THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

New Australian Government Data Sharing and Release Legislation – Issues Paper for Consultation

1 August 2018

Department of the Prime Minister and Cabinet
1 National Circuit
Barton ACT 2600

By email: datalegislation@pmc.gov.au

Contact: **David Turner**
President, NSW Young Lawyers

Irene Halforty
Vice Chair, NSW Young Lawyers Communications, Entertainment and Technology Committee

Editors: Irene Halforty, Eva Yi Lu
Contributors: Ashleigh Fehrenbach, Irene Halforty, Eva Yi Lu, Ravi Nayyar and Sophia Urlich

THE LAW SOCIETY OF NEW SOUTH WALES
young LAWYERS

The NSW Young Lawyers Communications, Entertainment and Technology Law Committee (Committee) makes the following submission in response to the New Australian Government Data Sharing and Release Legislation – Issues Paper for Consultation.

NSW Young Lawyers

NSW Young Lawyers is a division of The Law Society of New South Wales. NSW Young Lawyers supports practitioners in their professional and career development in numerous ways, including by encouraging active participation in its 15 separate committees, each dedicated to particular areas of practice. Membership is automatic for all NSW lawyers (solicitors and barristers) under 36 years and/or in their first five years of practice, as well as law students. NSW Young Lawyers currently has over 15,000 members.

The Communications, Entertainment and Technology Law Committee of NSW Young Lawyers aims to serve the interests of lawyers, law students and other members of the community concerned with areas of law relating to confidential information and privacy, information and communication technology (including technology affecting legal practice), intellectual property, advertising and consumer protection, entertainment, and the media. As innovation inevitably challenges custom, the CET Committee promotes forward thinking, particularly about the shape of the law and the legal profession as a whole.

Introduction

The Communications, Entertainment and Technology Law Committee (**Committee**) of NSW Young Lawyers welcomes the opportunity to comment on the proposed New Australian Government Data Sharing and Release Legislation.

The Committee is broadly supportive of the proposal to improve data sharing and release in the public sector. This represents a key opportunity to realise and maximise the benefits of public sector data which has the potential to improve interactions with the public, drive expenditure reductions, deliver beneficial public policy and improve efficiency.

However, the Committee cautions against any expectation that data sharing or release will provide solutions to complex social problems and submits that any benefit that may be achieved can only be achieved with a strong and consistent emphasis on data safeguards, privacy protections and public trust to avoid repeating the failures of other public sector data sharing and release initiatives.

The Committee acknowledges that the Issues Paper is the first step in the development and design of the new Data Sharing and Release Bill (**DS&R Bill**). Many of the questions in the Issues Paper are broad in scope with considerable overlap. The Committee has chosen to respond to the Issues Paper by addressing the following four overarching issues:

1. the Purpose Test;
2. privacy concerns;
3. data safeguards; and
4. the role of the National Data Commissioner.

The Committee strongly recommends further consultation opportunities on a more detailed level with both the Privacy Impact Assessment and Exposure Draft Bill processes.

Please note that the views and opinions expressed in this submission are on behalf of the Committee and its contributors and do not reflect the views or opinions of any employer or company related to the contributors.

1. The Purpose Test

The Issues Paper outlines a framework for the DS&R Bill which would enable the sharing of data by Commonwealth entities and companies where this sharing is otherwise barred or faces complex and ineffective pathways (**Framework**). This Framework comprises a 'Purpose Test' which must be satisfied for the data to be shared or released. The Committee has serious concerns about the proposed Purpose Test.

The Committee submits that the proposed Purpose Test is unacceptable due to its breadth of scope and would be an inadequate mechanism for determining whether data should be shared or released. The four purposes do not provide reasonable restrictions or protections against data sharing or release. For example, two of the purposes are to "inform government policy making" and "support the efficient delivery of government services or government operations". The Committee considers that these tests are unnecessarily broad and would enable any number of (if not most) uses of data to meet the Purpose Test. This is likely reflective of the DS&R Bill giving *carte blanche* to the relevant Commonwealth entity or company to share and release data, even if another regulatory regime bars it.

