Australian Government
Attorney-General's Department

Data Availability and Use
Attorney-General's Department Submission

The Attorney-General's Department (the Department) welcomes the opportunity to make a submission on the Productivity Commission's *Data Availability and Use Issues Paper* (the Issues Paper). The submission provides the Department's view on steps that can be taken to improve appropriate use and sharing with respect to Government data within Government.

Data use and sharing within Government

Government data is subject to a complex legislative and administrative regime that includes regulation of general application, such as the Privacy Act 1988 and the information security requirements of the Protective Security Policy Framework, and a plethora of subject specific regulation, including more than 500 secrecy provisions across the Commonwealth statute book.

The sharing of government data is readily permissible under this regime, both in specific circumstances and in bulk, but the complexity of the regime can lead to a perception that the law is more restrictive than it is in reality. This perception has powerful impacts on data use and sharing.

Irrespective of the legal regime that applies to specific data, agency culture has a significant impact on the use and availability of data within government. Agencies regularly point to concerns such as privacy or security, but the real issue can be a reluctance to make data available. This reluctance can be driven by a concern for how an agency's information will be used by other entities (loss of control), concerns about the cost of changing systems and processes to enable sharing of data, and concerns about exposure to criticism and/or legal risk. Public servants are primarily focussed on the actions and performance of their own agency, whereas sharing is likely to be for the purposes of other agencies. In addition, public servants have a positive obligation to control access (the need to know principle), which makes increasing accessibility counter-cultural.

From the perspective of those who own the data and consume government services, the same information might be provided by an individual to multiple separate agencies, for multiple purposes. Individuals might prefer to have the option to provide the information only once, on the basis that it can then be shared between particular agencies for specified purposes. Relevant and related information that could enable quicker and higher quality decision-making about the individual or about their community may be held by other agencies again. Citizens may be both mistrustful of government's ability to handle their data and highly critical that government does not operate in a joined up way to provide them with quality services.

Openness, capability, security and oversight

Improvements to agency data use and sharing is best realised within a framework of openness, supported by appropriate agency capability and data security arrangements, and underpinned by a robust oversight regime.

Government should be open about the practices and policies it applies to data. It should clearly articulate why it collects data and for what purposes that data is retained, used and shared. While this is particularly important for personal information covered by the Privacy Act, openness also applies to other types of data. Openness promotes community understanding and acceptance of Government's approach to data and allows for early feedback when community expectations are not being met. Openness also promotes cultural change within government agencies.

Government has always collected data. However, it is only in recent years that technology has allowed for the easy storage, retrieval and analysis of data on a mass scale. Government needs to invest in its own capability to use data for public purposes, to manage data in ways that minimise privacy risks, and to keep data secure. Not all agencies have the capability to manage data in this way. In the short term, centres of excellence within government could be highlighted and encouraged to assist a wide range of agencies to responsibly manage data in the public interest, in accordance with accepted standards and subject to appropriate oversight.

Appropriate security arrangements are essential to the management of Government data. Government holds personal information and sensitive data whose unintended release could compromise the public interest. Ensuring appropriate security arrangements are in place for Government data not only improves public trust but gives agencies greater comfort in making their data available to other agencies where this is appropriate and lawful.

Finally, robust oversight provides an avenue to address individual concerns, improve agency culture and practice and promote public trust in the uses the Government makes of data.

