Queensland Government

Minister for Innovation, Science and the Digital Economy
Minister for Small Business

GPO Box 5078 Brisbane
Queensland 4001 Australia
Telephone +61 7 3719 7110
Email innovation@ministerial.qld.gov.au
Website qld.gov.au

Ref: 01547-2016 – C16-69

06 SEP 2016

Mr Peter Harris AO, Chairman
Ms Melinda Cilento, Commissioner
Data Availability and Use Inquiry
Productivity Commission
Email: data.access@pc.gov.au

Dear Commissioners

Thank you for the opportunity to respond to the Productivity Commission's issues paper on *Data Availability and Use*. I am pleased to submit a response to the issues paper from the Queensland Government.

The Queensland Government is committed to maximising the value of data and information to our state and the national economy. As the government champion for innovation and open data, I am committed to increasing the openness and transparency of government information. I understand the contribution that increased availability of data makes to economic development, and opportunities for driving improvements in government services.

I trust the inclusion of feedback from a range of representatives across the Queensland Government, while not formal policy, will provide meaningful input into the inquiry.
I understand that the feedback received on the issues paper is a precursor to the draft report and the Queensland Government will consider providing a formal response at that stage.

If you require any further information, please contact Mr Mark Gordon, Senior Enterprise Architect, Queensland Government Chief Information Office, Department of Science, Information Technology and Innovation by email at

Yours sincerely

Leeanne Enoch MP
for Innovation, Science and the Digital Economy
and Minister for Small Business

Encl. (1)

Productivity Commission Issues Paper into Data Availability and Use

Queensland Government response

Queensland Government

Document details

Security classification	UNCLASSIFIED – Internal use only (PUBLIC following approval)					
Date of review of security classification	August 2016					
Authority	Queensland Government Chief Information Officer					
Author	Queensland Government Chief Information Office					
Documentation status		Working draft	☑	Consultation release		Final version

Contact for enquiries and proposed changes

All enquiries regarding this document should be directed in the first instance to:

Queensland Government Chief Information Office
qgcio@qgcio.qld.gov.au

Acknowledgements

This version of the *Productivity Commission Issues Paper into Data Availability and Use* was developed and updated by Queensland Government Chief Information Office.

Feedback was also received from a number of agencies, which was greatly appreciated.

Copyright

Licence

Information security

This document has been security classified using the Queensland Government Information Security Classification Framework (QGISCF) as UNCLASSIFIED – Internal use only (PUBLIC following approval) and will be managed according to the requirements of the QGISCF.

Contents

Introduction

The intent of this submission is to present a range of views from the Queensland Government sector in response to the Productivity Commission Inquiry into Data Available and Use. This submission is a collection of opinions from a diverse range of stakeholders and therefore does not represent formal Queensland Government policy.

Approach

The issues paper consists of a number of questions related to key themes. Not all the questions posed by the Commission were answered. A subset of questions to be answered were selected by a panel consisting of representatives from the Department of Communities, Child Safety and Disability Services, the Queensland Government Chief Information Office and the Department of Science, Information Technology and Innovation.

A cross-agency workshop was facilitated by the Department of Science, Information Technology and Innovation, where participants could provide their responses to the selected questions. A list of participating agencies is provided in Appendix 1, followed by a list of the workshop questions (Appendix 2).

In addition to this, the Queensland Government Privacy Commissioner has also provided a response to specific questions in relation to Privacy in a separate submission. The comments related to privacy in this submission are not those of the Privacy Commissioner.

The workshop responses have been categorised to reflect the issues paper themes, and have been contextualised to enhance the understanding of key points made.

Response

Public sector data: high value and data linkage

The identification of individual high-value public sector datasets can often be context specific for the end user of the data. There are however a number of datasets that are enablers for linkage of public sector data from multiple publishers:

- The Geocoded National Address File (G-NAF)
- Local government, suburb and locality administrative boundaries
- The Australian Statistical Geography Standard (ASGS)
- Classification reference data; e.g. ABS 1292.0 Australian and New Zealand Standard Industrial Classification (ANZSIC)

The release in February 2016 of the G-NAF and the PSMA Australia Administrative Boundaries datasets under a less restrictive licence is a significant, positive activity which will increase the ability to link data. Previous licensing restrictions, and, or costs of the G-NAF often stopped the sharing of cleansed address data which had been geocoded with latitude and longitude coordinates or a persistent address identifier.

An address with optimal data quality and verified identifiers supports the often quoted rule of data management, 'create once and share'. Geocoding the address at point of capture using the definitive 'golden source' of address data supports sharing of address data which only involve the identifiers for the majority of addresses being shared. Data preparation by publishers and ingestion by data consumers will be simplified, as only the identifiers (latitude and longitude, or the persistent address identifier) are shared, along with an indication of the accuracy or reliability of the geocoding.

