THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: BusLaw: GUlb1225145

16 December 2016

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

By email: natasha.molt@lawcouncil.asn.au

Dear Mr Smithers,

Productivity Commission Data Availability and Use Draft Report

I refer to the Law Council's memorandum dated 11 November 2016, seeking input in relation to the Productivity Commission's *Data Availability and Use Draft Report*.

The Law Society of NSW has provided comments in relation to a number of the draft recommendations and findings in the enclosed table.

Thank you for the opportunity to provide comments to this inquiry. I would be grateful if questions can be directed at first instance to Liza Booth, Principal Policy Lawyer, by email at liza.booth@lawsociety.com.au or phone (02) 9926 0202.

Yours sincerely,

Gary Ulman
President

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
T +61 2 9926 0333 F +61 2 9231 5809
www.lawsociety.com.au

Law Council
OF AUSTRALIA
CONSTITUENT BODY

FINDING / RECOMMENDATION	COMMENT
Addressing specific impediments to *private* sector data access	
DRAFT RECOMMENDATION 4.2 All Australian governments entering into contracts with the private sector, which involve the creation of datasets in the course of delivering public services, should assess the strategic significance and public interest value of the data prior to contracting. Where data is assessed to be valuable, governments should retain the right to access or purchase that data in machine readable form and apply any analysis that is within the public interest.	Under this recommendation, it would be reasonable to expect that contracts between government agencies and the private sector would contain provisions that stipulate data standards and/or handling practices which would facilitate access or retention of data by the agency. These requirements would impose costs which private enterprises would have to bear and (depending on the extent of the requirements) could constitute a barrier to entry and result in costs passed on to consumers. It is therefore important for any such requirements to be reasonable and be consistent, across agencies, in relation to: • what datasets government agencies consider to have strategic significance and/or public interest value; and • data standards and handling practices that agencies would require. For transparency, key institutions in the proposed data governance framework can issue standards on what datasets are considered valuable, as well as data standards and handling practices that are expected in relation to valuable datasets. It is also worth considering implementing standards and requirements that are consistent within sectors (consistent with the principles in recommendation 6.1).

FINDING / RECOMMENDATION	COMMENT
The conundrum of personal data	
DRAFT FINDING 5.1 The boundaries of personal information are constantly shifting, in response to technological advances and community expectations. The legal definition of personal information, contained in the Privacy Act 1988 (Cth), gives rise to uncertainty. This uncertainty will only increase in future, as new technology continues to emerge.	• While the draft report found that the definition of 'personal information' under the *Privacy Act 1988* gives rise to uncertainty, it has not recommended any changes to it. • We note that the Office of the Australian Information Commissioner ("OAIC") has issued guidance on what is 'personal information'. We expect that case law (such as the Grubb v Telstra case) and regulator guidance will evolve over time to clarify what 'personal information' may include. Such evolution should reflect changes in technological advances and community expectations. If there are other reasons as to why the definition gives rise to uncertainty, our view is that the Commission should consider whether there is merit in reviewing it.
DRAFT RECOMMENDATION 5.1 In conjunction with the Australian Bureau of Statistics and other agencies with data de-identification expertise, the Office of the Australian Information Commissioner should develop and publish practical guidance on best practice de-identification processes. To increase confidence in data de-identification, the Office of the Australian Information Commissioner should be afforded the power to certify, at its discretion, when entities are using best practice de-identification processes.	We agree that the OAIC is the appropriate regulator to carry out the recommended functions relating to de-identification.

