Law Council
OF AUSTRALIA

Office of the President

15 August 2018

Dr Phillip Gould
Assistant Secretary
Office of the National Data Commissioner
Department of Prime Minister and Cabinet
1 National Circuit
CANBERRA ACT 2600

By email: datalegislation@pmc.gov.au

Dear Dr Gould

New Australian Government Data Sharing Release Legislation: Issues paper for consultation

1. The Law Council welcomes the opportunity to provide a submission on the New Australian Government Data Sharing and Release Legislation: Issues paper for consultation (**Consultation**).

2. The Law Council acknowledges the assistance of its Privacy Law Committee (**the Committee**) of the Business Law Section and the Law Institute of Victoria in the preparation of this submission.

3. The Law Council has had the benefit through the Committee of a briefing by the Department of Prime Minister and Cabinet (**Department**). The Law Council is grateful for the opportunity afforded by the Department and welcomes the opportunity for further consultation and discussion in respect of the Data Sharing and Release Bill (**the Bill**), specifically on an exposure draft the Bill once available.

4. At this stage of the Consultation, the Law Council is focussing on the following legal issues as these relate to privacy:

    - confidentiality and secrecy;
    - de-identification; and
    - accountability and liability.

Confidentiality and secrecy

5. As noted in the Consultation, the scope of the data release is intended to include data currently covered by secrecy and confidentiality provisions across more than 175 different types of Australian Government Legislation. Many of these provisions remain relevant, current and are actively relied on by the various departments and agencies.

Telephone +61 2 6246 3788 • ***Fax*** +61 2 6248 0639 • ***Email*** mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra • 19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Organisations and individuals sharing information with those departments and agencies provide information in trust and reliance on confidentiality and secrecy. Changes to the confidentiality and secrecy arrangements will have numerous consequences for all parties in the information collection and dissemination process. These need to be carefully reviewed and addressed accordingly.

6. Typically, confidentiality and secrecy provisions are specific and prescriptive.[1] Many carry criminal sanctions for non-compliance.[2] The Bill is proposed to be a piece of principles-based legislation that adopts a risk management framework. It is not clear how the principles will sit with existing prescriptive confidentiality and secrecy requirements. For example, what will be the consequences for a decision maker in an agency subject to a prescriptive secrecy provision who releases information, having assessed the elements of the Five-Safes framework and the adequacy of relevant controls, if the controls assessed by him or her as adequate turn out to be ineffective? Will the relevant secrecy provision have been breached and the sanction for non-compliance apply?

7. Often the information in question is collected under compulsion of law and the corresponding confidentiality and secrecy provisions are the only protections that attach to the data. It is unclear from the Consultation, how the change in the rights and obligations will be addressed. This will remain an important issue to address especially where the data will be used for secondary purposes and/or disclosed to new users.

8. The Law Council recommends that the Bill contain clear carve out provisions for agencies and departments on the ground of confidentiality and secrecy (in addition to in other grounds).

De-identification

9. The Consultation suggests that all data provided will not include personal information, namely 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable'.[3] The intention is that any information that is personal information will be de-identified prior to such release.

10. The test of what amounts to de-identification remains a complex issue of fact and law in Australia[4] and internationally.[5] In addition to the existing guidance on de-identification noted in the Consultation, the Bill will need to articulate the requisite controls that will need to be in place to ensure effective de-identification.

---

[1] For example *Reserve Bank Act 1959* (Cth) s 79A.
[2] For example 2 years imprisonment for breach of section 79A above.
[3] *Privacy Act 1988* (Cth) s 6.
[4] See Department of Heath Enforceable Undertaking made pursuant to section 33 of the *Privacy Act 1988* (Cth) https://www.oaic.gov.au/privacy-law/enforceable-undertakings/department-of-health-enforceable-undertaking
[5] For example in *Patrick Breyer v Germany* (*Judgement*) (2016) ICJ Rep. The Court of Justice of the European Union held that in certain circumstances IP addresses will be personal data as defined. This is supported by the expanded definition of personal data under Article 4 of the European Union's *General Data Protection Regulation*, which defines personal data to mean 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

11. The Law Council recommends that the Bill contain clear provisions of accountabilities and responsibilities for effective de-identification and what remedies are to be available to affected individuals and other any parties seeking to rely on or use the information.

