




THE LAW SOCIETY  
OF NEW SOUTH WALES

Our ref: P&DL:EEap1783143

16 October 2019

Mr Jonathan Smithers  
Chief Executive Officer  
Law Council of Australia  
DX 5719 Canberra

By email: [john.farrell@lawcouncil.asn.au](mailto:john.farrell@lawcouncil.asn.au)

Dear Mr Smithers, 

### **Data Sharing and Release Legislative Reforms discussion paper**

Thank you for the opportunity to comment on the Office of the National Data Commissioner's Data Sharing and Release Legislative Reforms discussion paper. The Law Society's Privacy and Data Law Committee has contributed to this submission.

In its 2017 report, 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>

We note the discussion paper reflects these proposals and proposes empowerment of data sharing between federal government agencies, provided the data sharing arrangements comply with relevant data governance requirements (detailed in the discussion paper). The Law Society supports this approach.

Our general observations about the proposed reforms are outlined below.

### **Data analytics output transparency**

The Law Society notes that the objectives of the 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 Society supports the removal of unnecessary barriers to government data sharing. In our 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

---

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

<sup>2</sup> *Ibid.*

appropriately justified, controlled and transparent. We support the development of a single, unified approach to data sharing to improve the fragmented and often unclear approach that currently exists.

The Law Society submits that regulatory settings must, however, 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.

The discussion paper does not specifically address how government will deal with data analytics outputs that effect outcomes that citizens might not anticipate. We note 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.

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). We consider, however, there is a risk of reasoned 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.

While perhaps outside the scope of this current consultation, we recommend 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 and Equal Opportunity Commission's *Technology Rights Project*.

### **Consent issues**

As recognised in the discussion paper, some of the criticisms that have been leveraged against the proposed data sharing and release legislative reforms centre around the issue of consent. We note 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 government. Often, a citizen will face a choice of providing 'consent' to obtain a government service or benefit, or not getting that service or benefit.

We believe however it is important to consider either obtaining consent or providing more stringent requirements for the release of sensitive data and data relating to 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 unforeseen consequences of the sharing of address and location data through the My Health Record which has had an impact on women and children at risk of family violence. For the purpose of the draft data sharing and release legislation we submit 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. We also submit consideration be given to the suppression of data for those at risk or the implementation of a similar process used by the Australian Electoral Commission with regard to silent voters.

## Data Governance

Data governance requirements must be paramount in the establishment of any legislative regime of this kind. We submit 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. We note 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.

The data governance requirements detailed in the discussion paper largely reflect the National Data Commissioner's (NDC) *Best Practice Guide to Applying Data Sharing Principles*,<sup>3</sup> released in March 2019. 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, we consider the Principles can assist in maximising the usefulness of the data.

We note 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.

The Law Society supports this approach.

## Other Issues

It will be important that training for Data Custodians include the potential risks of sharing sensitive data and how to properly share sensitive data.

It is also 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. We submit 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.

Thank you again for the opportunity to provide our input to a submission to this consultation. Should you have any further queries in relation to this issue, please contact Adi Prigan, Policy Lawyer, on (02) 9926 0285 or at [adi.prigan@lawsociety.com.au](mailto:adi.prigan@lawsociety.com.au).

Yours sincerely,



Elizabeth Espinosa  
**President**

---

<sup>3</sup> Department of Prime Minister and Cabinet (Cth), 'Best Practice Guide to Applying Data Sharing Principles' (15 March 2019).