Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.htm

19 December 2016

Productivity Commission

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

RE: Draft Report - Data Availability and Use

This submission from the Australian Privacy Foundation (The "APF") responds to the Productivity Commission Draft Report on Data Availability and Use.

General comments

In summary, we are disappointed by the recommendations in the Draft Report. The recommendations are focussed on data sharing as a "transformative" development. There are no considerations or recommendations to ensure:

1. privacy laws are adequate;
2. individuals that suffer harm due to a privacy breach have free access to justice and compensation;
3. there are adequate and tested laws in place to ensure both Government and business have both incentives and enforceable obligations to ensure individuals have control over their personal information;
4. the changes to data sharing policies and practices would be implemented by an independent body with a clear mandate to protect individuals' interests and their rights; and
5. there is a process to build trust when a lack of trust is a real concern

The Draft Report has been drafted in a vacuum, with no concern, consideration or understanding of the growing mistrust Australians have about the use of their personal information. The APF contends that any move to increased data sharing, and any attendant potential benefits, cannot proceed without obtaining the trust of individuals. The APF further submits that building trust depends upon proper protection of privacy and personal information, including strong legal and technological safeguards.

The Draft Report has given priority to the interests of business and Government at the expense of individuals. The Report's recommendation to offer an individual access to their own data has little to recommend it when they already have this right. What is not provided is any real rights and remedies consequent upon the loss of control that individuals over their own personal information with increased data sharing as envisioned in the Draft Report.

The proposed changes in the Draft Report are privacy abusive, offer real risk of harm to individuals, build mistrust, breach human rights and must be abandoned.

The consultation process

The consultation process for this Inquiry by the Productivity Commission has been poor. The consultation began with a ridiculously broad scope which then asked for submissions. The resulting very long Draft Report recommended sweeping changes with very little evidence to support those changes. There is insufficient evidence that the changes would also achieve the desired objectives (which remain unclear). It is likely that this will then cause a round of submissions where interest groups will concentrate on their particular issue. Subsequently, a Final Report will no doubt be issued with (in our opinion) little chance of implementation because the entire process was a dog's breakfast.

This is not good policy development. It is devoid of real evidence and has all the appearances of "a tick in the box" approach

Inadequate privacy laws

In our previous submission we pointed to the difficulties that arise because Australia has inadequate privacy laws. We contend that data sharing cannot even be contemplated until Australia has adequate privacy protections in place.

We believe that it is necessary to enact further privacy protections immediately which include:

1. A statutory tort for serious invasions of privacy
2. A right to compensation for data breaches and re-identification of data
3. Free or at least affordable access to justice (for example external dispute resolution) to seek a determination and compensation
4. A regulator with sufficient resources and power

If the privacy laws remain inadequate, any enhanced data sharing leaves individuals at risk of harm with no effective access to justice.

Recommendations:

1. **Enact further privacy protections including a statutory tort for serious invasions of privacy, right to compensation for data breaches and re-identification of data, access to justice**
2. **Ensure the regulator has sufficient power and resources**

Data Sharing and Release Act

While the APF acknowledges that proposals for enhanced data sharing require serious attention to legal reform, we submit that the priority must be to ensure proper protection of privacy and personal information. Privacy is the key consideration in any data sharing proposal. The APF therefore opposes the recommendation to introduce a new *Data Sharing and Release Act* (Draft Recommendation 9.11). In our view, law reform should first focus on amending existing information privacy laws in order to ensure a robust regime for the protection of personal information in the context of greater data sharing.

Recommendation:

Any data sharing proposals should be premised on amendments to the Privacy Act to ensure proper protection of personal information, and proper enforcement, in the context of greater data sharing.

Access to personal information

A key recommendation of the Draft Report is to provide greater control to individuals over their personal information in the form of a Comprehensive Right of access. The Comprehensive Right would give individuals the rights to:

- Retain the power to view information held on them, request edits and corrections and be advised of disclosure to third parties;
- Have improved rights to opt out of collection in some circumstances; and
- Have a new right to machine readable copy of their data, provided to them or a nominated third party.

The APF supports greater control over personal information and is supportive of these measures; however, they are inadequate. The measures fail to take account of the most important right individuals should have, that data should only be collected if it is reasonably necessary and there is a user-friendly opt-in process.