It is noted however that the license type for the G-NAF dataset is not a full Creative Commons Attribution license, but is based upon the Creative Commons Attribution 4.0 International license. This might create confusion or misunderstanding as to what this valuable dataset can and cannot be used for. It is therefore suggested that an ongoing awareness campaign is initiated, possibly in conjunction with AusGOAL, local nodes of the Open Data Institute, and geospatial communities of practice as to what are the allowed uses of this data, and the dataset attribution requirements.

A trusted, open source of classification reference data is a valuable tool in defining consistent, comparable demographic groups, and then being able to link them across multiple public datasets generated by vertically siloed service systems. Historically some of the classification reference data required paid subscription licensing; e.g. International Organization for Standardization (ISO) codes. The Australian Bureau of Statistics (ABS) has for several years provided a number of open source datasets of classifications. Unfortunately, these are still mostly only available as file downloads. It is suggested that the ABS classification data should be published as datasets on data.gov.au to download from there, or accessed via an open data portal API. This will improve the adoption of this data in frontline service delivery systems which will result in consistent, comparable classifications being shared across service delivery siloes.

These measures align with the current Frictionless Data movement (frictionlessdata.io) whose aims are '...removing the friction in working with data'. They seek to remove the friction in getting, sharing and validating data which currently can be very manually intensive, and require significant time and computing resources when gathering data from multiple publishers or even from datasets from a single publisher.

Other types of high-value data are:

- Property data, including zoning plans, known environmental issues, recent and historical sales data, flood plain maps, rights and obligations.
- Transport network stop/station locations.
- Transport network routes, including current status and planned closures or maintenance
- Transport network scheduled and real-time timetables.
- Medical research data.
- Data which tracks a de-identified people across a service system, or their life stage interactions with public entities.
- Real-time environmental warning.
- Real-time localised environmental response data (where to go or not go, what help is needed where in my area).
- Awareness of people who are in situation of financial distress, have suffered the loss of a family member or partner, are currently experiencing significant health issues, or have limited resources (government welfare payment recipients). All governments want to help those who have limited resources to have a dignified life. Being able to recognise a person's circumstances and provide an appropriate service is the objective of many public services.

Suggested characteristics of high-value data are:

- The data is designed for linking with data from other publishers; e.g. community services unit record data is published for frontline services which uses ABS classifications, and can be linked to ABS Census data using an appropriate statistical geography.
- The data is licensed using a Creative Common Attribution 4.0 International license (CC BY 4.0), or in the case of machine generated data, the Creative Commons Public Domain Mark, which is also endorsed for use by government and research sectors under AusGOAL.
- Data is published for what is happening now; real-time data.
- Historical data is provided to compare the 'then' with the 'now' to identify trends.
- Data is published in bulk, and not in multiple datasets from multiple agencies for a specific topic; e.g. funded government services or procurement.
- Adoption of dataset standards such as Open Contracting Data Standard or 360Giving.
- Data quality, lineage and provenance statements are published with the data.
- Datasets are provided with 'fit for use' guidance.
- The dataset is accurate and complete (and is stated as such).
- Geospatial data which is aligned with the ANZLIC Foundation Spatial Data Framework.
- Frontline, service delivery unit record data which is geocoded according to the ABS Statistical Spatial Framework.
- Personal information of a client which is shared across the public and publicly funded service system, with approval of the client, so as to provide contextually aware services for the client. This might include data being shared across jurisdictions; e.g. Victorian public housing waiting list clients approving sharing of their Centrelink contact data with the state for notification when a publically funded residence is available.
- Datasets with a well published data quality rating; e.g. have a four or five-star rating on the 5 Star Open Data scale as proposed by Sir Tim Berners-Lee.
- A clearly identified, named individual who is the data custodian of the dataset, with contact details.

Governments of all jurisdictions are facing issues of falling revenues and rising costs. Giving citizens and businesses access to control and encouragement to share more of their data across the whole public sector will eventually lead to more self-service. The customer service improvement and cost savings can be seen in industries like banking who have embraced ever increasing levels of data sharing, where the customer is the prime source for data capture, and third party service providers analyse the data for the banks to monitor risks, or to provide insights of current or future customer needs or behaviour.

There currently is an unreported cost to government, and thereby to the taxpayer, where data is re-captured at every service system outlet when a client presents, or sometimes multiple times through the one service system.

Sharing of de-identified personal data across multiple public service systems, across multiple levels of government to create client personas and life journeys, as used in many private enterprises will benefit the community and the governments supporting them; frontline service providers will start to better understand what a client needs, why, and where or how they would like it to be provided.