The Issues Paper also does not take into consideration the potential problematic implications for policy development or service delivery when using data in a context alien to that in which the data was originally gathered (i.e. secondary data analysis). Where the original data was collected for one purpose, the same data may not provide accurate or even useful results when analysed for a different purpose. The Committee recommends that data should be evaluated for certain criteria such as the design and methodology of data collection, accuracy, quality, period of data collection, purpose for which it was originally collected, whether the data has been manipulated and the content of the data before a decision can be made about the sharing or release of that data.

Further, in order to make a balanced decision about the sharing or release of data, the Committee recommends that the Purpose Test must be appropriately balanced with additional factors such that there are demonstrable justifications for the sharing and release of data. The Committee recommends that these should include considerations of (for example):

i. **Objectives** – A clear set of objectives (as opposed to purposes) for which the sharing or release of data is required. This should include an analysis of the likelihood of the objectives being achieved with or without the requested data, as well as the consideration of issues with secondary data analysis.
ii. **Benefits** – The expected benefits or improvements to individuals and society as a result of the sharing and release of data. This should include an assessment as to whether the likely benefits of sharing justify the overriding of the individual's privacy.

iii. **Risks** – The risks associated with the sharing or release of data, in particular the data outputs, to individuals and society, including any disproportionately negative or inequitable impact on particular individuals, groups, or sections of society.

2. Privacy Concerns

The *Privacy Act 1988* (Cth) (**Privacy Act**), including the Australian Privacy Principles (**APPs**) set out in Schedule 1 of the Privacy Act, governs the collection, handling, use and disclosure of personal information in Australia. The Privacy Act applies to all Commonwealth entities as well as many private businesses and not-for-profit organisations. On 1 July 2018, the Australian Government Agencies Privacy Code (**Code**) registered under the Privacy Act also came into effect. The Code requires Commonwealth government agencies to take practical steps to comply with the APPs to ensure a high standard of personal information management across all agencies.

The Committee is particularly concerned that the proposed Framework does not contemplate obtaining consent from individuals nor giving individuals a notification of how their personal information may be shared or released. The Framework also does not contemplate the impact of data sharing and release on individual privacy nor the preservation or protection of individual privacy. The Committee notes that the Five Safes framework contains considerations of whether the data discloses identity (Safe Data) and whether the project results are likely to disclose identity (Safe Outputs). However, the Committee submits that data safeguards are not privacy safeguards. That is, simply because the data is secure or does not reveal identity, does not necessarily mean there was no breach of privacy if the personal information was used or disclosed without notifying or obtaining consent from the subject individual.

APP 6.1 provides that if an entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless the individual has consented to the use or disclosure or if an exception applies. Although not explicitly referenced in the Issues Paper, the Committee speculates that rather than obtaining consent from the subject individual, it is likely that the proposed Framework under the DS&R Bill will seek to rely on the exception under APP 6.2(b), which permits use or disclosure of information if required or authorised by or under an Australian law.

While an individual may expect public sector entities to share their personal information where it is reasonable and necessary to provide them with the services they seek, an individual would not reasonably expect the public sector to use and disclose their information for another purpose without obtaining their consent and possibly without any obvious benefit to them or society. The Committee submits that despite any exceptions

that the DS&R Bill may create, it is incumbent upon the entity to ensure that individuals are fully aware of all uses and disclosures of their personal information (including how it will impact on the individual and the safeguards for their personal information), as well as the need to provide individuals with meaningful choice as to their participation in the collection, use and disclosure of their personal information.