As it stands, every day, individuals in Australia hand over personal information in circumstances where:

- the information is requested but not required and the individual is misled about this;
- consents to use the information for a wide range of purposes are buried in "bundled consents";
- opting out is often ineffective, for example, spam email; and
- getting personal information deleted is almost impossible, for example, Facebook

Individuals already have the following rights in the Privacy Act:

1. the power to access information held, request corrections, and be advised of disclosure to third parties; and (APPs 12, 13)
2. the rights to opt-out

The additional proposed right to get machine readable data (Draft Recommendation 3.1) is an overdue reform, but is far from adequate.

Even with most of these rights in place, we already know:

- Individuals rarely access their personal information because:
    - often they do not know who holds it;
    - they cannot find who to ask as privacy disclosures are often difficult to find and read;
    - it is a bureaucratic and annoying process that can cost money; and
    - there is no confidence that they will get the actual information and there is no way to get that checked; and
- The Federal Court Appeal case in the matter Federal Court Privacy Commissioner v Telstra Corporation Limited will consider the meaning of personal information.

The current decision is that personal information is interpreted narrowly meaning that individuals have less access to their own information.

In effect, the recommendation is "privacy window dressing" and fails to offer individuals any real substantive control over their personal information. The APF therefore recommends that attention be given to ways of practically enhancing the ability of individuals to enforce rights of access to, and control of, their personal information. In short, without adequate enforcement proposals to enhance access and correction rights are meaningless.

Personal information

Draft Finding 5.1 of the draft report points out that, especially in the context of rapidly changing re-identification technologies, the 'legal definition of personal information … gives rise to uncertainty'. The current litigation before the Federal Court in *Privacy Commissioner v. Telstra Corporation Limited,* which concerns the status of IP addresses, is just one illustration of the difficulties in applying a definition based on identifiability. Accordingly, Draft Recommendation 9.1 proposes introducing a new definition of 'consumer data' in the proposed new *Data Sharing and Release Act*, which would encompass more information than falls within the definition of 'personal information' in the Privacy Act.

As explained above, the APF submits that proposals for enhanced data sharing must be premised on reforms to the Privacy Act to ensure proper protection of privacy and personal information. The APF therefore opposes the recommendations for dealing with enhanced data sharing by means of *sui generis* legislation. Similarly, the APF considers that attention should be focused on reforming the definition of 'personal information' in the Privacy Act to ensure that it is fit for purpose in the context of proposals for enhanced data sharing and rapidly developing re-identification technologies and practices. The APF therefore recommendations that serious attention be given to investigating the scope of information falling within the Privacy Act to ensure the proper protection of the individuals' privacy rights in the context of rapidly-changing technologies.

Recommendations:

The comprehensive right would need to be enhanced to include:

1. **A broad definition of personal information, which includes different types, such as financial, health, relationship etc.**
2. **Strict time frames to provide information for free (say 3 days)**
3. **Personal information is only obtained when reasonably necessary**
4. **Strict rights that individuals must opt-in for personal information to be shared overseas or used for marketing purposes**
5. **Independent audit processes to check how personal information is stored**
6. **Free access to justice for failure to provide comprehensive information on request and within time**
7. **Individual control over how information is used that is beyond the scope of what the information is given for.**
8. **Recognition that different rights may apply to different types of personal information.**

Data Linkages

The APF opposes the use of unique ID numbers for all individuals in Australia. We contend that this is a Digital Australia Card. We note that Australians comprehensively rejected an Australia Card in 1980's.

Recommendation:

There should never be a unique identifier used for each individual Australian

Statistical Linkage Keys

The government is increasingly using a Statistical Linkage Key for individuals using government services. Both health and social services use this key. The SLK is supposed to be anonymous and de-identified, but is not. We understand it is a combination of part of last name, part of first name, date of birth and gender. For example, the Department of Social Services used a Data Exchange protocol which is published at https://dex.dss.gov.au/policy-guidance/dex_data_exchange_protocols/.

The SLK contains personal information, at least partially, in the clear. It is not an encrypted key. It is purported in the DEX protocol that the use of the SLK is an effective means of de-identification. We contend that the SLK is easily re-identifiable now with current technology.

Currently, personal information is provided to the DSS from a wide range of community organisations and the DSS then turns that information into a SLK. Similarly in health, data is gathered then turned into a SLK.

The purpose of the SLK is to be used in data linkages both in research and evaluation. The problem is that the fundamental assumption underlying the data sharing (being that the SLK is anonymous) is wrong. This means that any Privacy Impact Assessment is flawed as it has not evaluated the risks; the community thinks they are protected when they aren't, and individuals are at real risk of harm when the data is re-identified.