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

- Multiple and inconsistent data privacy laws. Why do citizens need more than one law to protect their data rights across the one country?
- Research shows most citizens and business see different levels of government as a single, amorphous body which they expect to be sharing data. Private organisations are able to share data with other organisations when providing services, or monitoring risks, but governments often only do so when they are forced to do so via legislation. For governments to deliver services in the 21st century, they need to see themselves as the 'government sector' and not isolated eco-systems.
- Many pieces of legislation are drafted with explicit barriers to data sharing due to perceived risks, or have contradictory or overlapping data sharing restrictions. For public sector data sharing to be improved, efforts at all levels of government need to be made to significantly simplify the legislative framework with respect to privacy (Privacy Act 1988 (Cth) and/or Information Privacy Act 2009 (Qld)) as the cornerstones on which all data sharing is built upon.
- In many public bodies data sharing is formalised via a Memorandum of Understanding (MoU) agreement. This requires multiple legal departments to be engaged on projects, along with external legal counsel. These are often drafted by policy and legal teams with little or any knowledge of where the data was captured, or what is the end-to-end journey of the data across a service change. Therefore, these MoUs are often complex, difficult to understand, unrealistically constrained to where the data can come from, or be used for, and bear little relation to what data is really required. A key point going forward must be the recording of 'informed consent' for data sharing by public entities. This would simplify many MoUs, as the initial basis for many would be that personal data will only be shared for citizens who have an explicit or implied use for that information through 'informed consent'.

Public sector data: collection and release

Queensland Government agencies hold vast stores of valuable information within agency networks. The challenge in recent times has been to make this information easily available while balancing protections over that information to prevent inappropriate access. There are many barriers to more widespread information sharing, however, the majority of key issues are not technical in nature.

Many of the issues identified as barriers to information sharing are common across government agencies and organisations – indicating there is an opportunity to more holistically solve information sharing issues across government agency boundaries once for many.

Some of the difficulty in sharing comes from legislative restrictions, and particularly the varying legal and agency interpretation of legislation. It could be proposed that when seeking a legal opinion on whether legislation restricts the sharing of information we are potentially asking the wrong question. The question is often 'can we share', when it should be 'how can we share' – potentially resulting in differing legal interpretations.

It is therefore important to establish a framework which provides a level of consistency when interpreting legislative acts to ensure that the intent to share information is not diffused from the beginning.

Other key barriers identified include the lack of cohesive information architectures to provide a level of understanding and support to information sharing activities. Information architectures can provide a large degree of comfort and certainty to risk-averse information custodians about sharing information assets.

Coupled with appropriate architectures, information governance is a key part of many successful information management strategies but is often overlooked as part of the overall delivery of project outcomes. The use of open standards in some circumstances offers a clear direction as to how information can be shared in a standardised way, however they seem to be struggling for acceptance in some areas of government.

A key factor for businesses wanting to share agency information is that of 'where to go' for help and support. There are pockets of sharing excellence embedded within agencies, however without a mechanism to make these more visible agencies will potentially develop solutions that already exist elsewhere. In addition, the establishment of whole-of-government sponsors and information sharing facilitators to lead, coordinate and make information sharing activities more visible, are seen as essential to success.

Information quality seems to be considered both an enabler and a barrier to information sharing – the constant content review and feedback into an information asset of questionable quality improves the quality of that asset with the result the asset may be used more often. Conversely the perceptions around the risks of providing poor quality information can mean custodians are unwilling to release their information to a wider audience.

Custodian's also have valid concerns as to how their information will be used and interpreted, as well as how it will be combined with other information sources which fuels perceptions of risk leading into additional unwillingness to share.

There are also huge opportunities for government to use its information more efficiently and

effectively. Cross jurisdictional collaboration was seen as providing a great deal of value as individual governments did not need to solve common problems on their own – solutions could be leveraged. Additionally, a significant portion of the information managed by both local and state governments has context at a national level so being able to share more efficiently between local government, states, territories and the federal government was identified as a priority.

Education and cultural change was seen as an integral part of the change required to ensure governments are using their information to the fullest. Development of a sharing culture right through government organisations was seen as essential to improve information sharing across the sector.

Information licencing was also seen as an important part of the picture with the adoption of standards such as Creative Commons (AusGOAL in Australia) to appropriately licence information products and manage intellectual property rights to ensure information is appropriately used and referenced. Embracing open standards is a vital enabler to ensure that information is being exchanged in a standard way and that there are no technical barriers to sharing.

In addition, government agencies need to ensure the data they procure and share to third parties is under a licence (possibly an open licence) to allow the legal sharing of data with members of the public. When the government releases third party datasets that are cleansed or value added, the nested copyright should be dealt with at the procurement stage and not as an afterthought or at the release stage.

