office of the
privacy
commissioner

Mr Peter Harris AO
Chairman
Productivity Commission
GPO Box 1428
Canberra City ACT 2601

Our Reference:
IPC16/A000357

12 DEC 2016

By online submission to: http://www.pc.gov.au/inquiries/current/data-access/submissions

Dear Mr Harris

Submission to the Inquiry into Data Availability and Use
Response to Draft Report

I have reviewed with interest the Productivity Commission's *Inquiry into Data Availability and Use Draft Report* released on 3 November 2016, which examines the costs and benefits of increasing the availability of public and private sector data for individual and organisational use.

No discussion of data can occur without a discussion of privacy[1] and such discussions need to include a sound understanding of community expectations based upon consultations with a wide range of stakeholders.

Introduction

The rapid rise of data analytics presents new opportunities to gain insights that can inform policy development, service delivery and commercial decisions. As the Draft Report discusses, this produces tangible outcomes for the community in areas such as health, research and economic activity. A data driven economy needs privacy protections – such protections are an essential prerequisite to achieving these outcomes.

Contrary to the themes in the Draft Report, privacy protection is an enabler of effective and responsible data availability and use. Trust in the mechanisms adopted to make data available provides the confidence the community needs to support data sharing initiatives.

[1] The Federal Attorney-General's Department's submission (p8) to the Productivity Commission.

The changing technological and communication landscape creates new data breach risks and regulatory challenges. In NSW alone, over the last financial year there was a 300% increase in voluntary data breach notifications made to my Office and a 71% increase in requests for privacy advice.[2] Some of these matters related to the use of data analytics by NSW public sector agencies to facilitate improved service delivery.

It is a principle of privacy law that entities refrain from using or disclosing personal information for a purpose other than the purpose of original collection, unless lawful exemptions apply. Data analytics as typically envisaged and one suspects practised, fundamentally challenges this as personal information is used for a wide variety of secondary purposes without consent.

As privacy protection is essential to the development of a person's personality and their ability to enjoy their private and family life, responsible data access and use must start from a human rights perspective. In a nation that does not have Constitutional protection for privacy, a Bill of Rights enshrining privacy, or a common law tradition of a tort of privacy, rarely is the human rights context of privacy protection remembered.

Internationally, privacy protection is recognised as a human right and this approach is also applied in relation to trade and commerce in personal and health information. In the global knowledge economy, where Governments wish to participate for economic and productivity reasons, clear accountability and strong privacy frameworks are important from an international trade and economic perspective. The greater awareness and expectations in Europe and the USA of the necessity for the protection of personal and health information within international commerce, means that Australia needs to recognise the strategic value of clear, strong privacy frameworks and regulations, and the dangers of not doing so. This need will become more relevant and pressing as the work of the United Nation's first Special Rapporteur on the Right to Privacy brings new scrutiny and comparative analysis to bear across jurisdictions internationally.

The discussion in the Draft Report presents data as a commodity, which is not consistent with this emerging reality. The Productivity Commission's Inquiry is an opportunity to align Australia's use of data to this international context and to facilitate the benefits this alignment can return. The final Report and recommendations need a deeper understanding of the issues at stake, the risk of unintended consequences and the most constructive mechanisms to achieve the public benefit aims.

[2] See NSW Privacy Commissioner, *2015/16 Annual Report* (Office of the NSW Privacy Commissioner, 2016) 5, 10.

Support is given to the approach of 'privacy by design' to achieve increased efficiencies and data uses facilitative of the broader societal, commercial and individual benefits within a framework of privacy protections consistent with international standards.

A need for a privacy cause of action

When over 40 years ago, NSW led Australia in 1975 by introducing privacy legislation, it was a world-leader in advocating privacy protections. This provided individuals with the confidence that entities were handling personal information in accordance with community expectations. Today, this is not the case. Australia's privacy laws lag behind the protections offered by other jurisdictions, and one could say 'our competitors', in the knowledge economy. This may create barriers for Australian business.

The new European Union General Data Protection Regulation (GDPR) will come into effect on 25 May 2018. It will provide higher privacy protection standards than those proposed in the Draft Report. Amongst other obligations, entities will be required to:

- demonstrate they are applying privacy by design and by default;[3]
- undertake compulsory data protection impact assessments prior to data processing where the type of processing is likely to result in a high risk for the rights and freedoms of EU individuals; and
- implement measures to enable mandatory data breach notification to relevant authorities within 72 hours of discovering a breach. Where the breach may result in a high risk to the rights and freedoms of individuals, breach notification must be provided to those individuals affected.