FINDING / RECOMMENDATION	COMMENT
DRAFT RECOMMENDATION 5.2 The *Privacy Act 1988* (Cth) exceptions that allow access to identifiable information for the purposes of health and medical research without seeking individuals' agreement, should be expanded to apply to all research that is determined to be in the public interest. The Office of the Australian Information Commissioner should develop and publish guidance on the inputs required to establish a public interest case.	• We assume this recommendation relates to the "permitted health situations" under section 16B(2) (regarding collection for research) and 16B(3) (regarding use or disclosure for research). • Both sections 16B(2) and 16B(3) apply only where it is impracticable for the organisation to obtain the individual's consent to collection (s16B(2)(c)) and to use or disclosure (s16B(3)(c)). The draft recommendation appears to go much further by removing the need to seek individuals' agreement. We query whether the intention is to retain the impracticability criteria in sub-section (c), or to totally remove the need to seek individuals' agreement where research is determined to be in the public interest. • From a privacy protection perspective, we caution that individuals may not expect that access to their identifiable sensitive personal and health information will be permitted for all research that has a public interest element. While individuals may agree to their information being used for research that is relevant to them personally, they may not want their information to be used for any health and medical research, where the individual has no information about the nature of the research and the individuals involved in it.

FINDING / RECOMMENDATION	COMMENT
DRAFT RECOMMENDATION 5.4 To streamline approval processes for data access, the Australian Government should: • issue clear guidance to data custodians on their rights and responsibilities, ensuring that requests for data access are dealt with in a timely and efficient manner; • require that data custodians report annually on their handling of requests for data access; • prioritise funding to academic institutions that implement mutual recognition of approvals issued by accredited human research ethics committees. State and territory governments should mirror these approaches to enable use of data for jurisdictional comparisons and cross-jurisdiction research.	We support the recommendation that State and Territory governments should mirror the approval processes for data access. To increase the level of consistency across all jurisdictions in Australia, our view is that the recommendations in relation to consumer rights, regulation and enforcement should also have a nationally unified approach. These include: • The proposed 'consumer data' definition (recommendation 9.2); • The proposed Comprehensive Right (recommendation 9.2); • The proposed enforcement and oversight framework (under recommendations 9.3 and 9.5). We suggest that the Commission should consider whether other recommendations in the draft report should also be mirrored at the State and Territory level.

FINDING / RECOMMENDATION	COMMENT
Making data more useful	
DRAFT RECOMMENDATION 6.2 The private sector is likely to be best placed to determine sector-specific standards for its data sharing between firms, where required by reforms proposed under the new data Framework. In the event that voluntary approaches to determining standards and data quality do not emerge or adequately enable data access and transfer (including where sought by consumers), governments should facilitate this, when deemed to be in the public interest to do so.	We agree that the private sector is best placed to determine sector-specific standards. Any data standards and handling requirements that government agencies may impose as a result of recommendation 4.2 should take into account any sector specific standards that are self-imposed by the private sector. Otherwise, there could be a risk that government agencies may require data handling by private sector service providers in a manner that would be inconsistent with private sector specific standards. Such standards would, of course, be in addition to any requirements mandated under the *Privacy Act 1988*.

FINDING / RECOMMENDATION	COMMENT

FINDING / RECOMMENDATION	COMMENT
Valuing and pricing data	
DRAFT RECOMMENDATION 2.1 In determining datasets for public release, a central government agency with policy responsibility for data should maintain a system whereby all Australian governments' agencies, researchers and the private sector can, on an ongoing basis, nominate datasets or combinations of datasets for public release, with the initial priority being the release of high value, in-demand datasets. A list of requested datasets should be published. Decisions regarding dataset release or otherwise, and access arrangements, should be transparent. Agencies should provide explanations where priority datasets are not subsequently released on legitimate grounds. Where there are not legitimate reasons for withholding requested data, remedial action should be undertaken by the Australian Government's central data agency to assist agencies to satisfy data requests. Existing government data initiatives, such as data.gov.au, should be leveraged as part of this system.	We support having transparency in the central agency's policy and decision making.

