THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: P&DL:JWap2068103

7 April 2021

Ms Elizabeth Owers
Office of the Secretary
Department of Customer Service

By email: data.sharing@customerservice.nsw.gov.au

Dear Ms Owers,

Review of the *Data Sharing (Government Sector) Act 2015*

Thank you for the opportunity to contribute to the review of the *Data Sharing (Government Sector) Act 2015* (NSW) (the Act). The Law Society of New South Wales' Privacy and Data Law Committee has contributed to this submission, which responds to various questions posed by the Department of Customer Service (the Department) as part of this review.

1. General comments

The Law Society supports efforts to better regulate, and clearly define the scope, permissible uses and reasons for the sharing of data, both in the public and private sector.

We consider that well drafted and managed data sharing statutes play an important role in facilitating controlled and safeguarded data linkage. In this context, the Law Society supports the existence of fit-for-purpose data-sharing laws that clearly establish how relevant state government agencies may use and share data. Such statutes should supplement, and not displace, data privacy laws and administrative law.

We recognise that the sharing of data between government agencies, including for analytics purposes, is necessary. Data sharing must, however, also be proportionate, and respectful of the rights and expectations of individual citizens to have data about their movements and other activities, and their interests and preferences, handled fairly by each government agency. Such data sharing must not erode each citizen's right to go about their private life without undue oversight and surveillance. While the NSW Government and its agencies may legitimately seek to facilitate fair and respectful data sharing, the Government must also ensure that it does not undermine citizens' current levels of trust in the Government's handling of data about them.

The NSW Government has expressed an intention to be a leader in the adoption of data use and sharing to benefit citizens of NSW. The Department's ability to implement initiatives to improve the efficiency and convenience of citizens dealing with the Government and its agencies largely depends upon high levels of citizen trust that the Department will ensure that uses of data about them are fair, proportionate and consistent with citizen expectations about how this data will be used and shared. However, the Auditor-General for NSW's December 2020 Report into Service NSW's handling of personal information, which focused

THE LAW SOCIETY OF NEW SOUTH WALES
170 Phillip Street, Sydney NSW 2000, DX 362 Sydney
ACN 000 000 699 ABN 98 696 304 966
lawsociety.com.au
T +61 2 9926 0333 F +61 2 9231 5809
E lawsociety@lawsociety.com.au
Law Council OF AUSTRALIA
CONSTITUENT BODY

on processes, technologies, and governance arrangements for how Service NSW handles customers' personal information, found clear deficiencies in that handling.[1] Citizens' digital trust requires assurances that such deficiencies will not occur, through government agencies' demonstrably reliable adoption of best practice in data use and sharing, and not only through the detection of deficiencies after problems occur. Before-the-event prevention is necessary to protect all data sharing initiatives, because any problem in any data sharing instance can undermine the digital trust of citizens.

COVID-19 data management has accelerated citizen understanding about how appropriately controlled and safeguarded data sharing between government agencies may aid service delivery by government. It has also heightened expectations that data sharing will be appropriately and demonstrably controlled and safeguarded. Because of the vulnerability of digital trust among many citizens, and community concerns about disproportionate Government oversight and surveillance, government agencies must demonstrate high levels of transparency and openness in relation to when, how and why data about citizens (whether or not that personal information is protected by data privacy laws) is shared between government agencies.

2. What is your experience with the Data Sharing Act? What is working well? What isn't working?

The Law Society considers there are gaps and limitations in the current Act, which largely reflects its age: five years is a long time in the modern field of applied data science. We consider the Act is due for substantial review and amendment.

In addition to NSW, two other states have enacted data sharing statutes: South Australia, under the *Public Sector (Data Sharing) Act 2016* (South Australian Act), and Victoria, under the *Victorian Data Sharing Act 2017* (Victorian Act). The Data Availability and Transparency Bill 2020 (Commonwealth Bill) is currently before the Commonwealth Parliament.

Each act is an authorising statute, overriding limitations imposed by earlier statutes as to how relevant state government agencies may use and share data, subject to any further limiting conditions as defined in the relevant data sharing act.

Divergences between the state statutes include:

- the extent to which the statutes override relevant state information privacy or health data privacy statutes in relation to data inputs provided to the authorised data analytics authority, and

- the extent of jurisdiction and control of the state privacy / information commissioner in relation to uses and disclosures of personal information, being information about individuals that are reasonably identifiable by any recipient of relevant information, whether or not the subject individual is identifiable to the data discloser.

In our view, data privacy law provides a measure of assurance as to data sharing between agencies, but should not be the only or primary control of data sharing. In some circumstances, data privacy laws may reasonably be qualified by a data sharing statute. However, the data sharing statute should then ensure that any data sharing that is authorised by that statute is appropriately and demonstrably controlled and safeguarded.

[1] Audit Office of NSW, *Service NSW's handling of personal information* (Special Report, 18 December 2020).

