple administrative data collections, and organisations that merge and de-merge with changes of government. It will be important to have strong governance arrangements to ensure that assessments are consistently applied and do not become the responsibility of any single individual within an organisation.

8. **Is the *Best Practice Guide to Applying Data Sharing Principles* helpful? Are there areas where the guidance could be improved?**

Yes, the Guide is very helpful and essential to facilitating a functioning data sharing and release environment. We have identified some areas of the Guide that could be enhanced. In **the data sharing request (page 8 of Guide)**, a standardised form for data custodians could allow more uniform application of the principles within and across government organisations. This would assist with streamlining and transparency. Further clarity may be needed around **Data Sharing Agreements (page 9 of Guide)**. As currently stated, the Agreement is between a data custodian and an organisation but several projects can be covered by the Agreement. The purpose test will need to be applied to all projects and, in some large research organisations, there may be multiple projects that are different in purpose. This leads to two possible scenarios: an Agreement for each project (potentially multiple within an organisation); or a single Agreement with an organisation with separate schedules outlining specific details per project. The latter would allow an Agreement with an accredited organisation, covering wider issues of governance and IT security, and specific schedules to the Agreement that relate to each project and the people involved. We agree it is important to have a responsible officer, or dedicated team, which has oversight of an organisation’s Agreement and projects. We support **the idea (page 13 of Guide) of streamlining assessments** of project proposals for experienced data users.

In the set of **questions to ask before applying the data sharing principles (Page 11 of Guide)**, we believe some of these will be covered by the overarching question of whether the organisation and the individual are accredited data users. Similarly, in **the set of questions to ask on applying the settings principle (page 21 of Guide)**, much of this could be covered by the accreditation process.

In the set of **questions to ask on the project principle (Page 14 of Guide)**, some of these appear to be pitched to a data custodian starting from scratch within an organisation. For example, questions 3, 4 and 6 are about the process within the agency for dealing with data requests that need to be standard practice. This should ideally be a committee, and not an individual, and should include a group of individuals with a high-level strategic view who can understand the benefits, and risks, of projects in a wider societal context.

While recommending that data sharing projects be considered by an **ethics committee approval process (page 13 of Guide)**, it is not clear what steps are involved in ethics approval, and the approval order. In some Australian States (e.g. Western Australia), custodian approval is required before going to an ethics committee. This seems logical where specific data collections are covered by separate legislation, as the custodians can determine if the data request is feasible and the data can be legally released. An ethics committee also has to assess public good and privacy concerns (as guided by conditions in the NHMRC National Statement for Ethical Conduct in Human Research, 2.3.10), the need for consent, and assess an organisation's capacity to maintain data security. These intersecting roles of data custodian and ethics committee need clarifying. Furthermore, where data requests involve multiple agencies or require access to integrated data sets held by an Accredited Data Service Provider (such as ABS or AIHW) it is not clear who the data custodian will be.

Overall, we believe there is an opportunity to further streamline data sharing, release and access processes, for relatively low investment, by developing a more coordinated and legislatively-aligned system for Commonwealth custodians than currently occurs in many States. This would provide a more efficient system for all. Central to this system, could be an ONDC-housed Data Sharing and Release Project Approval Panel. This could act as a "one-stop shop" for applications and approvals, with only the most challenging projects and those requesting "non-standard" data sources, requiring review outside the panel and within the relevant custodian agencies. The panel could include ONDC, data custodians, the National Indigenous Australians Agency and selected community members, and would have broad oversight, rather than individual custodians making decisions in departmental silos. This would relieve individual custodians of the responsibility of project approval and rely on a central panel for decision-making and review of projects requesting data from a core set of linkable datasets. The panel could be supported by a published repository of all metadata for available datasets to assist approved researchers with refining their research questions and applications. This concept would allow custodian agencies to concentrate on their core business while their administrative data is managed by people who are expert in the field and best placed to judge the appropriateness of the use of that data proposed by government, academia, or commercial use.

9. **Do the safeguards address key privacy risks?**

The safeguards are comprehensive, but there will always be an element of risk involved and the public may want a better understanding of how their details will be used for research. An example worth mentioning is when DHS identified patients who had been prescribed lithium to recruit patients for a bipolar disorder study. The DHS mailed letters on the behalf of a research team. Although there was no breach and the project had ethics approval, it was not well received and the letters represented a threat to privacy that had not been well considered. Sensitive topics and vulnerable populations need more stringent processes. An ONDC-housed Data Sharing and Release Project Approval Panel would be well placed to preside over such processes.