The Committee further submits that sharing of health information, such as medical data uploaded by physicians to the My Health Record profiles of their patients, is arguably asynchronous with community expectations. This is in light of the sharing of users' health information without their express consent by booking application, HealthEngine [1] and the recent public outcry over the issues with the My Health Record. [2] While the HealthEngine example does not relate specifically to the sharing and release of data as between Commonwealth entities, it does demonstrate a concerning issue of Commonwealth entities' interaction with other private entities, and the real possibility of the sharing and release of data beyond the scope of the Framework.

As an example, if two Commonwealth entities share data with one another to draw insights, the resulting data set will be enriched with the data and insights of the other entity. In these circumstances, any private company that interacts, or has access to either of those entity's data sets (for example HealthEngine), will necessarily and by implication have access to data sets of the other entity, with which it has no contractual or other obligations. The Issues Paper does not adequately address issues or privacy concerns relating to the ability for private entities to access these larger or enriched government data sets without the knowledge or consent of individuals to whom that data relates.

The Committee also submits that many legislative regimes, including for example the metadata retention regime under the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**), contained express measures to limit the use of the data beyond the purposes of that Act. These additional measures, aimed at protecting individual privacy, were key to the community's support for, and acceptance of, the metadata regime. The Committee is concerned that the DS&R Bill would disturb incumbent data access and management regimes under existing legislation, and the associated privacy protections therein, and would ultimately lead to a disregard for, and frustration of these protections. The Government's experience to pass the metadata retention regime, and its proposed extension of the regime for use of metadata in civil proceedings, points to the importance that the Australian community places on their privacy, and the need to

[1] Pat McGrath, Clare Blumer and Jeremy Carter, *Medical Appointment Booking App HealthEngine Sharing Clients' Personal Information with Lawyers* (26 June 2018) Australian Broadcasting Corporation <http://www.abc.net.au/news/2018-06-25/healthengine-sharing-patients-information-with-lawyers/9894114>.
[2] Ben Grubb and Jennifer Duke, 'Breach 'Inevitable' in Digital Health Records', *Sydney Morning Herald* (online) 15 July 2018 <https://www.smh.com.au/technology/breach-inevitable-in-digital-health-records-20180715-p4zrmb.html>.

be cognizant of express measures included in other Acts that provide a greater degree of privacy protection, especially in light of the absence in Australia of any explicit legal right to privacy.

The Committee strongly recommends that the DS&R Bill make it clear that the Privacy Act and the Code will continue to apply and that the DS&R Act does not override the privacy protections contained within the Privacy Act and the Code. The Committee also strongly recommends that the DS&R Act does not override prohibitions placed on data release and sharing for privacy protection reasons such as in the TIA Act and any proposed restrictions on sharing for the My Health Record.[3]

In addition, emphasis should be placed on the Commonwealth entity or company to use, share and release only the minimum amount of data (including about as few people as possible) needed for an approved purpose under the DS&R Bill; publish privacy impact assessments; have a clear demonstrable justification for the individual data sharing arrangements; and a requirement for frequent independent audits. The Committee suggests that the Australian Privacy Commissioner be given an opportunity to play a more active and direct role in the implementation, monitoring and enforcement of the DS&R Bill and associated legislative instruments.

The Committee strongly recommends that the Department considers the legislative regimes of other jurisdictions, including specifically Part 9A of the *Privacy Act 1993* (NZ) on Information Sharing. Section 96I of the *Privacy Act 1993* (NZ) sets out the form and content of an information sharing agreement and section 96N(2) sets out a list of matters to which the relevant Minister must have regard before recommending the approval of an information sharing agreement.

The Committee also recommends that the development and consideration of the DS&R Bill should not occur in isolation to other data access regimes, such as the development of the 'Consumer Data Right' currently being overseen by the Treasury. The resulting implications to privacy are far greater when these two regimes are combined than when they are considered in isolation.