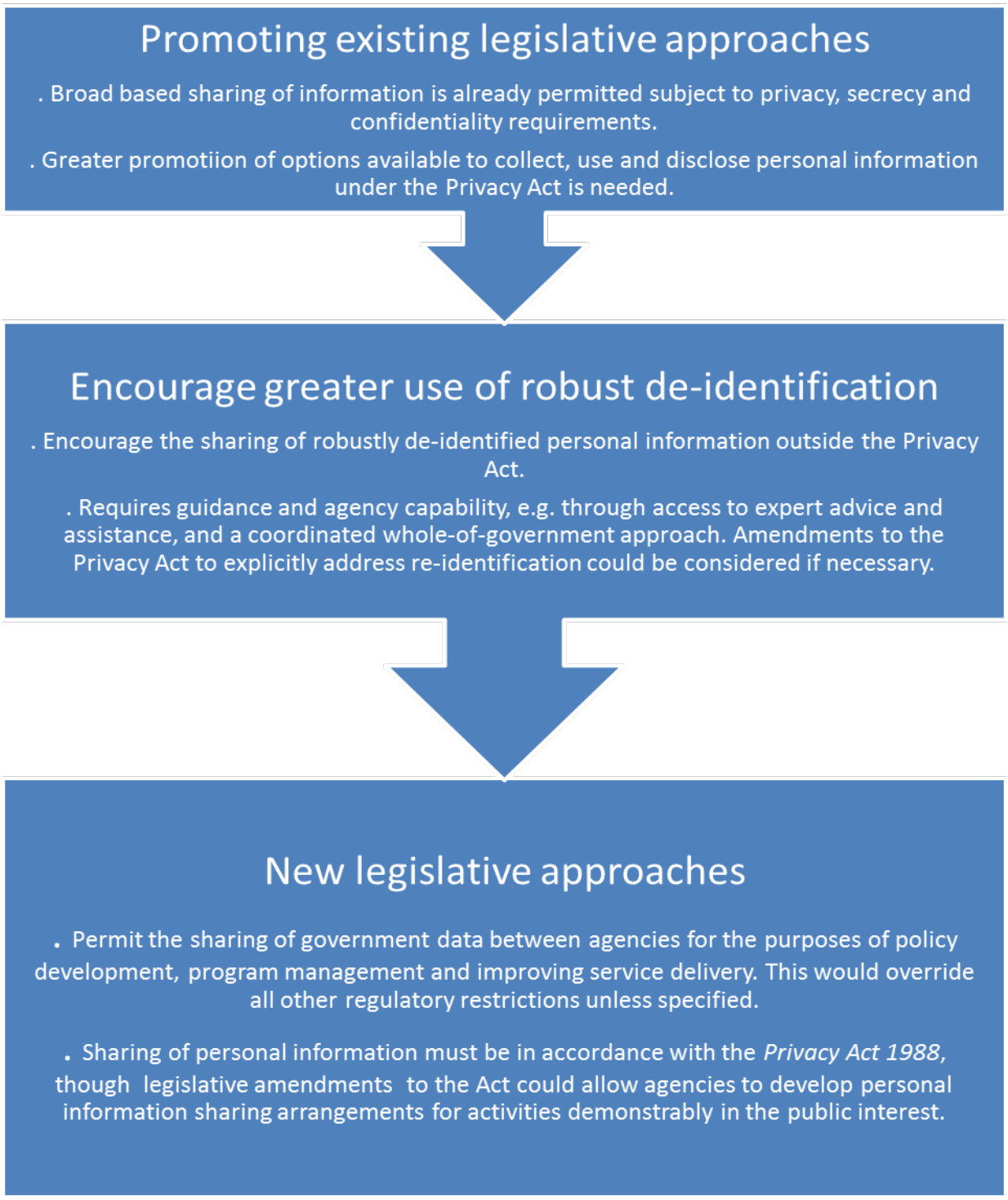
Improving data use and sharing

As noted above, the regulatory framework that applies to Government data is complex and has resulted in erroneous, but persistent, misconceptions. The department believes a number of small but significant enhancements would promote better use and sharing of data for public purposes whilst promoting openness and accountability.

The department suggests a tiered approach to improving data use and availability. Firstly, the department believes that more could be done to promote sharing within the existing legal framework, including under the Privacy Act. Secondly, the use of robust de-identification procedures should be encouraged where information cannot otherwise be shared. Finally, the legislative framework could be improved and modernised through reform. Two options would be

the introduction of stand-alone data sharing legislation and amendments to the Privacy Act to allow personal information sharing agreements between agencies.

The three tiers are intended to operate in a cascading fashion, if information can be shared at the highest level of the framework (broad based data sharing legislation or personal information sharing agreements) then you do not need to proceed to the next level and so on. The framework is summarised in the following diagram:



A: Sharing under existing legislative framework

The existing legislative framework already supports sharing of data between agencies providing there are no specific restrictions or provided that, in the case of personal information, the sharing occurs within the framework of the Privacy Act.

