THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: HRC/BLC:GUak:1180316

3 August 2016

Ms Rosalyn Bell
Data Availability and Use
Productivity Commission
GPO Box 1428
Canberra ACT 2601

By email: data.access@pc.gov.au

Dear Ms Bell,

Productivity Commission Inquiry into Data Availability and Use

The Law Society of NSW welcomes the opportunity to provide comments on the Productivity Commission's Inquiry into Data Availability and Use ("Productivity Commission Inquiry").

We respond to the specific questions in the Issues Paper as set out below.

High value public sector data

What characteristics define high/value datasets?

The definition of 'high-value datasets' in the EU *Report on high value data sets from EU institution* (2014)[1] can be considered, for example:

- The data contributes to transparency and openness of government.
- Publication of the data is enforced by law.
- The data set has relevance or is useful to a large audience or can bring high value to the audience.
- The data has high re-use potential.

Collection and release of public sector data

What are the main factors currently stopping government agencies from making their data available?

There may be public policy reasons for not making certain data available, such as national security.

[1] https://joinup.ec.europa.eu/node/93785/

The need to protect privacy of personal information means government agencies generally are not able to share personal information, unless individual consents or exceptions apply.

Data linkage

Which rules, regulations or policies create unnecessary or excessive barriers to linking datasets?

Existing privacy laws and health information laws can be a barrier to linking different datasets that are held by different public sector agencies. However, we do not consider privacy or health information laws to create excessive barriers because agencies can ask individuals to consent to their data being linked and there are legislative frameworks for providing exceptions to these requirements. In addition, use of de-identified datasets could be used where appropriate, and where there is no need to have identifiable personal data.

High value private sector data

What private sector datasets should be considered high-value data to: public policy; researchers and academics; other private sector entities; or the broader community?

In each case cited, what characteristics define such datasets?

See our comments above regarding public sector high-value data sets.

Access to private sector data

Are there any legislative or other impediments that may be unnecessarily restricting the availability and use of private sector data? Should these impediments be reduced or removed?

The lack of quality in consents obtained in the digital world and in some cases, lack of record of what consent was captured, means businesses that purchased the right to use third party data may not have certainty and clarity over what consents were given by individuals to the data collector. This can impede the use and sharing of data in the private sector.

What are the reasonable concerns that businesses have about increasing the availability of their data?

Data is an asset for businesses. Increasing availability to business data may create concerns including:

- **Loss of competitive advantage**: Increasing availability of data can remove or reduce the competitiveness of businesses that use data (which has commercial value) to create competitive advantage.
- **Loss of potential source of income**: Increasing public access to business datasets can erode the value of commercially valuable data and in turn adversely affect businesses whose core business involves deriving an income from making data available for a price.
- **Breach of confidentiality undertakings**: Valuable data that is shared between private enterprises is often subject to confidentiality requirements.

- **Breach of trade practices laws**: Where competitively sensitive information is shared among competitors, it can result in a lessening of competitive tension and/or inference of collusion. Data access or sharing should not be implemented in a manner that can result in anti-competitive behaviour.

To what extent can voluntary data sharing arrangements — between businesses / between businesses and consumers / involving third party intermediaries — improve outcomes for the availability and use of private data? How could participation levels be increased?

Would such voluntary arrangements raise competition issues? How might this change if private sector information sharing were mandated? Is authorisation (under the Competition and Consumer Act 2010 (Cth) relevant?

Authorisation under the *Competition and Consumer Act 2010* (Cth) could be relevant if information sharing is mandated. Competition law issues may arise when competitors share information in a way that can be seen as anti-competitive behaviour, even if the intention was not to be anti-competitive.

Who should have the ownership rights to data that is generated by individuals but collected by businesses? For which data does unclear ownership inhibit its availability and use?

Businesses that collect data generally assume ownership of that data. Ownership by the business gives it the right to use collected data to create enhanced datasets that are used in business enterprises and other socially beneficial activities such as private sector research.