Accountability and liability

12. The Consultation is silent on the responsibilities that data sharers may have to each other (in addition to the affected individuals where the information is personal information). For example, what reliance can be placed on the accuracy and currency of a given data set? Will this be a matter that is contemplated by the agreements as noted in the Consultation? Will the Bill prescribe relevant terms as minimum standard or will there be a series of statutory requirements under the Bill? The issue here is that some data sets, because of the way that they are established, may have inherent inaccuracies or be incomplete in a material respect. The agencies which create and use these data sets do so with an understanding of their inherent limitations. The issue which is to be managed is how any lawful holders in due course will be able to understand the limitations, and what restrictions (if any) should be placed so that the inherent limitations in a data set do not result in misleading outputs from a subsequent recipient.

13. The Consultation is also silent as to governance surrounding the decision as to what information is suitable for release under the Bill. Who will be accountable for making the decision as to what information can be released? How will this operate alongside existing obligations, including those under the various enactments under the *Privacy Act 1988* (Cth), such as the *Australian Government Agencies Privacy Code* which came into effect on 1 July 2018?

14. In this regard, the Law Council notes that some data custodians may have an institutional tendency in favour of secrecy while others may have an institutional tendency in favour of disclosure. The Law Council understand that a key driver of the Data Commissioner is to encourage custodians with a tendency towards secrecy to be more open. However, there also should be a role in making sure that custodians with a tendency towards openness continue to implement appropriate protection frameworks.

15. The Law Council recommends that the further consultation is undertaken by the Department as to appropriate models for accountability and liability and that such further consultation considers the existing responsibilities that public sector agencies have in respect of data and privacy.

Law Institute of Victoria comments

16. The Law Institute of Victoria (**LIV**) has provided the following comments in relation to the Consultation.

17. At the outset, the LIV considers that the Issues paper for consultation (**Paper**) is currently couched in very general terms, making it difficult to provide a detailed response. The LIV notes, for example, that the Paper does not advise under what circumstances agencies are currently not sharing data due to either legal or operational constraints where they would share the data under the Bill. In addition, the LIV suggests that it is difficult to formulate a comprehensive appraisal of the Bill without a clearer understanding of what it will actually change in practice.

Purpose Test

18. The LIV is unaware of how effectively the purpose test for sharing data works in the jurisdictions which use it and is therefore unable to comment on the decision to introduce it into Commonwealth law. The LIV submits that it is unclear how the purpose test will apply to different facts and circumstances and that it appears that data custodians or Australian Data Archives (**ADAs**) will have wide discretion to apply this principle. The LIV considers that there is also the potential for the purpose test to be viewed as unmanageably wide.

Five-Safes Framework

19. The LIV considers that the Five-Safes framework will provide some assurance to agencies that their sharing of data is appropriate. The LIV submits that there is always a risk that individuals will opt for 'tick-the-box' compliance as opposed to prudent risk management and, as such, principles-based regulation is likely to be beneficial. However, the LIV is of the view that it remains unclear how the Five-Safes framework will apply to different facts and circumstances and, further, it appears that data custodians or ADAs will have wide discretion to apply this principle. The LIV also suggests that the Five-Safes framework cannot sit alone and must be assessed in relation to currently accepted information communications technology controls, standards, and frameworks.

National Data Commissioner

20. The LIV suggests that the proposed independent National Data Commissioner (**NDC**) may create confusion, as it may be unclear where the authority of the NDC concludes and where the authority of the Office of the Australian Information Commissioner (**OAIC**) commences. The LIV considers that, taking into account the state-based regulators that already exist in this space, there is currently a blend of regulators in this arena which may make it difficult for the general public (and even public servants) to know which bodies to consult.

Scope of Proposed Bill

21. The LIV points to the fact that the Commonwealth and other government agencies have, for many years, been collecting data which spans a diverse range of subject matter and is significant in quantity. The LIV suggests that when this is considered in relation to publicly available information, such as that found on social media, the capacity to draw inferences, desired or undesired, is unavoidable. The LIV proposes that it will be more beneficial for a unified strategy to be developed which seeks new means of securing Australia and its citizens in terms of introducing order and stability to the constant proliferation of information and information sharing.