FINDING / RECOMMENDATION	COMMENT
Fundamental reform is needed	
DRAFT RECOMMENDATION 9.1 The Australian Government should introduce a definition of consumer data that includes: • personal information, as defined in the *Privacy Act 1988* (Cth) • all files posted online by the consumer • all data derived from consumers' online transactions or Internet-connected activity • other data associated with transactions or activity that is relevant to the transfer of data to a nominated third party. Data that is transformed to a significant extent, such that it is demonstrably not able to be re-identified as being related to an individual, should not, for the purposes of defining and implementing any Comprehensive Right, be defined as consumer data. The definition of 'consumer data' should be provided as part of a new Act regarding data sharing and release (Draft Recommendation 9.11). Given the need for this definition to have broad applicability, it should also be included within the *Acts Interpretation Act 1901* (Cth). Consequential amendments to other Commonwealth legislation would ensure harmonisation across federal laws.	• Given the finding (at 5.1) that the legal definition of 'personal information' in the *Privacy Act 1988* gives rise to uncertainty, basing a new definition of consumer data on 'personal information' may create further uncertainty. • Having a definition of 'consumer data' in the *Acts Interpretation Act 1901* which is based on a definition of personal information (which is found to be unclear as to its scope) lacks the certainty which definitive interpretation legislation should provide. That is not to say the *Acts Interpretation Act 1901* is not the right place for the 'consumer information' definition to be included. • At a policy level, it needs to be determined whether 'consumer' includes businesses for the purpose of data rights. Recommendation 9.2 suggests that consumer data in the context of the Comprehensive Right relates only to individuals (and not businesses). The *Competition and Consumer Law Act 2010* has recently given some expanded protection to small businesses in recognition that small businesses should have some rights as consumers of services. In relation to the third bullet point of this recommendation, we suggest clarifying whether 'consumer' (in 'consumer data') would cover both individuals and businesses, and if so, whether it should apply to small businesses only). • 'all data derived from consumers' online transactions or Internet-connected activity' is a very wide description. It would capture raw transaction data, back-office data and meta-data that are derived or created to support transaction and processing, as well as any enhanced data that may be created through transformation and analytics (such as business intelligence

FINDING / RECOMMENDATION	COMMENT
	data). It may not be appropriate to give consumers access to, and a right to transfer, some of this data (eg. due to commercial sensitivities under contracts; appropriateness for meta-data to be transferred from one service provider to another). Unintentionally catching a wider range of data than is necessary to address data accessibility concerns could impose unwarranted costs on businesses and government agencies in making data accessible and transferable.
DRAFT RECOMMENDATION 9.2 Individuals should have a Comprehensive Right to access digitally held data about themselves. This access right would give the individual a right to: • continuing shared access with the data holder • access the data provided directly by the individual, collected in the course of other actions (and including administrative datasets), or created by others, for example through re-identification • request edits or corrections for reasons of accuracy • be informed about the intention to disclose or sell data about them to third parties • appeal automated decisions • direct data holders to copy data in machine-readable form, either to the individual or to a nominated third party. Individuals should also have the right, at any time, to opt out of a data collection process, subject to a number of exceptions. Exceptions would include data collected or used as: • a condition of continued delivery of a product or service to the individual	• This recommendation refers to 'digitally held data about themselves', ie. data about the individuals (presumably, the individuals who posted information about themselves). In contrast, in recommendation 9.1 the bullet point which broadly describes 'all files posted online by the consumer' would include data/information that is not about the person who posted the information (eg. It could be a drawing or music clip with no individuals in it, or it could be a photo of someone else). Where consumer data relates to individuals who did not post that data, it needs to be clarified which individual, the person who posted, or the person to whom the information relates, can exercise a Comprehensive Right over that data. • Clarity is needed on what would be considered 'automated decisions (such as those based on statistical profiling)' (see page 17 of the Overview document). Would an individual's credit rating be considered an automated decision? What about risk profiles which insurers generate using automated systems for applicants of insurance policies? Similar considerations apply to mortgage and personal loan processes. On page 309 of the draft report, the issue of the right of individuals to appeal automated profiling decisions that are made based on