As between private sector contracting parties, ownership of data may be specified under contracts but this is not always the case. Mandated private sector information sharing arrangement may be difficult to implement where there is no clear data owner to be bound by and to execute the mandated arrangement.

Consumer access to, and control over, data about them

What impediments currently restrict consumers' access to and use of public and private sector data about themselves? Is there scope to streamline individuals' access to such data and, if there is, how should this be achieved?

Individuals have rights under privacy legislation to access their own personal information, but these rights are subject to exceptions. There is no private sector equivalent of legislation such as the *Government Information (Public Access) Act 2009* (NSW) and the *Freedom of Information Act 1982* (Cth). Short of issuing a subpoena (which is costly for individuals), it can be difficult for individuals to access their own information. The ability of individuals to access, amend and delete data about them held by private sector organisations and by governments is likely to continue to be a problem. This is already an issue in relation to credit reporting agencies, tenancy blacklists and private sector companies like mobile phones, ISPs, social media applications etc.

While Australian privacy laws (both in the public and private sector) generally require businesses to notify individuals about how their information is used and disclosed, there is no requirement for notification to be clear, concise and effective. Privacy notices and any consent wording often use descriptions that broadly describe a range of disclosures and recipients, the specifics of which may not be expected by an individual. This results in individuals not knowing where their information will be sent to, who holds a copy of

their personal information and where their personal information is held. This in turn impedes access by the individual to their personal information and control as to how it is used. This is particularly the case in the digital world, which impacts on vulnerable people such as children, who may give consent to their data being collected and shared online without due consideration.

At the other end of the spectrum, privacy notification on many consumer forms (eg. tenancy application forms) can be lengthy and difficult for consumers to understand. As part of a lengthy form the primary purpose of which is not for obtaining privacy consent, consumers may suffer information fatigue by the time they reach the page which has a tick-box and a lengthy privacy notification which asks them to consent to their data being used and shared. In some cases, these forms require the consumer to tick 'yes' otherwise their application will not be considered. This can also be an issue with online forms in the digital world.

Are regulatory solutions of value in giving consumers more access to and control over their own data?

Privacy laws in other jurisdictions (eg. in New Zealand) go some way to requiring intended recipients of personal information to be specified in privacy notifications. There needs to be a balance between requiring the public and private sector to make clear disclosures of who would receive an individual's personal information, and not imposing undue disclosure costs on businesses.

Privacy regulators can play a role in testing whether the content of privacy notification and consent wording is effective, adequate and accurate. We note that the Office of the Australian Information Commissioner will require adequate resourcing to carry out more investigative activities.

What role do third party intermediaries currently play in assisting consumers to access and use data about themselves? What barriers impede the availability (and take-up) of services offered by third party intermediaries?

Intermediaries can create barriers to consumers accessing and correcting their own information. We note that this has been recently reported in the media in relation to credit reporting agencies that hold incorrect credit information without the individual's knowledge, leading to individuals not being able to obtain credit.

Privacy protection

What types of data and data applications (public sector and private sector) pose the greatest concerns for privacy protection?

Personal information, including sensitive information, as currently defined in various State and Federal privacy and health information legislation, poses the greatest concern for privacy protection.

The Law Society notes that governments have a role to play in upholding societal norms on privacy protection, as acknowledged in the Issues Paper. The right to privacy is recognised as a fundamental human right in the *Universal Declaration of Human Rights*, the *International Covenant on Civil and Political Rights* ("ICCPR") and other international

instruments and treaties.[2] As Australia is a signatory to the ICCPR, the Law Society notes that state intrusions on the right to privacy must be necessary and proportionate.

Article 17 of the ICCPR states:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

We note that the Productivity Commission Inquiry will look into the benefits and costs of options for increasing availability of and improving the use of public and private sector data by individuals and organisations. In considering whether to increase the availability of such information, it is important to ensure that both Government agencies and private sector organisations are regulated in the same way, to maintain consistency and necessary safeguards for individuals.

