SA NT DataLink submission

Productivity Commission

Data access and availability

July 2016

As given by the Terms of Reference, the scope of this inquiry is "*to conduct a broad ranging investigation into the benefits and costs of increasing the availability and use of public and private data by Australian individuals and organisations, including individuals' access to data about themselves*". The very wide scope is also reflected in the large number of questions for which it is seeking responses. SA NT DataLink has addressed the questions in the order provided in the discussion paper, but in summary has also provided what it considers to be the key messages in its Executive Summary that it would like the Productivity Commission to consider.

SA NT DataLink was established in 2009 to provide a high quality data linkage service to support research, policy development, service planning and evaluation. It is part of the Population Health Research Network (PHRN). It offers data linkage services for the university research sector within South Australia and the Northern Territory involving health and human services data and also supports research undertaken within the public health and education systems. It supports cross jurisdictional data linkage for other organisations, and access to Commonwealth data. A list of the datasets currently linked by SA NT DataLink, its governance structure and the security and privacy protections it provides is available on its website.

SA NT DataLink recognises the value and need to link data beyond the health sector and, in response to this and the research and policy analysis proposals it receives, is continually progressing authorisations to receive new datasets outside of this sector. It is SA NT DataLink's experiences of seeking the required authorisations from numerous government agencies (including the Commonwealth) and the regulatory frameworks in which it has operated over a number of years which has informed its responses in this submission.

SA NT DataLink is uniquely located in the South Australian Health and Medical Research Institute (SAHMRI) providing direct access to significant research work undertaken by SAHMRI and by whom it is recognised as having a significant role in clinical research and the translation of research into greater public benefits, particularly in the population health, genomics and biomedical areas.

SA NT DataLink's experience and its network as part of the PHRN gives it particular practical insight into many of the issues raised in this paper and it strongly supports the need to address these as a matter some urgency if the potential for greater public and economic benefits are to realised.

SA NT DataLink has restricted its more detailed responses to the key areas where it has the strongest expertise but acknowledges that all areas need careful consideration.

SA NT DataLink would also refer the Commissioners to the Senate Select Committee on Health's sixth interim report Big health data: Australia's big potential which has addressed many of the same issues being considered by the Commissioners. The recommendations in the Senate report are consistent with the views of SA NT DataLink (included in Attachment 1).

In response to this Inquiry SA NT DataLink offers the following:

Executive Summary

- SA NT DataLink would endorse the *Recurring data themes* in Box 2 as being the key issues that need to addressed.
- SA NT DataLink's experience is that the variations in data availability, access and its timely provision create significant barriers characterised by variability in jurisdictional regulatory requirements, different and multiple authorising environments (including multiple ethical approvals) and organisational polices/cultures resistant to more open access.
- At the State/Territory and Commonwealth levels, Australia needs to develop consistency in the regulatory frameworks and authorising environments to create a more efficient and timely process for data provision along with privacy protection. Developing a nationally consistent framework may need to be driven through COAG and should consider the government, non-government, not for profit and private sectors.
- Leadership and support for an open data approach at mid-management agency levels is also crucial as this is where the support from senior management and chief executive levels for this approach often stalls because of functional custodian resistance and/or their other competing priorities.
- Agencies are being asked to provide or limit services in a framework of increasing reductions in human and financial resources. Their real capacity for the timely provision of data is therefore increasingly limited as they focus on their business priorities and lose the staff with the necessary analytical skills. Government and their agencies need to consider the access to and timely provision of data (particularly to bodies outside of the government sector) as part of core business and make budget provisions for this.
- It is SA NT DataLink's observation that there is a national and internationally competitive environment for those who can undertake the necessary data analytics work at the high level of complexity required. Providing the longer term financial and resource requirements to attract appropriately skilled people should be a part of the considerations when addressing concerns about greater data access and availability.
- Consumers must be engaged and be convinced of the efficacy of the privacy protecting principles and regulatory frameworks that ensure the risks to privacy are properly managed and are acceptable to them.
- Risks to privacy arising from data mining and the potential for re-identification of previously de-identified data through for example, geocoding and also linkage to other data should be carefully considered and responded to through legislated protections and potential sanctions for breaches of privacy to ensure the public's confidence in this area.
- The tensions between privacy protections and data availability will be (or are already)

particularly felt in developing technological areas such as: biometrics technologies; video surveillance; e-commerce; workplace monitoring; location tracking; data profiling; criminal identity theft; background checks; information broker industry; public records on the internet; financial privacy; medical records confidentiality; genetic privacy. Considerable more effort in community engagement and investment in regulatory protections and organisations supporting consumers is required.