Domestic and International Law

22. The LIV notes that the Paper does not provide an analysis of domestic law and relationships with the international community. The LIV considers that Australia cannot avoid the context of international law and its interplay with, and implementation into, domestic law, through, for example, mutual cooperation treaties and laws. The LIV refers to the Clarifying Lawful Overseas Use of Data Act (**the US Cloud Act**) as an example. The US Cloud Act recognises foreign law enforcement and allows the US President to sign data sharing agreements with other countries without congressional

oversight. The LIV understands that the US Cloud Act will also allow foreign law enforcement to require data on their own citizens (such as Australians) stored in the US, without obtaining a warrant providing probable cause. The LIV suggests that this must be viewed in light of Alistair McGibbon's (Head of the Australian Cyber Security Centre) recent announcement that the Australian Government will be employing the services of Microsoft Azure to store and process Australian Government information in Microsoft Cloud. The LIV contends that this example highlights the insufficient scope of the proposed Data Sharing Release Legislation. The LIV is uncertain whether Australians are aware of, or would agree to, such an arrangement. The LIV is concerned that this international arrangement entirely nullifies the assurances sought through consultation in relation to the proposed legislation.

23. The LIV suggests, further in relation to its comments above regarding the international context, that as Australian privacy law is dissimilar to any other international set of privacy laws, the introduction of international terminology such as 'controllers' and 'processors' would be beneficial. The LIV notes that there are useful parallels to be drawn when one understands these roles and accountabilities in relation to business or government processes. This is as opposed to concepts such as 'data custodian' and 'responsible user'.

Data Sharing and Analytics

24. Regarding data sharing in general, the LIV understands that there is a significant volume of Australian laws which concern data sharing and information acquisition. The LIV notes that many of these fall under the Attorney General and law enforcement and that, as a general rule, the majority of them prohibit collection or sharing of data. The LIV observes that the focus appears to be regarding the private sector and individuals, but suggests that the raft of legislation that currently governs information specifically, under telecommunications and data laws, cannot be overlooked. The LIV submits that prior to a framework such as that envisaged under the new Data Sharing and Release Legislation may be considered, it is necessary to examine the body of law that currently governs the various kinds of information that may be shared. The LIV notes that it is not simply Government information but, rather, Government information combined with all other publicly available information, resulting in big data analytics and potentially unforeseen outcomes. Whilst analytics in relation to Government purposes and services appears to be the object of the proposed legislation, the LIV considers that the impact is far-reaching.

25. The LIV proposes that the success of implementing any Data Sharing and Release Legislation is contingent on the ability of responsible organisations to classify their data. That is, identifying which laws govern what kinds of information, and require particular handling criteria in relation to that kind of information. An example is personal information under the *Privacy Act 1988* (Cth). The LIV notes that classification and handling criteria within the public sector are normally governed in relation to secrecy (on the one side, and publicly available information on the other). In the private sector, however, the LIV observes that classification focuses on the confidentiality of data. The LIV suggests that this results in a blending of the two spheres (public and private). The LIV considers that the reality is, in fact, more complex than may be apparent if the proposed legislation is limited in scope to only Commonwealth entities and Commonwealth companies.

Conclusion

26. The LIV considers that a 'big picture' analysis is required prior to the finer details of the proposed legislation being finalised. The LIV suggests that issues may arise regarding securing the data and sourcing the human resources to manage it. The LIV proposes that a less precarious method of achieving what is necessary is to commence by analysing and understanding applicable law regarding Commonwealth data and then, if necessary, providing an overarching framework to provide for sharing. Presently, the effect of the proposed legislation is that it serves as an amendment to all other information laws. The LIV observes that the scope of the proposed legislation is too broad and its definitions of concepts are too wide and vague.

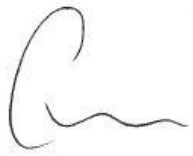
27. The LIV also suggests that useful lessons may be learned from the rollout of the privacy and data security standards for Victorian Government agencies. The LIV understands that this involves Victorian entities identifying what information they have, to allow them to know how to manage it, and to determine what may be discarded. In terms of identifying what information each agency has, the LIV notes that there are a range of technologies and software applications which may assist with this process and which include structured and unstructured information.

Thank you for the opportunity to provide these comments.

The Law Council would be pleased to elaborate on the above issues, if required.

Please contact Dr Natasha Molt, Acting Director of Policy, Policy Division (02 6246 3754 or at natasha.molt@lawcouncil.asn.au), in the first instance should you require further information or clarification.

Yours sincerely



Morry Bailes
President