The establishment of a capability which coordinates information sharing for government was seen as mandatory, to ensure those willing to share have a standard approach to sharing activities and can do so with certainty and minimal risk. Also establishing an 'accredited user' system for key information assets would pave the way for more widespread sharing when concerns about the misuse of information are high in custodian's minds.

Much of this is driven by a need for governments and organisations through their executive to actively mitigate risk and create safe environments for custodians to share information. Custodial perception is that adverse effects of sharing are borne by the custodian rather than by the organisation as a whole. Government and organisations need to openly accept risks of sharing in order to yield the many benefits sharing brings by presenting these activities as a considered balance between outcomes and risk. This can be facilitated by presenting real and tangible benefits as part of any case for sharing to justify the decision.

Much of this work should be also be underpinned by the establishment of a ministerial sponsor to ensure that sharing activities are part of the wider government agenda and are viewed favourably amongst competing priorities.

The use of appropriate standards can be seen as an enabler as well as a barrier to information sharing. Discrepancies between a nominated standard and an information asset can be seen as a reason not to share the information, however when the appetite to share is large, then standard approaches to the way information is mapped and shared can solve problems related to different system schemas.

The use of standards for both the appropriate management of information assets as well as the sharing of information, along with the use of open standards for the exchange of information and metadata should be encouraged and promoted.

Consumer access to, and control over, data

It is generally accepted that privacy is the main factor to consider in disclosing personal information, whether it is collected by a private business or by the government. Where a service has the potential to impact on community or individual health and safety there are overriding factors which may negate the availability of personal information. In this scenario there is a risk the information may also be shared without knowledge and or consent.

To enable a customer to access and use information about themselves there are a number of points that need to be addressed. These include but are not limited to:

- the creation of the customer as an entity that is easily shared and understood and consistently described across services in both the public and private sector or service clusters
- the consistent application of rules across services holding personal information and the applicability of availability given the health and safety constraints
- a minimum acceptable threshold on the quality of the data so as to ensure that it is fit for purpose and trusted
- the provision of the information to the end user so that it is consumable and in a format that is future proofed
- a mechanism to allow the customer to update any information that is deemed inaccurate, incomplete or misleading.

Some of the impediments to the above are included below. By removing these impediments an individual's access will be streamlined.

Currently, a single point of entry that will enable a customer to access to all of their personal information across or within sectors, whether this is through a portal or service centre with a consistent user experience, does not exist. A number of channels will need to be catered for here based on the technical literacy and personal preference of the population. The jurisdiction of such a service will need to be clearly defined along with how the personal information services are linked, shared and change managed. The data relevance will be an important consideration here as the customer will only want to retrieve the information that is relevant to their interest at a point in time. An example of this is the Midata program in the UK that groups the information into sectors such as energy, finance and telecommunications. In some cases, the customer may not know who has their data after either a period of service cessation or unfamiliarity of the terms and conditions of the service. The single landing space will need to enable a customer to discover which services are associated with their unique entity. Superannuation aggregation in the financial services industry has achieved a similar outcome.

There are separate privacy acts between the state and federal governments with the potential for inconsistency and or confusion in certain scenarios. For example, where a state manages a service that may impact on a health and safety aspect of the community or individual there is the potential scenario where the federal act takes precedence thereby releasing the information and creating an undesirable and unsafe or unhealthy situation. There is no consistent provision for how the data is to be made available and in what format which may be critical to future proofing the availability and storage of the information. The total process does not seem streamlined and although there are provisions for timeframes in the responses to requests - it may be overly onerous and a factor in preventing the attempted retrieval of personal information by an individual or release managed by an organisation. Will the customer feel a sense of control over the engagement process or will the red tape and regulation overheads become too much of an engagement burden? Does a right to anonymity also weigh in to the equation?

The sharing of information between organisations in certain sectors is quite immature and this will directly impact on the ability to search for a unique individual across separate systems which are in disparate physical and logical locations. Without the capability to share an individual's details to determine the uniqueness of an entity there is no way to ensure that this same system abstracted entity exists in another organisations and to what depth. The identification of personal information relevant to a unique identity is hard to link together when these relationships are not known by either the user or the organisations. Which roles are responsible for enabling this and managing any discrepancies that may arrive?

Once the discoverability of information that is related to an individual is limited the problem is further compounded by the shortcoming of no clear mandate to adopt information sharing standards (the interoperability and metadata) across the private and public sectors. Where sensitive information is involved the customer may not be willing to provide the consent to the data sharing. Will this granular level of control be feasible from an end user perspective given that some of this information may be shared without consent due to health and safety considerations?