Recommendations:

- **Personal information should only be obtained when completely necessary**
- **The Statistical Linkage Key is abandoned due to the real risk of re-identification**

Health Data

Health Data is a very complex and volatile subject and deserves specific treatment and protection.
Technologies such as eHealth and the Internet of Things (IoT) are enabling the creation and storage of vastly more personal data than ever before. Initiatives such as the Federal Government's My Health Record are collecting and aggregating large amounts of patient data, often without their explicit consent.

Initiatives such as the PM&C's (The Public Sector Data Management Project) are attempting to make sharing and linking of government managed data on individuals much easier.[1]

[1] https://www.dpmc.gov.au/public-data/public-sector-data-management-project

Advances in data de-identification and re-identification techniques, especially in the context of the availability of other data sets on individuals, mean that it is not possible to say with any degree of certainty if a particular "de-identified" data set is "safe". It should also be recognised that de-identification of personal data has the inevitable consequence of distorting that data.

We note that the newly created Australian Digital Health Agency has not developed its strategy for either eHealth or the My Health Record and we draw attention to a recent paper on this system, *My [Electronic] Health Record – Cui Bono (For Whose Benefit)?* by Danuta Mendelson and Gabrielle Wolf of Deakin University published in the Journal of Law and Medicine 24 (2016)[2], which raised some major concerns about the Federal Government's gathering and use of patient data.

We support the approach outlined in the Public Sector Data Management Project, "*A careful, staged approach to implementation is required to adequately address the different risks, governance requirements and other considerations that each type of data poses*, however what this means is unclear and raises a number of concerns and questions.

We particularly draw attention to statements such as Barrier - Challenges to data management "Social license – privacy provisions in legislation and community expectations limit the use of data."[3]In our opinion, privacy should not be seen as a "barrier" to be overcome - it is a necessary condition of use, one which should have the highest priority.

In view of all these uncertainties regarding what is possible now and what might be possible in the near future, we contend that a number of principles should be applied to personal information such as Health data sets:

1. A blanket or generic approach to the sharing or use of health data s is not appropriate
2. There needs to be a differentiation between population health data and an individual's health data, with protections applied dependent on the nature and risks associated with each type
3. The issues surrounding health data are far too complex and uncertain for an individual to give informed consent to their health data being used for secondary purposes. Any assumption that they can is simplistic and unwarranted.
4. Data sharing and use should be on a case by case basis, with an independent body reviewing and approving requests to share data. The body should comprise and reflect a range of interests including subject matter expertise, privacy interests, legal representatives and data specialists.
5. Data should only be made available for a fixed period of time after which all copies must be destroyed

Public information and non-personal information

There is enormous scope for data sharing and improving availability of data in this area. We contend that should be a major focus moving forward. When there is no personal

[2]https://www.dpmc.gov.au/sites/default/files/publications/public_sector_data_mgt_project.pdf Slide 7.

[3] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2881787

information involved there should be a move towards transparency and a rejection (as much as possible) of commercialisation that interferes with transparency.

Credit reporting

The Draft Report recommends (at Draft Recommendation 4.1) that mandatory Comprehensive Credit Reporting (CCR) be introduced if 40% of accounts do not have CCR by 30/6/17. As it is unlikely that a Final Report will be finalised by mid next year this is a ridiculous and unworkable recommendation. It is apparently an effort to scare credit providers into sharing CCR with complete disregard of serious data quality concerns. Again, this is not good policy. Mandatory CCR is not used internationally, was not recommended by the Australian Law Reform Commission and no evidence has been presented to necessitate it.

Public Sector Data

The APF contends that the government should be more transparent in many of its programs. To this end we recommend that the government makes available data sets and reports that provide measures on all large scale government initiatives. This will require the establishment, before a program is approved, of relevant measures against which the program can be measured an example, the My Health Record should be measured against the type and number of health services that have been enhanced and enabled by access to patient data. It should also include measures of the reduction in health care costs as well as systemic improvements in service delivery. At the moment the Department of Health is reporting data on measures that are irrelevant to service delivery, e.g. the number of registrations for a My Health Record and the number of Shared Health Summaries that have been uploaded during the life of the system.

The My Health Record is of particular interest because the obvious risks patenting health information needs to be balanced against the benefit obtained by patients. Without access to meaningful data, Australians are not in a position to assess the performance of government departments in the delivery of public sector services.

My Health Record has been used as an example only; there are many more public sector programs that could be reported on.

If you have any questions please do not hesitate to contact the writer.

Yours sincerely

Kat Lane, Chair
0447 620 694
Kat.Lane@privacy.org.au