Companies are increasingly heading to Europe to take advantage of higher privacy requirements to garner consumer trust in their products and services. As of 2015, Apple has invested £1.7 billion in its European call centres, Salesforce.com has opened a new French data centre to 'double down' on its European commitments, and Zettabox.com has based its entire operations in Europe to provide a 'high quality' cloud service.[4]

[3] Under the GDPR, a 'data processor' is any entity which processes data on behalf of the data controller; a 'data controller' is the person or entity which determines the purposes for which, and the manner in which, any personal data will be processed.

[4] See European Commission, *The EU Data Protection Reform and Big Data: Fact Sheet* (EU, 2016). Available at http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf

Privacy protections will not be an impediment to obtaining a competitive advantage in data driven economies. Rather, they will be a necessary entry point to do business in those countries.

As the privacy right is not part of our constitutional landscape, a comprehensive cause of action compatible with international standards, that will concurrently promote protections and effective regulation will be appropriate for the benefit of the community, and, the domestic and international organisations that operate in Australia. Such a cause of action may also facilitate a future assessment of "adequacy" when Australia may join the network of trusted jurisdictions.

A need for awareness raising

A central theme in the Draft Report is the perception that Australia's public sector culture for risk aversion is creating significant barriers to effective data sharing. The Draft Report states:

> 'While in some cases genuine legislative barriers to sharing data exist, a public sector culture that is risk-averse and creates reluctance to share or release data has been described by both members of governments and the general public as perhaps posing an even greater barrier (to data sharing) than actual legislation'.[5]

This conclusion is supported and we have found that a culture of risk aversion, rather than effectively managing risk, has a variety of causes. The consistent message from studies and research is that privacy legislation is not the barrier but territorial tensions, legacy systems, data quality as well as a lack of understanding of how privacy rights and obligations operate, frequently are described as 'privacy barriers'. This observation has been made in several submissions to the Inquiry.[6]

My engagement with stakeholders has identified a need for regulatory certainty and guidance from the relevant regulator to perform data analytics and initiate open data projects that comply with statutory requirements. Privacy regulators play a critical role in ensuring that the community is informed of their privacy rights and the corresponding obligations of organisations. The Commission's Inquiry is a good opportunity to encourage the provision of an awareness program and training, so that misapprehensions regarding privacy obligations do not remain obstacles to effective but privacy respectful data sharing.

[5] Productivity Commission, *Inquiry into Data Availability and Use: Draft Report* (Australian Government, 2016) 123.
[6] See, for example, the NSW Government's submission, the NSW Law Society and the Federal Attorney-General's Department, Submission to the Inquiry into Data Availability and Use Issues Paper (Submission 209, 2016) 1.

Similarly, the Commission's final report needs to consider proposals for awareness raising on the need for further research regarding the risks of re-identification when releasing data considered privacy preserving, appropriate processes and a plan to develop the necessary methodologies.

The definition of 'consumer data'

The Draft Report recommends the introduction of a new class of 'consumer data.' This includes personal information, files posted online by a consumer and data derived from online transactions or activity, including transactions or activity relevant for facilitating third party access. This consumer data will be afforded protections under the proposed Comprehensive Right.

The definition of consumer data does not include data that is transformed to such an extent that it is considered no longer identifiable. According to the Draft Report:

> 'the desired outcome from defining consumer data should be that if the data point was received from an individual and subsequently remains substantially unaltered such that it is able to be linked within the systems of the firm back to that individual, then it is consumer data.'[7]

I note that the majority of submissions received after the release of the draft report question the introduction of new and additional regulatory provisions. I also question the need for another definition of data relating to individuals and particularly one that only relates to individuals as consumers and in addition, a definition that is so similar to the definition of personal information within the Commonwealth *Privacy Act, 1988* that one has to ask 'Why? What is gained by this additional definition and regulation?'.[8] In the interests of 'better regulation' it needs to be remembered that reducing rather than adding regulation is what business and Governments, seek.

And to expand upon this point, privacy is a human right that should be asserted and embedded beyond consumer settings consistent with Australia's status as a signatory to these international conventions.

[7] Productivity Commission, *Inquiry into Data Availability and Use: Draft Report* (Australian Government, 2016) 303.

[8] The reference to the test of 'identifability' creates uncertainty as to what distinguishes consumer data from 'personal information'. The examples of consumer data provided in the Draft Report do not convincingly argue the case for this additional regulatory regime.

The term 'personal information' appropriately recognises that privacy protections concern attributes to the totality of one's personhood. The term 'consumer data' reduces individuals to mere transactional beings.