FINDING / RECOMMENDATION	COMMENT
• necessary to satisfy legal obligations or legal claims • necessary for a specific public interest purpose (including archival) • part of a National Interest Dataset (as defined in Draft Recommendation 9.4). The right to cease collection would not give individuals the capacity to prevent use of data collected on the individual up to the point of such cessation.	inaccurate information about individuals is discussed. However it does not give any examples of what these decisions could be to help decide whether giving a blanket appeal right is the most appropriate way of addressing any identified concerns. It would be useful to understand the concern which this recommendation is intended to address, and to enable businesses to identify any practical issues that may arise from this right to appeal automated decisions. • We suggest looking to the European Union ("EU") data protection regime for guidance and comparisons in relation to the rights of individuals ('data subjects' under EU laws). • Regarding the right to be 'informed about the intention to disclose or sell data to third parties': Australian Privacy Principle ("AAP") 5 currently requires APP Entities (as defined in s 6 of the *Privacy Act 1988*) to notify individuals of any potential disclosures of personal information. We seek clarification on whether the recommendation requires businesses to take active steps to inform each individual about the intention to disclose data prior to the business actually making a disclosure (or prior to the business selling the individual's data). If businesses or agencies will need to take an active step to notify individuals before each disclosure, this will impose a huge administrative burden on businesses and agencies and create delays in businesses' processes that require disclosure to third parties. We support providing individuals with greater transparency as to the potential sale of their personal information. However, we seek further details in relation to the circumstances in which the requirement to notify would apply. There are practical ramifications for businesses even if they are not in the business of selling information. For example, a sale of business would ordinarily include a sale of customer records as a business

FINDING / RECOMMENDATION	COMMENT
	asset. Would such a sale need to be notified to the individual? • Under the *Privacy Act 1988*, there is existing protection under APP 6 which provides that certain disclosures require consent of the individual. This existing regime gives businesses and agencies the ability to make disclosures for day to day operations, but recognises that certain disclosure should have the individual's consent. It would be useful to understand what the proposed right to be informed of disclosure is seeking to address. The draft recommendation does not address what individuals do if they don't agree to the disclosure or sale of their information. If it is about the sale of personal information without the individual's consent, perhaps that could be addressed in the *Privacy Act 1988* as part of the regulations around disclosure and impose requirements for consent. If there is other information, which is not personal information, the disclosure or sale of which should be regulated, there should be a discussion and consultation in relation to what this information may be.
INFORMATION REQUEST The Commission seeks views on what methods of disclosure would be most likely to result in consumers making a meaningful choice about how their personal information is being used, and how these disclosure requirements might best be implemented.	We agree with the Commission's view that adding more text to a privacy notice or terms and conditions is not an effective method of disclosure. Mandating disclosure text is not necessarily going to help – it simply adds to the length of privacy notices. Disclosures should be clear, easy to read and not bundled with other disclosures or notices and terms and conditions. Mandating a format of disclosure (eg. using check boxes) or setting some parameters for presentation could help standardise the presentation of the disclosure. It may be worth discussing how the Facebook example that is given on page 312, figure 8.2, could be adapted offline. While this report

FINDING / RECOMMENDATION	COMMENT
	is mainly about data in a digital world, data is also used in traditional businesses that do not have a digital shopfront. A lot of day to day consent capture by traditional businesses is still made on a paper form. It seems inevitable that these would be yes/no checkboxes on a paper form. Recommendations in this report surrounding information disclosure and consent capture need to be adoptable by both online and offline businesses.
DRAFT RECOMMENDATION 9.3 The Australian Government should provide for broad oversight and complaints handling functions within a reformed framework for individual data access. Key roles should be accorded to the Australian Competition and Consumer Commission (ACCC) the Office of the Australian Information Commissioner (OAIC), and to existing industry ombudsmen. Any charging regimes, policies or practices introduced to address costs associated with data access, editing or transferability should be transparent and reasonable. The ACCC should be responsible for monitoring and assessing the reasonableness of charges applied. The ACCC, supported by state and territory Fair Trading Offices, should also educate and advise consumers on their new rights in regard to data access and collection. For specified datasets (such as in banking) the relevant ombudsman scheme would need to be expanded to deal with disputes.	Our view is that there are more synergies in giving primary responsibility for the proposed data access framework and the Comprehensive Right to the OAIC, rather than the Australian Competition and Consumer Commission ("ACCC"). The OAIC is Australia's privacy and information regulator. It currently has jurisdiction over freedom of information, privacy and government information policy. It handles complaints about privacy breaches and is expected to handle mandatory data breach notifications. It provides guidance on information and data related matters, such as information security and de-identification. We therefore consider the OAIC better placed, compared to the ACCC, to enforce and give guidance on data use matters, as well as taking a consistent approach to handling privacy and Comprehensive Right breaches, both of which involve handling of an individual's personal information. From a data availability perspective, the primary contact point should be the OAIC and we suggest that the OAIC should liaise with the ACCC on competition policy matters. The OAIC can liaise with the ACCC in the development of data related consumer right policies. Pricing issues should be regulated by the ACCC.