There are massive cultural challenges internal to an organisation to ensure the free flow of information based on a customer's consent and health and safety regulations. Typically, information is in silos within an organisation and full control is therefore maintained at the cost of the information flow. To relinquish this perceived power there is going to have to be strong strategies from the top down to change the mindset and allow information to be exchanged based on the rules of customer consent and health and safety regulations. Information interchange agreements and a classification framework will need to be in place and streamlined to help enable this mind shift.

Personal information that is managed through a service should abide by information management policies and standards such as record keeping and the rules for the creation and destruction of the unit records based on service separation (terms and conditions) and health and safety constraints. If a customer initiates service separation, then the information sharing consent rules and information clean-up will need to be managed according to the service terms and conditions and the governing regulations. Once a service is terminated there needs to be clarification on who has access to the record if it needs to be maintained, under what circumstances this is acceptable and what rules are required to govern the ongoing storage of the information. These checks and balances will need to be transparent to ensure that the information is not used for unintended purposes (for customer assurance).

There are potentially conflicting views in relation to open licensing and cost recovery. As information creation, sharing and management relies on systems, integration and intellectual property there is a case for recovering the implementation costs of these systems. The alternative view is that tax payers (citizens and business alike) are already contributing to the cost of data collection and management. While a one size fits all approach may not be achievable, appropriate data licensing and cost models need to be addressed in the information sharing, accessibility and validation stages of the project lifecycle.

A single customer view across all of the services of government (or even within a single organisation) is difficult to produce as not all the constituent services are linked, nor are the customer records within these services linked. To achieve a single client view through master data management principles and patterns, the service complexity increases along with the service costs. Common standards and data models will help to achieve this goal and will make data matching more accurate. However, specifying that these standards and data models are used and trying to retrofit them into existing systems is a challenge both to an organisation's bottom line and their cultural capabilities. It is possible to push these transformations into an integration layer which

is inherently safer than making changes at the source however this will again add an organisational cost burden. Another way of achieving a single client view is to assign a unique global identifier to a person however there is public concern around privacy and a 'Big Brother' government which is one of the perceived problems of the ill-fated 'Australia Card'.

Public concern around identity fraud is also growing which requires a strengthening in verification and standards for record security. To some extent this has been mitigated in the public sector through the adherence to data sovereignty policies and ensuring that personal (sensitive) data is kept on-shore. This may not be the case with the private sector and any data sharing and service validation links will need to be aware of these particular constraints. In any arrangement where the sharing of information breaches the terms and conditions of the service and where there are security gaps that enlarge the attack vector there is going to be public backlash and the potential for public or private sector embarrassment and a degradation in reputation. This may lead to a loss of revenue and trust which has a negative flow on effect to the objectives of each of the sectors.

An example of a privacy and security service is RealMe which is a collaboration between the Department of Internal Affairs and New Zealand Post that allows the customer to prove who they are online and to log into New Zealand sites and services. This is achieved through providing an easy and secure way for customers to manage their online identity as the source of truth for both the public and private sectors. This services should be looked at in the context of providing online verification and a security framework for both the public and private sector services.

To remove any of the impediments that have been listed so far there is a need for dedicated funding to ensure that the problems are adequately addressed. As it stands there is no clear funding source or initiative that has been devised to accommodate both public and private sector personal information accessibility. Further to this there will be a need to educate the community and public and private sector participants on the proposed delivery model and to assist organisations in adopting the standards and policies. As all organisations harbour technical debt and system specific constraints there are additional costs to make enhancements and train staff. These will need to be factored in when on boarding services that allow customers to access information about themselves.

Privacy

Queensland has enacted several pieces of legislation to address privacy and information access concerns. Key pieces include the *Information Privacy Act 2009* (Qld) and the *Right to Information Act 2009* (Qld). This legislation is supported by the *Information Privacy Regulation 2009* (Qld) and the *Right to Information Regulation 2009* (Qld). Given the influence of technology on data and data applications, there is growing concerns for privacy protection. Sensitive information should be highly protected given the nature of its contents - however, there should be a wider range of exemptions that support greater data availability and use where appropriate.

Privacy in the age of technology is quickly becoming a paradox. If data is not managed appropriately, there are serious consequences to not only individuals, but also organisations, government agencies and the wider community. The privacy of individuals can be breached and genuine safety concerns that can arise. Given the rate of change in technology, the imbalance between maximising protection of individual's privacy and providing greater data availability and use has progressed. Organisations and government agencies have taken the lead on privacy and have become more accountable for their actions[1]. This has led to a culture of risk aversion associated with overprotecting privacy and restricting data availability and sharing, internally and externally between entities[2]. However, the cost of over-protecting privacy is that there is limited personalised experience for participants.

While the benefits of greater data availability and use are extensive, privacy protection is also important for instilling trust and confidence within Australia. To mitigate any imbalance, we must explore the parameters of individual consent. Not everyone that interacts with the government wants to be identified. The individual ought to maintain some control over their privacy and this should be balanced with what is in the best interests of the common good. The right to withhold information or to delete existing data should be balanced with an 'opt-out' system instead of the current 'opt-in' system.