The Comprehensive Right

The Draft Report recommends the introduction of a Comprehensive Right, which partially replicates Articles 20 and 21 of the GDPR.

This right will facilitate access to a person's own customer data and the right to request the data custodian to provide a copy of their data in machine readable format to third parties.

This right largely replicates existing access rights provided under State and Commonwealth privacy legislation. In relation to data portability, APP 12 provides a right to access personal information and stipulates that access must be given in the form requested by the individual.[9]

The right appears to depart from existing privacy standards by facilitating third party access to customer data. Under NSW privacy legislation, third party access that is requested or authorised by an individual does not satisfy the access privacy principle and the individual can still exercise their entitlement to obtain a copy of their personal or health information directly from the data custodian.

Where facilitating third party access, the right will need to allow that access and a remaining entitlement of the individual to request additional access to their information for their own purposes.

The right also provides individuals the right to stop collection, unless an exception applies. In its current form, the exceptions to the right to stop collection appear too wide in scope. If these become part of the adopted position, they may unduly limit the right. As the Draft Report notes, the intention of the exceptions is to prevent individuals from relying on the right where collection is conducted by any public sector agency or a private sector entity collecting data on behalf of a public sector agency.[10]

If this is the case, there will be a genuine risk that agencies may over-collect data where an exception applies. Such over-collection may undermine the collection limitation principle, which is a feature of current privacy laws and which acts also as an efficiency mechanism.

[9] *Privacy Act 1988* (Cth) APP 12.4(b).

[10] Productivity Commission, *Inquiry into Data Availability and Use: Draft Report* (Australian Government, 2016) 346.

Under the Draft Report's recommended approach, individuals will be able to request that a data holder cease collecting information about them subject to a number of exemptions. A key exemption is when collection is necessary for a 'public benefit purpose.'

The Draft Report indicates that:

> 'given the (above) exceptions, individuals would not be able to opt out of collection by a public sector agency, or by a private sector entity collecting data on behalf of a public sector agency.'[11]

This signifies a departure from accepted community standards. Given that the proposed *Data Sharing and Release Act* will permit agencies to share and release customer data with other agencies, this will allow Commonwealth agencies to collect and share personally identifiable information with minimal checks and balances in place. An oversight or review mechanism is not articulated despite the implied reduction in scrutiny by elected representatives. The desirability of placing this capacity without in the hands of the Firmer limitations decided at the Parliamentary level will ensure accountability, as opposed to a lowering of privacy norms by decisions made at the level of the executive or administrative arms of government.

A model data sharing law

In NSW data sharing between agencies is enabled by the *Data Sharing (Government Sector) Act 2015*. The *Data Sharing Act* allows agencies to share government sector data, subject to the safeguards that are specifically provided in the statute. These safeguards include the continued operation of the privacy legislation in data sharing, and, the requirement to ensure that any personal or health information contained in datasets is not handled in any way otherwise than in compliance with privacy obligations.

This framework motivates public sector agencies to ensure that any information shared within the sector is de-identified. This reduces the privacy risks associated with data sharing, including over-collection and the re-identification of data.

The NSW model is simple and balances efficiency in data sharing with privacy protections. The Commission could consider recommending that the Commonwealth and the States and Territories adopt a collaborative approach towards the development of any further data sharing legislation, such as a *Data Sharing and Release Act* proposed in the draft report, using the NSW data sharing legislation.

The NSW data Sharing Act clearly provides safeguards for three categories of data:

1. Personal and health information, by linking lawfulness in data sharing and data public releases to the protections in the NSW privacy legislation,

[11] Productivity Commission, *Inquiry into Data Availability and Use: Draft Report* (Australian Government, 2016) 348.

office of the privacy commissioner

2. Commercially sensitive information protections, and

3. Information protected by State sponsored interests, by way of a linkage to the categories of information listed in the two schedules of the NSW *Government Information (Public Access) Act 2009*.

It will assist the work of the Commission towards a final report to consider these categories of information and obtain the views of stakeholders in all jurisdictions as to the need for safeguards, so that the Commission may develop an approach regarding these categories of information that is compatible with existing standards. I note especially the special place that sensitive information occupies in the NSW privacy legislation, for example, in section 19 of the NSW *Privacy and Personal Information Protection Act 1998,* which includes "an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities".

Conclusion

I and my Office are happy to assist the Commission further with any questions that may arise from this submission.

I agree to this submission being published, should the Commission decide to publish submissions. Please ensure that prior to the publication of this letter my signature is redacted from the version to the published.

Yours sincerely

[redacted]

Dr Elizabeth Coombs
A/NSW Privacy Commissioner
12/12/2016