10. **Are the core principles guiding the development of accreditation criteria comprehensive? How else could we improve and make them fit for the future?**

The core principles will form a good basis for developing accreditation criteria, but the details will need fine-tuning. For example, in relation to skills and capabilities, will consideration be given to the track record of an organisation and individuals? There is also no mention of data integration skills and capabilities for Data Service Providers. Working with integrated data comes with higher risks, but it is not clear why individuals within accredited Data Service Providers will not be required to undertake accreditation. Some organisations will be data custodian and data user, and may need to show they do not have a conflict of interest in data use for a particular project. Further thought will be needed on how commercial users are accredited. A workshop with community members, academics, data custodians and commercial interests, could provide clearer direction.

11. **Are there adequate transparency and accountability mechanisms built into the framework, including Data Sharing Agreements, public registers and National Data Commissioner review and reporting requirements?**

The transparency and accountability mechanisms appear very adequate. The registers are an excellent idea not only for transparency but also to streamline processes. But it is not clear if the registers will miss projects with business-as-usual arrangements (i.e. no override necessary by the new legislation), or if they will encompass all data sharing. Annual system-wide reporting will be valuable and should focus on information not already obtainable from registers, and should not be too onerous. Highlighting success stories and identifying gaps would be effective ways to further improve and streamline processes.

12. **Have we achieved the right balance between complaints, redress options and review rights?**

This is a difficult question, as approaches are still being developed. A complaints mechanism is important for all in the system. At this point, it seems there is no avenue for appeal of data sharing decisions, but we understand that a data custodian with repeated refusals may be approached for discussion and assistance.

13. **Have we got our approach to enforcement and penalties right for when things go wrong? Will it deter non-compliance while encouraging greater data sharing?**

It is not clear what the penalties would be, other than reverting to penalties under the existing secrecy provision and consistent with existing provisions under the Privacy Act. This makes sense and is a good approach. Not applying strict liabilities to penalties is also a good approach, as it is more likely that a breach would be a genuine mistake rather than an act of malicious intent. However, the impact of these breaches may vary in severity, and the public need to know that appropriate recourse is available. We support having protections (good faith defence) in place for the data custodians who have shared data according to the principles authorised by the new legislation. The graduated approach to enforcement with tailored actions to suit problems is appropriate. As previously mentioned, ensuring that public trust in data sharing and release is built and maintained is paramount. To maintain this trust, serious deterrents need to exist for anyone contemplating using data in a manner that is not authorised by their data use agreement, especially if that use results in a data breach or public re-identification. Extreme penalties must exist for parties who make *deliberate and malicious* attempts at re-identifying public data via un-authorised matching outside of ONDC frameworks and agreements.

Nothing will erode public trust quicker than the knowledge that people who have acquired administrative information legitimately through official channels and processes are deliberately re-identifying persons for nefarious means, or simply to make private information public. This is potentially worse for public sentiment than governments using data for unpopular compliance purposes. Therefore, penalties for *deliberate and malicious* breach or nefarious use of data need to be severe, including the option of criminal charges. Those convicted of a deliberate breach should forfeit their trusted user accreditation for life. Accidental breaches or re-identifications should be treated differently, and case-by-case, with an emphasis on apology, investigation, training, fines and reviews of ONDC trusted user or Accredited Data Service Provider status.

The public needs to be assured of appropriate action for serious breaches that impact on lives, even if accidental. Re-accreditation may be required for organisations presiding over a breach. For accidental breaches, larger penalties should be directed to the organisation, rather than the individual. If the breach occurred via individual action, rather than organisational failure, the individual responsible for an accidental breach should be disciplined by their organisation and lose their individual trusted user accreditation for an appropriate period.

14. **What types of guidance and ongoing support from the National Data Commissioner will provide assurance and enable safe sharing of data?**

ONDC should continue to engage with the community to promote the benefits of data sharing and release, and address concerns about privacy. This should include discussions about consent and what it means for data use that aims to inform policy and improve services for wider community benefit. Another way to grow public support could be to include community representation on key committees and data advisory groups.

Work should also continue towards making data sharing a national system, including a synchronisation of Commonwealth and State legislation and removing barriers towards cross-jurisdictional and Commonwealth-State data sharing projects. ONDC also needs to ensure that Indigenous Data Sovereignty is incorporated into governance, representation and access arrangements. To date, it appears that consultation with the Aboriginal community on the proposed legislation has been limited. We support your inclusion of the new National Indigenous Australians Agency in your consultation process, and suggest you include a senior Indigenous representative on your Advisory Council.