



**Law Council**  
OF AUSTRALIA

*Office of the President*

**22 October 2019**

Ms Deb Anton  
Interim Data Commissioner  
Office of the National Data Commissioner  
PO Box 6500  
CANBERRA ACT 2600

By online submission portal.

Dear Sir/Madam

### **DATA SHARING AND RELEASE LEGISLATIVE REFORMS DISCUSSION PAPER**

1. The Law Council welcomes the opportunity to comment on the Office of the National Data Commissioner's (**ONDC**) *Data Sharing and Release Legislative Reforms Discussion Paper (Discussion Paper)*.
2. The Law Council is grateful for the assistance of the Law Society of New South Wales and the Data and Privacy Committee of the Law Council's Business Law Section in the preparation of this submission.
3. In its 2017 report, *Data Availability and Use*, the Productivity Commission concluded that 'lack of trust by both data custodians and users in existing data access processes and protections and numerous hurdles to sharing and releasing data are choking the use and value of Australia's data', and recommended 'the creation of a data sharing and release structure that indicates to all data custodians a strong and clear cultural shift towards better data use that can be dialled up for the sharing or release of higher-risk datasets'.<sup>1</sup> The Productivity Commission recommended reforms 'aimed at moving from a system based on risk aversion and avoidance, to one based on transparency and confidence in data processes, treating data as an asset and not a threat'.<sup>2</sup>
4. The Law Council notes that the Discussion Paper reflects the findings of the Productivity Commission and proposes empowerment of data sharing between Australian Government agencies, provided the data sharing arrangements comply with relevant data governance requirements (detailed in the Discussion Paper). The Law Council supports this approach.

#### **Data analytics output transparency**

5. The Law Council notes that the objectives of the proposed data sharing and release legislative reforms include developing more targeted government policies, programs and service delivery by streamlining and modernising data sharing arrangements. The Law Council supports the removal of unnecessary barriers to government data

---

<sup>1</sup> Productivity Commission, *Data Sharing and Use* (Report No 82, 31 March 2017) 2.

<sup>2</sup> Ibid.

sharing and the development of a single, unified approach to data sharing to improve the fragmented and often unclear approach that currently exists.

6. In the Law Council's view, constraints on data sharing that are reliable, consistently implemented and verifiable, as proposed in the Discussion Paper, are necessary to ensure data sharing between government agencies is appropriately justified, controlled and transparent. The Law Council submits that regulatory settings must ensure data sharing outputs between government agencies are appropriately evaluated and managed, so that when those outputs are used to create outcomes that affect individual citizens (whether or not identified or identifiable), or targeted cohorts of citizens that are inferred through data analysis to share like characteristics, these outcomes are demonstrably fair, equitable, accountable and transparent.
7. The Discussion Paper does not specifically address how the Australian Government will deal with data analytics outputs that effect outcomes that citizens might not anticipate. The Law Council notes that conventional data privacy regulatory analysis may not address how outputs might be used to infer characteristics of particular unidentifiable individuals, or to enable small cohorts of individuals to be treated differently from other individuals, or otherwise illegally or unfairly.
8. The important issues of algorithmic discrimination, and whether a citizen should have a right to inferences about them being fair and reasonable, are largely outside the scope of current Australian data privacy laws (although they are now under active consideration and debate). However, the Law Council suggests that there is a risk of discussions about responsible data sharing to create outputs becoming confused with ongoing debates about how to best ensure that governments' uses of analytics or behavioural 'nudges' to effect outcomes are fair, equitable, accountable and transparent.
9. The Law Council recommends that the development of any data sharing legislative reforms take into consideration the broader questions of acceptable bounds of government algorithmically-driven activities, that are within the scope of a number of other ongoing reviews, including the Australian Human Rights Commission's [Human Rights and Technology Project](#).