FINDING / RECOMMENDATION	COMMENT
INFORMATION REQUEST The Commission seeks further views on the establishment of a Parliamentary Committee to take community input on possible National Interest Datasets, to review nominations made, and make proposals for future designations. Views are also sought on practical alternatives.	The Commission may wish to consider undertaking surveys of the kind that the ACCC has conducted for the Australian Consumer Law review and ongoing stakeholder engagement. We suggest that the OAIC and/or ACCC (or perhaps jointly, as these two regulators have different policy interests) can undertake these surveys.

DRAFT RECOMMENDATION 9.11
 	
The Australian Government should introduce a *Data Sharing and Release Act* which includes the following:
• Provisions requiring government agencies to share and release data with other government agencies and requiring sharing between government agencies and other sectors.
  ○ These provisions would operate regardless of all restrictions on data sharing or release contained in other legislation, policies or guidelines.
  ○ The provisions may be waived in limited exceptional circumstances, and the Act should specify what these circumstances are.
• Strengthened provisions on access to data by individuals, including rights to access and edit data about them, a right to have data copied and transferred, and a right to request that collection cease.
 	
Provisions establishing the Framework for the governance of Comprehensive Rights of consumers, access to National Interest Datasets, approval of trusted users, and accreditation processes for Release Authorities.
	We support having a legislative framework that governs data sharing and access. Please refer to comments on the other recommendations in relation to the proposed Comprehensive Right.

FINDING / RECOMMENDATION	COMMENT
Other	
OPTIONS FOR IMPROVING THE DEFAULT CONTRACT (PAGE 314 OF THE REPORT) The commission seeks views on whether the 'take it or leave it' approach of requiring consumers to agree to privacy notices or default conditions as a pre-condition to getting services is clearly unfair. The suggestion here is that: 'If there were specific terms and conditions that were clearly unfair, there could be merit in reviewing the Australian Consumer Law framework to consider what additional consumer contract rights may be appropriate in the digital age.' The Commission stated that if there is a real issue with this, it would consider the matter further.	We agree with the Commission's comments in this section of the report. Businesses commonly use bundled consents and/or default contract conditions to capture consents from consumers. Consumers often have to agree to all of the disclosures and uses in a privacy notice or default conditions as a precondition to getting services. In a typical privacy notice, there are disclosures and uses which are required for the services that a consumer is acquiring, and secondary disclosures/uses that have nothing to do with the services being acquired (eg. marketing). A 'take it or leave it' approach means consumers have to agree to all of the disclosures and uses in the privacy notice, often without having read those notices, leaving them with no real choice to say no to marketing or other uses of their information that are not critical to the services they acquire. One may argue that consumers can decide not to agree to the default conditions, or privacy policies, and choose another service provider. The reality is that service providers often use similar approaches, leaving consumers with no real choice. We acknowledge the need to balance consumer rights and business efficiency. We note the use of multiple checkboxes to unbundle consents in the United Kingdom and suggest they are not overly onerous on consumers or businesses to put in place. Information that is presented to consumers in a way that does not allow meaningful and informed decision making can lead to poor consumer outcomes. According to the OAIC's 2013 Privacy Survey, 51% of people do not read online privacy policies because they are too long, complex or boring. (See: https://www.oaic.gov.au/engage-with-us/community-attitudes/oaic-community-attitudes-to-privacy-survey-research-report-2013#the-findings).

FINDING / RECOMMENDATION	COMMENT
	There is work to be done in making the checkboxes, as well as any documents they link to (eg. privacy policies), more readable by consumers.