Statutory protections and data sharing principles

The NSW Act does not limit the operation of the NSW data privacy statutes in any relevant way, or override the jurisdiction of the NSW Privacy Commissioner in her administration of those statutes.[2] Nothing in the NSW Act permits or requires the NSW Data Analytics Centre (DAC), or any other government sector agency, to collect, use, disclose, protect, keep, retain or dispose of any government sector data that is health information or personal information, except in compliance with the NSW privacy legislation. However, the DAC may operate with the benefit of authorisations by the NSW Privacy Commissioner, who has facilitated limited, controlled and safeguarded data linkage (for example, in the NSW Privacy Commissioner's Direction under subsection 41(1) of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) in relation to the *'Their Futures Matter'* Project).

By contrast, section 15 of the Victorian Act allows the sharing of identifiable data by data sharing bodies and designated bodies with the authorised data analytics body without an individual's consent and in circumstances where the sharing may not otherwise be permitted by relevant Victorian privacy legislation. To this extent, the Victorian Act limits a citizen's right to privacy. However, that limitation is itself subject to statutory protections, set out in sections 18 and 19 of the Victorian Act.

Most citizens' interactions with government, and the provision of information by citizens to government, cannot properly be characterised as voluntary and therefore, consensual. Because of the limited role that an affected individual's consent can play in relation to the collection, use and sharing by governments of data about those citizens, a data sharing statute might allow for limited circumstances in which data about citizens may be shared without their consent. However, appropriate controls, safeguards and oversight are necessary.

We suggest the Department consider amending the NSW Act to include similar statutory protections to the ones set out in sections 18 and 19 of the Victorian Act.

In addition, we suggest consideration be given to inserting required 'principles' to be followed in data sharing, such as the enactment of the so-called Five Safes framework as 'Trusted Access Principles' in section 7 of the South Australian Act, or proposed clause 16 (data sharing principles) of the Commonwealth Bill. Adoption of such principles would better articulate the requirements for controls and safeguards in the conduct of a data sharing environment, including the allocation and use of data linkage keys, or the operation of a deidentification data linkage environment, and what the reasonable controls and safeguards for the operation of that environment would be.

Sharing of data analytics outputs

Under the NSW Act, the DAC is authorised to share with the source government sector agency, the results of data analytics work that it has carried out on data provided to it by that agency. The DAC is not authorised to share outputs with any other agency, person or body.[3] In our view, an authorised data analytics service provider should be authorised to share appropriately aggregated, and therefore, deidentified, outputs with other government agencies for permitted uses.

Non-individuating data sharing purposes that might reasonably not be subject to consent are appropriately controlled and safeguarded data sharing; linkage; and the creation of outputs

[2] *Data Sharing (Government Sector) Act 2015* (NSW) s 12.

[3] *Data Sharing (Government Sector) Act 2015* (NSW) s 9.

of aggregated insights that assists in the planning for the better delivery of government services, informing government policy and programs, and research and development.

For data sharing and data outputs only for these purposes, the Privacy Commissioner's prior approval might not be required, provided there is appropriate independent oversight to ensure that relevant controls and safeguards are applied at all times, including (in particular, but not only) controls as to the use and application of outputs.

To this extent, we consider the NSW Act could be broadened to specifically cover data sharing which otherwise would be regulated by the NSW data privacy statutes, including the PPIP Act. Currently, each agency is subject to its own compliance obligations under the PPIP Act. Including data sharing requirements in the NSW Act would provide a legislative framework to support the current data sharing between NSW Government agencies.

We note the Act does not consider dynamic data sharing and is based on the concept of a disclosure and a recipient. In our view, this does not reflect the reality of current data interactions, and we consider the Act should envisage two-way data sharing and the management of created or generated data by each agency involved in generating that data.

Right to call-in data

The DAC cannot call-in data for data sharing. The Minister may direct a government sector agency 'in writing to provide specified government sector data that it controls to the DAC within 14 days or such longer period specified in the direction, but only if the Premier has advised the Minister that the data concerned is required to be shared for the purpose of advancing a Government policy'.[4]

We suggest a broader right to call-in data may be appropriate. However, any such right should be subject to certain requirements, outlined below:

- the person / agency calling in the data must be able to demonstrate that the Five Safes Principles (outlined above) have been considered and met in relation to the data,
- transparency requirements should be included in relation to the call-in right, for example in the form of an annual report to Parliament or the Privacy Commissioner on the use of this power (as is the case in Victoria),
- such a right should be subject to provisions in subject-specific legislation, for example, laws relating to access to driver licence information and CCTV information should not be overridden, and
- any right to call-in data should enable the one-off provision of a data set, rather than an ongoing data feed, or access to a database. That is, a call-in should replace the section 41 process in the PPIP Act, rather than set up a long term, comprehensive data sharing regime.

As outlined above, transparency, conditions and independent oversight must be paramount in the establishment of any regime of this kind. A commissioning entity must be required to demonstrate that certain conditions have been considered and met and that the call-in is appropriate and necessary in the circumstances. We consider that any erosion of citizen trust in the government's handling of data about them generally, for example through short-term focussed decisions for expediency, may have significant consequences for the future

[4] *Data Sharing (Government Sector) Act 2015* (NSW) s 7(1).

government use of data, even if that later use is in the public's interest (note for example, the public's response to the issues raised by the Robodebt scheme).