The Department suggests that, so long as no restrictions in other legislation apply, the Privacy Act does not block agency projects involving use or sharing of personal information. Agencies are just required to manage the project in accordance with the minimum information-handling standards contained in the APPs. For example, where no other legislative restrictions apply, an agency would not face barriers under the Privacy Act in using or sharing personal information where the agency:

- has a privacy policy that accurately and transparently reflects how the agency uses, discloses and otherwise handles personal information
- can justify a particular collection as reasonably necessary for, or directly related to, its functions or activities, or otherwise authorised by law or collected with the individual's consent
- takes reasonable steps to appropriately inform individuals how their information will be handled at the time of collection
- uses and discloses information for the purpose it was collected, for another purpose to which the individual has consented, or for one of the other range of permitted purposes in APP 6, and
- ensures it handles personal information securely, corrects defects in the information where it is aware of them, and responds to requests from individuals for access and correction of the information.

B: Encourage greater use of robust de-identification

If personal information use and sharing under the Privacy Act proves impracticable, increased agency use and sharing of robustly de-identified information may be a valid alternative. The Privacy Act does not apply to 'de-identified' personal information (which is defined with reference to the Act's definition of personal information, rather than the technical meaning of the term). De-identification is appropriate for sharing personal information within Government, and is also likely to be a useful option for cases where Government wishes to share data with trusted third parties, such as approved academic researchers, without giving access to personal information.

The Office of the Australian Information Commissioner (OAIC) and several privacy regulators and government bodies domestically and internationally have recognised the value of de-identification

and related statistical techniques as a way to mitigate the privacy risks of data sharing activities without irrevocably damaging the usefulness of the data.[1]

Implementing such an approach successfully would, however, require careful consideration of effective de-identification techniques and likely re-identification risks. Agencies would need to develop controls to deal with re-identification if it occurs. There may be merit in considering a whole-of-government approach to re-identification, to minimise risks that could arise due to agencies separately releasing de-identified data which could be cross-referenced to enable re-identification. Amendment to the APPs could be considered to provide additional clarity around re-identified personal information. These amendments, if deemed necessary, could make clear that, should re-identification occur, the data should be destroyed or managed in accordance with the APPs.

C: New Legislative Approaches

As already noted, the complexity of the current legislative regime can lead to a perception that the use and sharing of data within Government is more restricted than it is in reality. Further, this complexity does give rise to genuine barriers to use of data across Government including where secrecy provisions may operate or, in some circumstances, because of the operation of the Privacy Act.

If real or perceived barriers prove insurmountable to facilitate data sharing between agencies under current legislative settings, one option would be to introduce legislative changes to address cultural and systemic barriers to data use and sharing. In particular, legislation can promote greater sharing of information when it is drafted in permissive rather than restrictive terms – explaining when sharing is authorised rather than just when it is prohibited.

An example of legislation designed to achieve this goal is the Data Sharing (Government Sector) Act 2015 (NSW). This Act facilitates data sharing between NSW Government agencies and the

---

[1] See, e.g., OAIC, 2014, *Information Policy Agency Resource 1: De-identification of data and information*, available at https://www.oaic.gov.au/information-policy/information-policy-resources/information-policy-agency-resource-1-de-identification-of-data-and-information; and European Union Article 29 Working Party, 2014, *Opinion 05/2014 on Anonymisation Techniques*, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf; Information and Privacy Commissioner of Ontario, 2016 *De-identification Guidelines for Structured Data*, available at https://www.ipc.on.ca/images/Resources/Deidentification-Guidelines-for-Structured-Data.pdf; Information Commissioner's Office (United Kingdom), 2012, *Anonymisation: managing data protection risk code of practice*, available at https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf; National Institute of Standards and Technology (United States), 2016, *De-identification of personal information*, available at http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf; and Office of the Information Commissioner Queensland, *Dataset publication and de-identification techniques*, available at https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/dataset-publication-and-de-identification-techniques.

Data Analytics Centre within the NSW Department of Finance, Services and Innovation, while specifically providing privacy protections and linking to NSW privacy legislation. Specifically, in facilitating greater information sharing and data analysis within the NSW Government, the Act:

- includes an objects clause which recognises the importance of privacy in data sharing activities,
- sets privacy and information security standards which align with NSW privacy legislation and data security policies,
- provides a role for the NSW Privacy Commissioner, and
- contains some additional protections for categories of information deemed particularly sensitive, such as health and confidential/commercial-in-confidence information.