Rapid technological advances and changing public expectations, highlight the importance of coordinating data availability and use across jurisdictions. Queensland Government currently collects and shares data between several jurisdictions. All Queensland agencies adhere to privacy regulations; however, some agencies also have additional agency specific legislation to ensure maximum privacy protection when managing sensitive information. This individualistic culture can create concerns when coordinating data sharing across jurisdictions. Currently, there is no consistent approach to interpreting and applying privacy relevant legislation. Barriers to data availability are increasing as agencies conflict over interpretation of sections, definitions and its applicability to other agencies. To mitigate these concerns, memorandums of understanding are entered into by agencies to encourage greater data availability for specific and permitted purposes while ensuring privacy is protected. However, this is only a temporary solution to a growing problem.

There appears to be no consistent structure to data collection. Collection of data should promote privacy protection to enable successful data sharing between jurisdictions. Processes need to be

[1] http://www.ey.com/Publication/vwLUAssets/EY_-_Privacy_trends_2014:_Privacy_protection_in_the_age_of_technology/$FILE/EY-Insights-on-GRC-Privacy-trends-2014.pdf

[2] http://www.ey.com/Publication/vwLUAssets/EY_-_Privacy_trends_2014:_Privacy_protection_in_the_age_of_technology/$FILE/EY-Insights-on-GRC-Privacy-trends-2014.pdf

standardised across Australia. Information should not be shared in isolation; it must have a legitimate purpose and there should be a strong focus on the best outcome as opposed to a restrictive privacy protection approach.

Privacy regulations, including policies and legislation, need to be reviewed and amended regularly to keep up with advancing technology and the potential threats to privacy and data availability. It is time for regulatory bodies to reach consensus on facilitating the balance between privacy and data availability. The New South Wales and Victorian governments have taken steps to improve privacy protection and legislation to coordinate across different jurisdictions. The New South Wales government established a whole-of-government Data Analytics Centre to advise on best practice in regards to collecting, storing and sharing data and the subsequent privacy measures[3]. The New South Wales government also introduced the *Data Sharing (Government Sector) Act 2015* (NSW). The objectives of the Act are to:

- 'enable government sector agencies to agree to share government sector data with the DAC or other government sector agencies for certain purposes,
- enable the Minister for Innovation and Better Regulation to give directions in certain circumstances to require government sector agencies to share government sector data with the DAC,
- enable the Minister for Innovation and Better Regulation to obtain information for the DAC from government sector agencies about the kinds of data sets that they control, and
- specify safeguards (including in relation to the collection, use, disclosure, protection, keeping, retention or disposal of health information or personal information of individuals) to be complied with by the DAC and other government sector agencies in connection with data sharing under the proposed Act'[4].

This piece of legislation has only just recently been enacted, therefore, it is difficult to ascertain its success in promoting the sharing of data across jurisdictions[5]. The legislation ensures privacy is protected as it excludes the sharing of personal data and any data identified in the *Government Information (Public Access) Act 2009* (NSW). Victoria have taken a similar approach to balancing the protection of privacy and enhancing data availability and sharing[6].

The Information Technology Strategy for the Victorian Government outlines plans to establish a 'data agency' to improve the sharing of data between government agencies and ensuring privacy protection[7]. It will also aim to facilitate risk management and privacy concerns that act as a barrier to data sharing[8]. As individual States and Territories implement measures to address the growing imbalance between protecting privacy and improving data availability and use, it is imperative that a consistent approach be adopted. One option is to collaborate with States and Territories to either introduce an overarching piece of Commonwealth legislation or simply amend the *Privacy Act 1988* (Cth). This will ensure consistent coordination of collecting, storing and sharing data across jurisdictions while promoting and protecting privacy. This piece of legislation will need to be adopted by all Australian States and Territories and be consistently applied across all jurisdictions.

[3] https://www.finance.nsw.gov.au/nsw-data-analytics-centre

[4] https://www.finance.nsw.gov.au/ict/priorities/nsw-data-analytics-centre/data-sharing-legislation

[5] http://www.computerworld.com.au/article/589749/focus-data-update-nsw-ict-strategy/

[6] http://www.computerworld.com.au/article/599731/victoria-launch-data-agency/

[7] http://www.computerworld.com.au/article/599731/victoria-launch-data-agency/

[8] http://www.enterprisesolutions.vic.gov.au/wp-content/uploads/2016/05/Information-Technology-Strategy-for-the-Victorian-Government-2016-to-2020.pdf

Given the risk aversion associated with data sharing across jurisdictions and protecting privacy, a mechanism to deal with privacy breaches should be adopted. This mechanism should apply the same way as any overarching legislation; consistently adopted and applied by all Australian jurisdictions.