As acknowledged in the Issues Paper, there has been a number of recent inquiries into privacy matters that are of particular relevance to the Productivity Commission Inquiry. In particular, the Australian Law Reform Commission ("ALRC") inquiry into serious invasions of privacy in the digital era made a number of relevant recommendations. The Law Society made submissions to the ALRC inquiry supporting the creation of a Commonwealth cause of action in tort for serious invasions of privacy.[3] In particular, the Law Society endorses the ALRC's recommendations in relation to the types of invasions of privacy that the new tort should cover, as set out in recommendations 5-1 and 5-2 of the ALRC's Report.[4]

Also of relevance to the Productivity Commission Inquiry is the recent NSW Parliament Standing Committee on Law and Justice inquiry into remedies for the serious invasion of privacy in NSW. The Law Society's submission to this inquiry also draws on the recommendations of the ALRC, in support of a statutory cause of action in tort for serious invasions of privacy.[5] The NSW Standing Committee has recommended that a statutory cause of action be introduced in NSW that would enable people who have suffered a serious invasion of privacy to commence civil action, adopting the model based on that recommended by the ALRC in its 2014 Report on the serious invasions of privacy in the digital era.[6]

Finally, we note that, since the ALRC's 2014 Report, the Commonwealth has legislated to allow for the collection and retention of metadata. The Law Society has made submissions expressing its concerns that, given the breadth of the scheme, and the fact that judicial warrants are not generally required, this scheme is unlikely to be compatible with Australia's obligations to protect the right to privacy under Article 17 of the ICCPR.[7] On this issue, the Law Society submissions to the ALRC and NSW inquiries into serious

---

[2] *Convention on the Rights of the Child*, opened for signature 20 December 1989, 1577 UNTS 3 (entered into force 2 September 1990) art 16; *Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families*, opened for signature 18 December 1990, 2220 UNTS 3 (entered into force 1 July 2003) art 14.

[3] See http://www.lawsociety.com.au/cs/groups/public/documents/internetpolicysubmissions/856881.pdf

[4] Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, ALRC Report 123 (2014).

[5] See http://www.lawsociety.com.au/cs/groups/public/documents/internetpolicysubmissions/1050773.pdf

[6] NSW Legislative Council Standing Committee on Law and Justice, *Remedies for the serious invasion of privacy in NSW*, March 2016.

[7] See http://www.lawsociety.com.au/cs/groups/public/documents/internetpolicysubmissions/942145.pdf

invasions of privacy have sought consideration as to how a new tort for the serious invasion of privacy might address the surveillance of individuals by police and government agencies (including in relation to the collection and retention of metadata) in a way that conforms with Australia's international human rights obligations.

What weight should be given to privacy protection relative to the benefits of greater data availability and use, particularly given the rate of change in the capabilities of technology?

Privacy protection remains important regardless of the benefit of greater data availability and use.

Are further changes to the privacy-related policy framework needed? What are these specific changes and how would they improve outcomes? Have such approaches been tried in other jurisdictions?

The current, principle based, privacy policy framework gives guidance mainly on data protection principles but does not provide a framework for balancing the benefits of data use and protection of personal privacy.

What are the benefits and costs of allowing an individual to request deletion of personal information about themselves? In what circumstances and for what types of information should this apply?

Businesses need to retain certain records for a period of time, eg. 7 years for tax reasons, or the statute of limitation period. Personal information of individuals/consumers that are kept within those records should not subject to deletion requirements.

Data security

How should the risks and consequences of public sector and private sector data breaches be assessed and managed? Is data breach notification an appropriate and sufficient response?

We refer to our comments in relation to privacy protection above.

We also support data breach notification as an appropriate response. However, the current draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill does not provide sufficient clarity on notification thresholds. We enclose a copy of the Law Society's submission on the Bill.