Any equivalent legislation at the Commonwealth level would provide an opportunity to consider what protections and oversight mechanisms should apply to data use and sharing activities. This might include allowing for data to be used and shared in cases that might otherwise be prevented by restrictions in other legislation, though noting again that in many cases it would likely be appropriate to maintain secrecy, non-disclosure and confidentiality legislative restrictions.

This model would provide a high-level commitment to data sharing. This could then be supplemented by a legislated scheme for personal information sharing agreements. The Department of the Prime Minister and Cabinet's Public Data Management Report discussed the difficulties agencies can face in establishing agreements to share data.[2] There may be value in considering whether data sharing legislation should include a formalised mechanism to support the sharing of personal information for specific activities deemed to be in the public interest, for example to facilitate service delivery improvements or for identity verification purposes. Such agreements would provide agencies with certainty about sharing data with other agencies, and could include appropriate safeguards reflecting existing privacy or other legislative controls. These safeguards could include appropriate approval and oversight mechanisms, most notably through the OAIC, and possibly also through other regulators or bodies where desirable.

An example of such agreements can be found in New Zealand. Part 9A of the Privacy Act 1993 (NZ) contains an 'approved information sharing agreement' mechanism which allows New Zealand Government agencies and other entities to share personal information for service delivery purposes. Elements of the New Zealand model that could underpin such agreements here include the focus on considering each data sharing proposal on its own merits, being transparent about data sharing activities and providing a role for the privacy regulator.[3] Other elements, such as the status of approved information sharing agreements as legislative instruments requiring Cabinet approval, would likely not be appropriate in the Australian context as they would not be flexible enough to

[2] Department of the Prime Minister and Cabinet, 2015, *Public Sector Data Management*, p 18.
[3] *Privacy Act 1993* (NZ), ss 96O, 96S.

facilitate the dating sharing activities that will occur under the Australian Government Public Data Policy Statement.

Specific Mechanisms

In cases involving particularly sensitive information, where sharing is nonetheless in the public interest, it may be appropriate to develop specific legislation governing the activity to ensure the necessary degree of transparency and to provide appropriate safeguards.

In some circumstances, it may also be appropriate to include an obligation to share information openly in legislation. This goes beyond allowing for sharing to positively requiring such sharing.

Other jurisdictions offer examples of useful, appropriately-designed data sharing provisions, such as dedicated family violence sharing legislation that permits identified agencies to share information in order to support integrated responses to high risk family violence cases. For example, the Crimes (Domestic and Personal Violence) Act 2007 (NSW) allows an agency to disclose personal information and health information about a threatened person and any person that the agency reasonably believes is a cause of the threat (the 'threatening person') to a central referral point or a local co-ordination point where an agency believes on reasonable grounds that a person is subject to a domestic violence threat. The legislation applies to any threats to the life, health or safety of a person that occur because of the commission or possible commission of a domestic violence offence.

Another example in New South Wales is Chapter 16A of the Children and Young Persons (Care and Protection) Act 1988 (NSW). This positively authorises, encourages or requires agencies that have responsibilities relating to the safety, welfare or well-being of children and young persons to provide and receive information.

The Future

The current legislative framework for managing data within Government was conceived at a time when paper was the predominant means of conducting business with Government. The opportunities to use data to improve citizens' lives were limited by the capacity of individual public servants to process and analyse huge volumes of written material. Though legislative amendments have kept pace with technological developments in some cases — the technology neutral framework enacted in the Privacy Act in 2014 being one example — it is reasonable to say additional flexibility appears to be required to ensure Government can use and share data in the way the public expects, subject to appropriate safeguards.

The capacity to use and apply data is of a different order than it was when much of the current legal framework was conceived and this capacity is only going to grow into the future. At the same time, budget-pressures, complex policy challenges, the need to improve Government services and the demand for tailored support to individuals are driving a desire by Government to improve how it

uses the data it collects. However, citizens remain concerned about the security of the information they give Government and the uses to which that information might be put. Any discussion of data cannot be divorced from a discussion of privacy.

The challenge facing Government is how it can use the data it collects in more effective ways while also maintaining privacy protections for the individual. This does not have to be a choice or a trade-off. However, arguably the current legal framework can be updated to better advance these twin objectives. To ensure acceptance of any new approaches, it will be important that they be developed in an open and consultative fashion.