Broader accreditation / authorisation framework

The DAC is the only data linkage authority authorised under the Act. Provided that technical and operational controls and safeguards are appropriately articulated in amendments to the Act and imposed as a condition to obtaining and mandating accreditation as a data linkage authority, we consider that the Act could establish an accreditation framework that would allow other public or private bodies to manage data sharing and operate data linkage environments handling NSW government data sets. The Commonwealth Bill provides an example of an appropriate accreditation framework.

We suggest an authorisation framework should also allow for mutual recognition of accreditation of relevant linkage authorities under corresponding State and Territory schemes and under the Commonwealth scheme, so as to better facilitate coordinated and controlled data sharing of data sets controlled by different levels of Australian government.

Where data is shared under an authorisation and handled within a data environment managed by the DAC or another accredited data handling authority, further use and applications of outputs outside the authorisation framework might also be allowed, but only then with prior, case-by-case review and consideration by the NSW Privacy Commissioner, as is currently required. Any authorisation framework that stands outside the case-by-case control and oversight of the NSW Privacy Commissioner should be clearly delineated, as well as subject to its own, transparent controls and safeguards, and supervision by an oversight authority.

3. What changes are needed to the Act?

We have made a number of suggestions for amendments to the Act above. The following comments further explain the basis for our recommendations.

Data analytics output transparency

We note that there are deficiencies in the existing combination of data privacy laws and administrative law remedies, both in NSW and Commonwealth legislation, in relation to potential outcomes enabled by data outputs from data sharing. Many forms of data sharing (such as through data linkage of disparate data sets using a pseudonymised transactor key) are not closely regulated by data privacy law, yet may still enable the creation of outputs that can be used to impose individuated (differentiated) outcomes upon individuals or small cohorts of individuals. That outcome might be any of denial of offer of a service, a different price for a service, withdrawal of a service, a demand for payment or reimbursement, an investigation or enforcement action.

The Law Society submits that regulatory settings must ensure that 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.

We note the Act does not address how government agencies should deal with data analytics outputs that effect outcomes that citizens might not anticipate. We suggest consideration be given to controlling such algorithmic individuation, including in relation to whether a citizen should have a legislated right to appropriate regulation of algorithmic individuation. We also

suggest consideration be given to enacting requirements to ensure that inferences made by government agencies using data about individual citizen's movements and other activities, or interests and preferences, are fair and reasonable.

Consent issues

We note that citizen consent is currently not required for a range of data linking activities conducted by governments in Australia, 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.

The Law Society considers it important, however, to consider either obtaining consent or providing more stringent requirements for the sharing 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 system, which has had an impact on women and children at risk of family violence. We submit the definition of sensitive data should 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.

As noted above, some non-individuating data sharing purposes might reasonably not be subject to consent. Contrast, for example, enforcement related purposes, which should not be so permitted. The definition of 'enforcement related purpose' in clause 15(3) of the Commonwealth Bill provides a good example.

4. Part 3 of the Act deals with data sharing and privacy safeguards – are the current safeguards effective in protecting public sector data? Why?

The Law Society notes that Part 3 of the Act provides high-level provisions around data privacy, government confidentiality and commercial confidentiality safeguards. However, no detail is provided about technical, operational and legal data governance, and data management.

The Law Society considers that data governance requirements must be paramount in a legislative regime of this kind. We submit that any data sharing 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 Australian governments are kept adequately and appropriately secure.

Additional safeguards

In addition to the enactment of statutory protections and principles outlined above, we consider section 12 of the Act should be significantly strengthened, including by amending the Act to prescribe mandatory privacy requirements. These could be based, for example, on the recommendations in relation to data sharing between agencies that the Auditor-General made in her report on Service NSW's handling of personal information. We suggest the obligation to establish and implement detailed protocols for the sharing of data, including personal information, the monitoring of risks and complaints, and the response to mitigating risks, could be a legislated obligation and should, as a minimum, be required to be reported

on, on an annual basis, by any agencies involved in sharing data involving personal information.

5. **Do you think the Act needs to enable data sharing outside of NSW Government (i.e. other governments, non-government organisations, private businesses)? If so, with who? Why? Should there be any limitations?**

The Law Society considers the Act should not preclude data sharing that involves third party data sets, whether from other governments or businesses. However, wherever the data sharing involves data about citizens for which a NSW government agency is a data custodian, the framework outlined above should apply.

That noted, and as suggested above, we consider an authorisation framework should also allow for mutual recognition of accreditation of relevant linkage authorities under corresponding State and Territory schemes and under the Commonwealth scheme.

For completeness, we note that many of the issues raised in this submission are the subject of national consideration and debate. Further, the privacy landscape at the Commonwealth level is currently under review and possible amendment (through the current review into the *Privacy Act 1988* (Cth) being conducted by the Commonwealth Attorney-General's Department). To the extent that any data sharing legislation will establish and maintain robust processes and procedures that ensure the integrity and security of public data is maintained (as recommended throughout this submission) we consider it will be important to address interoperability with the Commonwealth regime.

Thank you again for the opportunity to provide out 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.

Yours sincerely,

Juliana Warner
President