Political champions can also lead the way for coordinating cross-jurisdictional information sharing. Currently, there appears to be no compulsion to release information and a political champion could drive change to minimise the threats of privacy breaches. This approach needs to be standardised and a framework approach adopted. Canada appears to have found the balance between protecting privacy and facilitating greater data availability across jurisdictions. For example, the regulatory authorities in Canada 'expressly require organisations to appoint an individual responsible for compliance with the obligations under the respective statutes'[9]. This responsibility is echoed in the European Union, with the creation of European Data Protection Supervisors (EDPS). These champions help to identify privacy concerns and coordinate resolving any potential breaches. The Australian Government Office of the Australian Information Officer provides a 'guide to handling personal information security breaches'[10]. However, there is no mandated approached to resolving and learning from privacy breaches.

Other restrictions

The cost of sharing data – Cost has been identified as a significant barrier for custodians who generally are only funded to manage their information to support specific business outcomes and services.

What is required is a total cost model which can adequately justify the extra expense of sharing government information in the public good. Support of such a model by executive government level could have the effect of enabling custodians to more proactively share information.

Releasing data is resource intensive as it adds cost to existing services through identifying, cleansing, standardising, filtering, proofing and approval for release – which almost always requires additional staff and processes. In addition, any interpretation of the data as a 'value add' enhances and improves service delivery, but again costs custodians.

The costs associated with not sharing government information has not been quantified and highlights such issues as:

- each agency collects their own similar data – this could be done once for many agencies as customers repeatedly provide the same data to multiple agencies
- specific data may be inconsistent across agencies, or out-of-date in one agency
- insufficient data sharing results in limited services to customers and the inability to provide enhanced services
- knock on benefits to customers from improved sharing are simply not realised.

Such a total cost model would be able to highlight the not insignificant savings as there would be no need to collect information multiple times, customers would not need to provide their information

[9] https://www.dlapiperdataprotection.com/#handbook/data-protection-officers-section/c1_AU/c2_CA

[10] https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches

multiple times, information would be validated at source (avoiding costly remediation) and information updates could be shared across agencies. In addition, there are also those costs in managing the access and distribution of information which would be avoided by the custodial agency.

The application of standards to data for release – Data and information release is facilitated more quickly and with less risk (to both the supplier and consumer) if standards are applied to the data before release. This also results in improved contextual understanding by the consumer which should be reflected in any decision making the data is being used for.

Timeliness is also an important issue particularly when there is an imperative (e.g. emergency management) when data is needed quickly to solve problems. Government should be sharing before it's needed, as this gives consumers of the information time to appropriately assimilate the information into systems, the ability to be able to comprehensively observe and deal with restrictions on use, and to also seek feedback on quality as part of continuous improvement activities.

In addition, the sharing of basic information between agencies assists in performance of duties, and good decisions can drive better social outcomes due to additional information being available. For example, child safety, education, police (address information, child safety, location specific events/plans), health (patient information).

Other restrictions to the sharing of data – The organisational 'culture' of information sharing is a dimension which must be addressed in order to achieve sustainable information sharing outcomes. Perceptions of data ownership can mean that there is some confusion as to who is best placed to take responsibility for sharing government information – whether it be agency or whole-of-government. This confusion can be magnified also by differing interpretations of legislation with the default position being often not to share – as this appears to have the lowest risk. However, it is only part of the picture. It is important to understand that not sharing information can increase risk to the government as a whole even if it does lower the immediate agency risk – child protection is one notable example.

The 'over-filtering' of data can also be a barrier in that information is generalised to a point where it's of limited use to a consumer. As mentioned in other sections of this paper – the release of information should be done through an informed risk based decision making process that considers both the risks of release and the benefits of release for the greater public good.

It can also be difficult for agencies to determine what data to proactively share – that is what is in demand and what is less useful. This would assist agencies in prioritising effort onto that data which is in need. Establishing a request service where consumers could place requests for certain types of information and in what form, would help agencies determine the priority for release. The requests could also be categorised to allow for data which contains multiple subject types to appear in multiple categories.

In addition, a mediation process to determine sharing outcomes where there is a difference of opinion between the custodian and the government organisation will assist in improving sharing outcomes.

The ongoing development of Australian Legislation for Disclosure of Private Information along the successful lines of national privacy legislation should be promoted. This would clearly identify and authorise the release of private information. The national privacy legislation has been very successful – a similar legislation for release of information that interlocks with the privacy legislation would deliver certainty and encouragement for sharing of information.