Thank you for the opportunity to provide comments. Questions may be directed at first instance to Anastasia Krivenkova, Principal Policy Lawyer, on 02 9926 0354 or anastasia.krivenkova@lawsociety.com.au.

Yours sincerely,

Gary Ulman
President

THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: BusLaw: GUlb1096098

4 March 2016

Commercial and Administrative Law Branch
Attorney-General's Department
3-5 National Circuit
BARTON ACT 2600

By email: privacy.consultation@ag.gov.au

Dear Sir/Madam,

Exposure draft - Privacy Amendment (Notification of Serious Data Breaches) Bill 2015

The Law Society of NSW appreciates the opportunity to comment on the Exposure Draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 ("Bill") and accompanying Mandatory Data Breach Notification Discussion Paper.

1. Overview

The Bill will implement new obligations affecting almost all corporations (over a certain size) and Commonwealth agencies in Australia. The Law Society suggests that, to minimise the regulatory burden, adequate time should be allowed for implementation, after finalisation of the text of the legislation, and promulgation of the regulations. Most importantly, the scope of the obligations must be sufficiently clear, so as not to impose an unreasonable burden on Australian businesses.

The Law Society notes that, importantly, the Bill provides a mechanism for individuals whose personal information has been compromised in a serious data breach, to take remedial steps to avoid potential adverse consequences.

The Bill should effectively balance the interests of businesses with those of affected customers. In doing so, legislators must take into account the detrimental effect that notification obligations can have on the image, brand and profits of a business.

2. Scope of obligation

Under section 26WC, entities must notify affected individuals and the Australian Information Commissioner ("AIC") if a 'serious data breach' has occurred. Section 26WB provides that a 'serious data breach' occurs when there is unauthorised access or disclosure of specific information held by specified entities, which results in a 'real risk of serious harm'.

Section 26WG attempts to define the existence of 'real risk', stating that the risk must not be 'remote'. Although this provides some assistance, it does not go far enough to delineate the scope of the obligation. In addition, no attempt is made to define the term 'serious', although the explanatory memorandum at [129] indicates that the intention is that it means 'not minor'.

Serious consideration should be given to streamlining the description of data breach related risks and their likely impacts. If a clear threshold is not established, businesses may feel obliged to notify individuals and the AIC in a wide range of scenarios, as a precaution to avoid the risk of breaching their obligations under the proposed legislation. This could lead to 'notification fatigue', a rise in compliance costs and an unanticipated increase in the administrative burden to be borne by businesses.

3. Interaction of sections 26WB(1) and 26WC

Section 26WB(1) states that, for an Australian Privacy Principles ("APP") entity that holds personal information and is required to comply with the APPs, the 'serious data breach' definitions apply. Section 26WC then provides 'if an entity is aware' (of a serious data breach) then it must notify by following the procedural requirements in section 26WC. This suggests that all entities, whether or not they are an entity that falls under section 26WB(1), need to notify. It can also be read that if the serious data breach concept does not apply, section 26WC is not triggered (therefore there is no need to notify). That is, section 26WB must be satisfied first before s26WC is triggered.

The drafting of these two sections should be amended to clarify how these two sections interact with each other.

4. Application of the State government contract exemption under the *Privacy Act 1988*

Businesses that have obligations under State government contracts need clarity as to whether serious data breaches in relation to personal information that falls under the State government contract exemption (section 7B(5)) needs to be reported. It is not clear whether, because an act or practice falls under the exemption, any serious data breach that arises from those acts or practices is also exempt from the notification requirement. The current drafting of sections 26WB and 26WC requires amendment to clarify how those sections interact when read together with section 7B(5).

If you have any questions in relation to this submission, please contact Liza Booth, Principal Policy Lawyer, by email at liza.booth@lawsociety.com.au or phone (02) 9266 0202.

Yours faithfully,

Gary Ulman
President