3. Data Safeguards

The Committee is particularly concerned about the paucity of detail provided in the Issues Paper on the nature and extent of security requirements applicable to the sharing and release of data under the DS&R Bill. The Committee's concerns are heightened in light of the numerous cases of cybersecurity breaches faced by

[3] Caitlyn Gribbin, *My Health Record will need a Court Order for Access, Greg Hunt Says* (1 August 2018) Australian Broadcasting Corporation <http://www.abc.net.au/news/2018-07-31/court-order-needed-for-my-health-record-greg-hunt-says/10058544>.

Commonwealth entities and companies, including the public release of sensitive information in recent years, for example:

i. The accidental publication of the phone numbers of former and serving Members of Parliament;[4]
ii. The distributed denial of service attack against the 2016 census;[5] and
iii. The publication of Australians' Medicare data which was not properly anonymised.[6]

The Issues Paper outlines a principles-based approach to data safeguards in accordance with the Five Safes framework. On one hand, the Committee favours, generally, a principles-based approach for information security (**infosec**) standards, given the diversity of systems, protocols, levels of personnel training and organisational cultures across Commonwealth entities and companies. This creates different vulnerabilities to infosec breaches and different threat environments, necessitating a flexible approach to resolving these vulnerabilities.

On the other hand, the Committee is not wholly supportive of the DS&R Bill's reliance of the Five Safes framework in this context because of the degree of uncertainty denoted by its application to developing data safeguards. This is because, unlike a rules-based approach, the Five Safes framework does not target achievement of a specific outcome, but a very broad goal. In addition, the subjectivity involved with determining the appropriateness or reasonableness of a course of action under a principles-based approach is apt to result in disagreement or dis-alignment with community expectations. Such uncertainty and subjectivity are especially undesirable when data covered by the Framework could include highly sensitive medical data, the unauthorised release of which can have severe personal ramifications for the Australians who are the subject of that data.

The Committee notes that the National Data Commissioner is expected to develop guidance for applying the Five Safes framework, the Committee recommends that the Australian Cyber Security Centre is consulted for technical advice in conjunction with the Australian Bureau of Statistics.

---

[4] Matthew Doran, *Phone Numbers of Federal MPs, Former Prime Ministers Accidentally Published Online* (20 March 2017) Australian Broadcasting Corporation <http://www.abc.net.au/news/2017-03-20/phone-numbers-of-federal-mps-former-prime-ministers-published/8370418>.
[5] Paul Smith, 'Government, IBM and ABS All Criticised as Census Failure Reports Released', *Australian Financial Review* (online) 24 November 2016 <https://www.afr.com/technology/government-ibm-and-abs-all-criticised-as-census-failure-reports-released-20161124-gswzrv>.
[6] Ariel Bogle, *Not So Anonymous: Medicare Data Can Be Used to Identify Individual Patients, Researchers Say* (18 December 2017) Australian Broadcasting Corporation <http://www.abc.net.au/news/science/2017-12-18/anonymous-medicare-data-can-identify-patients-researchers-say/9267684>.

The Issues Paper also does not refer to the Australian Signals Directorate Essential Eight mitigation strategies as a minimum standard under the Framework for sharing and release of data, irrespective of whether the recipient is a Commonwealth entity or company. The Committee notes that one of the purposes under the Purpose Test is "research and development with clear and direct public benefits", which could authorise the on-sharing of data about Australians with non-government research institutions and academics who may lack the same degree of infosec measures as Commonwealth entities and companies. The Committee is not aware of the level of compliance by Commonwealth entities (including employees, agents and contractors) with infosec best practice. The on-sharing of data increases the chances of the compromise of, for instance, highly sensitive health information. As the UK Office for National Statistics emphasises, "arguably the biggest challenge for this increased use of data [by the private and public sectors] is the need to reassure the public… that their private information won't ever be made public".[7]

The Committee strongly recommends that more specific details should be provided about the security protocols that would apply to Commonwealth entities and companies sharing data under the Framework. For instance, the Issues Paper neither defines whether anonymisation of datasets is mandatory and under what circumstances; nor does it define whether mandatory infosec standards and best practice training is required to be undertaken by the personnel of the relevant Commonwealth entity or company or any on-going training that will be provided to minimise the risk of breaches. The need for on-going training is accentuated by the fact that human risk is the most significant factor underpinning infosec breaches. The Committee is concerned that Commonwealth entities with weak infosec standards or practices could be receiving data under the Framework which is highly sensitive and from an entity with commensurately higher standards of cybersecurity. This increases the chance of a breach and would be particularly undesirable in light of the sensitivity of the data Commonwealth entities and companies hold.