There is an opportunity to acknowledge that much personal data is now collated through the various internet/mobile applications. This has the inference that some of the restrictions related to data sharing between government agencies does not add protection to some personal information and has the additional effect of stopping agencies from providing effective services.

This can be potentially mitigated by the establishment of a series of scenarios where the benefits of sharing personal or restricted information outweighs the risk of not sharing the information e.g. health emergency (such as a heart attack in another state – gaining access to a person's medical history such as allergies and medications) or terrorist event (such as gaining access to phones in a specific GPS location to send messages). This information is provided for a limited time only and agreements in place to remove after the event.

Other restrictive issues and solutions include:

- provide greater awareness of AusGOAL to provide support and guidance to government and related sectors to facilitate open access to publicly funded information
- standardised metadata definitions would allow greater sharing and consistency of data and encourage the collection and sharing of high value data
  establish a unique identifier (e.g. number) for each individual/organisation that can be used to collate data without identifying the individual.

Security

Data security measures and their interaction with the Privacy Act – The privacy principles require agencies to ensure personal information is protected against loss, unauthorised access/use/modification/disclosure or any other misuse. Security safeguards must be adequate to provide the level of protection that can reasonably be expected for that class of information.

The Privacy Act is not the only challenge to the sharing of information. Other legislation places significant restriction on information movement and often in a less user/subject centric manner. Health, Child safety, Law enforcement, community protection legislation all have specific constraints beyond base security concerns.

The Privacy Act/s, beyond the general concepts directly related to security of information, contain/s the following restrictions on information sharing (though they are not specifically a security issue):

- use private information without first checking it is correct and up to date
- use or give out more private information than needed to achieve the task for which is was collected
- use private information for anything other purpose than we collect it for (unless required by law)
- share private information with areas outside of the government area who collected it (unless required by law)
- send private information outside Australia (except in specific situations as allowed under Section 33).

How should the risks and consequences of public sector and private sector data breaches be assessed and managed?

While sharing of sensitive information makes maintaining information security and assurance more complex, to date major data breaches have generally not been the result of deliberate business led information sharing efforts.

Several organisations responsible for breaches to customer information have featured prominently in the media. As such, this is question has less to do with information sharing and more to do with what constitutions appropriate care of information. Appropriate care of information can then be applied to shared and non-shared information similarly.

In the context of information security, enabling information sharing requires:

- transparency of obligations and expectations
- contractual mechanism commensurate with risk to sharing organisation and though at risk from compromise to the information (including confidentiality, integrity and availability)
- means of gaining and maintaining assurance of equivalent or better care of information where it is shared.

Is data breach notification an appropriate and sufficient response?

Data breach notification has growing support domestically and internationally as a means of empowering victims to make informed choices knowing their data has been compromised, and as a means of incentivising better practices in the organisations that were responsible for protecting information.

A balance question of greater good with respect to timeliness and nature of notification is complex requiring detailed consideration before any codification of obligations.

Data breach notification obligations provide visibility as to the magnitude of the problem and help inform debate on the sufficiency of controls applied in managing information (protecting, detecting and responding). Notification obligations by themselves would not automatically constitute a sufficient response to data breach and the related goal of reducing the impact of future attempted/actual data breach activities.

Appendices

Appendix 1: Participating organisations

- Department of Agriculture and Fisheries
- Department of Communities, Child Safety and Disability Services
- Department of Education and Training
- Department of Health
- Department of Housing and Public Works
- Department of Justice and Attorney-General
- Department of Natural Resources and Mines
- Department of Science, Information Technology and Innovation
- Department of State Development
- Department of Transport and Mains Roads
- Department of Treasury
- Office of the Information Commissioner
- Public Safety Business Agency
- Queensland Government Chief Information Office
- Queensland Treasury
- Inspector-General Emergency Management
- Queensland Fire and Emergency Services
- Queensland Police Service

Appendix 2: Workshop questions

Questions on high value public sector data and data linkage:

What is high-value public sector data? What characteristics define high-value datasets?

What benefits would the community derive from increasing the availability and use of public sector data?

Which datasets, if linked or coordinated across public sector agencies, would be of high value to the community, and how would they be used?

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

Questions on public sector data: collection and release:

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

How could governments use their own data collections more efficiently and effectively?

Should the collection, sharing and release of public sector data be standardised? What would be the benefits and costs of standardising? What would standards that are 'fit for purpose' look like?

Questions on consumer access to, and control over, data:

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?

Questions on privacy:

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

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?

How could coordination across the different jurisdictions in regard to privacy protection and legislation be improved?

Questions on other restrictions:

Having regard to current legislation and practice, are further protocols or other measures required to facilitate the disclosure and use of data about individuals while protecting privacy interests?

What form should any such protocols or other measures take?

Questions on data security:

How do data security measures interact with the Privacy Act?

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?