### **Consent issues**

10. As recognised in the Discussion Paper, some of the criticisms that have been leveraged against the proposed reforms centre around the issue of consent. The Law Council notes that citizen consent is currently not required for a range of data matching activities conducted by the Australian Government, and that in many cases, the concept of consent is of limited practical utility when citizens deal with Australian Government. Often, a citizen will face a choice of providing 'consent' to obtain a service or benefit, or not receiving that service or benefit. This problem is magnified in circumstances where the personal information in question was collected on a compulsory basis for limited and often regulated purposes.
11. However, in the Law Council's view, it is important to consider either obtaining consent or providing more stringent requirements for the release of sensitive data and data relating to vulnerable people, particularly children. As set out above, data analytics outputs can lead to outcomes that citizens may not anticipate which need to be considered when dealing with more vulnerable citizens. By way of example, there have been significant concerns about the sharing of address and location data of victims of domestic and family violence through the My Health Record. For the

purpose of the draft data sharing and release legislation the Law Council submits that the definition of sensitive data needs to be wider than the definition under the *Privacy Act 1988* (Cth) to include the address and location details of victims or those at risk of family violence. Further, consideration should be given to the suppression of data for those at risk, or the implementation of a process similar to that used by the Australian Electoral Commission with regard to silent voters. Where sharing is needed, preference should be given to only doing so where the data is adequately, securely and permanently de-identified.

## Data Governance

12. Data governance requirements must be paramount in the establishment of any legislative regime of this kind. The Law Council submits that any data sharing and release legislation must require government agencies to establish and maintain robust processes and procedures that ensure the integrity and security of public data is maintained. The Law Council notes the ever-increasing role that online data plays in the lives of individuals and the commensurate importance of ensuring that 'big data' sources, such as those held by the Australian Government, are kept adequately and appropriately secure.
13. The data governance requirements detailed in the Discussion Paper largely reflect the ONDC's *Best Practice Guide to Applying Data Sharing Principles*, released in March 2019.<sup>3</sup> These Principles are based on the Five Safes Framework, developed in the United Kingdom. The aim of the Principles is to enable a privacy-by-design approach to data sharing, by balancing the benefits of using government data with a range of risk-management controls and treatments (particularly those managing disclosure risks). By focusing on controls and benefits, instead of merely reducing the level of detail in the data to be shared, the Principles can assist in maximising the usefulness of the data. The Law Council submits that such privacy impact assessments must be conducted by an independent body or expert and outcomes of such assessments shared with the community.
14. However, the Principles are not of themselves an authorisation framework, or an alternative to privacy impact assessment. A privacy impact assessment will be required to ensure that each stage in a data sharing environment is:
  - (a) appropriately assessed, through reliable and verifiable technical, operational and legal controls to address how an isolated data linkage and data analytics environment is established and managed; and
  - (b) to mitigate risk of disclosure of personal information outside that isolated environment.

## Other Issues

15. It is unclear what the mechanism will be for the reporting of data that has been shared including if, and how, citizens will be notified that their data has been shared. The Law Council submits that if consent will not be obtained, particularly when the shared data is sensitive data, that there is a need for transparency in the process.

---

<sup>3</sup> Office of the National Data Commissioner, *Best Practice Guide to Applying Data Sharing Principles* (15 March 2019) <<https://www.datacommissioner.gov.au/sites/default/files/2019-08/data-sharing-principles-best-practice-guide-15-mar-2019.pdf>>.

16. The Law Council notes that the proposed data sharing is likely to coincide with the implementation of the Consumer Data Right as an economy wide reform enabled by the *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth). It will be important to ensure that there is clarity as to how these reforms will intersect.
17. The Law Council also notes that it will be important that training for Data Custodians include the potential risks of sharing sensitive data and how to properly share sensitive data.

**Contact**

18. Thank you again for the opportunity to provide a submission in response to the Discussion Paper. The Law Council looks forward to engaging with the ONDC in 2020 following the release of an exposure draft of the legislation.
19. Should you require further information or clarification, please contact John Farrell, Senior Policy Lawyer on [REDACTED]

Yours sincerely



**Arthur Moses SC**  
**President**