The Committee considers it critical that the Commonwealth entities and companies ensure that the data will be protected at all stages of the data sharing and release arrangement, whether during the transmission, receipt of the data, and while the data remains with either party. The Committee considers that end-to-end encryption of data must be a mandatory requirement under the Framework. Particular categories of data, such as health information, should also require additional safeguards. In addition, any data shared under the Framework should be securely destroyed at the end of the data sharing and release arrangement.

---

[7] Peter Stokes, *The 'Five Safes' – Data Privacy at ONS* (27 January 2017) Office for National Statistics <https://blog.ons.gov.uk/2017/01/27/the-five-safes-data-privacy-at-ons/>.

The Committee is concerned about the Issues Paper's lack of clarity, namely in its outlining of (or lack thereof) government policy for data held by Australian law enforcement and intelligence agencies, especially that which is used by them in the detection and disruption of serious crimes and threats to national security. The Issues Paper merely reassures there will be appropriate exceptions to the application of the DS&R Bill for national security and law enforcement data. The Committee recommends that there must be a clear outline of what categories of data will be excluded from the DS&R regime under this exception. The Committee also submits that the Framework must not encompass information (potentially) critical to national security or ongoing law enforcement investigations; and any 'criminal law-enforcement agency' under section 110A of the TIA Act. This greatly reduces the chances of such sensitive information being released in an unauthorised manner or to an entity without the necessary infosec standards, protections and practices in place to safely handle that data.

4. The Role of the National Data Commissioner

The Issues Paper outlines that the National Data Commissioner (**NDC**) will have various roles, powers and responsibilities including leadership, technical direction, the provision of oversight and guidance on the implementation of the Framework and monitoring and enforcement of the provisions of the DS&R Bill and associated legislative instruments.

The Committee is supportive of these roles, powers and responsibilities, but submits that the NDC's roles, powers and responsibilities should be extended to include:

i. the provision of tailored education and training to the Commonwealth entities and companies on the Framework, in particular the operation of the Purposes Test, infosec standards, best practice and procedures, as well as privacy obligations under both the Privacy Act and the Code;
ii. monitoring the development of regulatory approaches to data sharing and release in other jurisdictions; and
iii. the assessment and determination of complaints from individuals.

The Issues Paper sets out that the DS&R Bill will give the NDC powers to penalise non-compliance, such as intentional misuse of data. The Committee considers that this should extend to the 'reckless' misuse of data. In addition, the Committee submits that the DS&R Bill should go further to incorporate a low-cost complaints and appeals mechanism in conjunction with these powers. Such a mechanism should address issues including unauthorised data sharing and release, misuse of data, improper data safeguards, improper de-identification of data as well as disputes as to whether the NDC should have authorised the sharing or release of data to an administrative tribunal. The mechanism should also include the provision of various forms of redress, including

monetary compensation, orders to restrict sharing, as well penalties, for example criminal offences for unlawful disclosure of data, where appropriate.

Concluding Comments

NSW Young Lawyers and the Committee thank you for the opportunity to make this submission. If you have any queries or require further submissions, please contact the undersigned at your convenience.

Contact:

David Turner
President
NSW Young Lawyers

Email: president@younglawyers.org.au

Alternate Contact:

Irene Halforty
Co-Vice Chair
NSW Young Lawyers Communications, Entertainment and Technology Law Committee

C/ Email: cet.chair@younglawyers.org.au