- Definitions of high value datasets will vary between sector needs and also over time. For example, locational analysis involving linkage to other datasets appears as a consistent requirement. Standardisation is important in for example, geocoding where high validity and reliability of addressing as part of a high standard reliable national geo-coding dataset is required.
- SA NT DataLink supports researcher access to Commonwealth data such as the Pharmaceutical Benefits Scheme, the Medical Benefits Scheme and Centrelink and is working in partnership with the Commonwealth Government to facilitate more timely access to these and other key Commonwealth datasets. However, the Commonwealth's tight control on the availability of these key and other highly valued datasets limits wider access and the ability to make optimal use of this information for data linkage by a SA NT DataLink and other linkage units.
- The above observations concerning control and access to Commonwealth data also apply to State/Territory government data and more variously to the agencies within these jurisdictions.
- State/Territory governments have or are seeking to address the above issue, but the provision of data outside of government remains problematic in terms of enabling regulatory frameworks and supportive organisational polices and cultures. Clear support for the development of capacities such as SA NT DataLink (and the PHRN more generally) is required to provide the secure and privacy protecting environments that can manage the data and provide public confidence regarding the protection of their privacy.
- The Productivity Commission has asked a number of important questions regarding access to government data by private for profit organisations. A key concern about the management of public data by the private for profit sector is about the potential for the lack of public transparency once public data is provided to or controlled by a private company. There are also concerns that commercial in confidence contract provisions governing the management and access to the data may restrict access or enable charges to be levied for access to data that was previously available at no cost or on a cost recovery principle only.
- For example, the Commonwealth government has contracted the management of the recently established National Cancer Registry to Telstra Health. Telstra Health, as a private for profit company, is being granted access to freely provided public health data under a contract classed as commercial in confidence. What costs, if any, may be

charged by Telstra has not as yet been made public. However, from SA NT DataLink's experience, research is significantly inhibited where there are new or unacceptably high cost barriers to accessing data, particularly where there were none previously.

- The lack of apparent information or consultation about such significant organisational changes to the way data is held and managed is of concern, particularly as it may impact on the interests of a number of key stakeholders, including researchers who would consider the data as high value.
- SA NT DataLink is also aware of concerns about the regulatory framework under which the Registry is to be established, a key one being that the proposed legislation does not express any stated objective as being for a public benefit. Underpinning this is a fundamental question as to whether a private company profit from freely provided information which is also provided apart from a clinical purpose, also on the basis of a public benefit and not for profit considerations.

General comments

The responses from SA NT DataLink are based on its well-developed understanding and experience of the importance of personal data in relation to the health and human service domains in particular, and its more general understanding of the issues related to data access, availability and privacy.

Responses to the questions and issues raised in this paper will be governed by the differing categories of data and/or businesses. Differentiation between the categories of data and the differing foci of businesses (including government businesses) is important to avoid treating data and businesses as having similar risks and significance. The same applies to responding to consumers as a reasonably homogenous group with similar awareness and needs about data and data access. This is inconsistent with Australia's socio-economic and cultural reality.

At the national and international level, the analyses of the importance of open data and the issues surrounding this are well addressed in publications as noted in the references provided in this paper. For example, the Productivity Commission, *Annual Report 2012-2013*; the "*Open government data and why it matters*" published by the Australian Government's Department of Communications and the *Arts—Bureau of Communications Research the OECD (2015)* reports provide excellent analyses of the main issues being canvassed in this paper. The analyses of the issues and directions in these references are generally supported by SA NT DataLink.

Non-government sector data should also be considered as part of the discussions. Non-government (or community-based) health and human service organisations make up a significant part of the service delivery sector in this area. More often they are at least part funded by government or operate as a not for profit private charitable organisation. The information this sector collects is a valuable source to consider in the provision of human services if a more complete understanding of the health and human services sector is to be developed. It also presents significant challenges, since it should be expected that the data collected and the collection systems are more often characterised by inconsistencies. Significant investments may be required to take better advantage of the data they hold, in particular for data linkage purposes.

The responses of SA NT DataLink to questions relating to privacy are premised on the fact that all data linkage is based on the 'separation principle' informed by Kelman, Bass, Holman (2002)[1] as best practice, and as used internationally. The separation principle:

- Minimises the risks of identifying or re-identifying individuals for data linkage projects.
- Requires the clinical/service information from a record be separated from the identifying information on that record.
- Ensures that apart from the data owners/providers, persons do not have access to both identifying information and clinical/service information.

1 Kelman CW, Bass AJ & Holman CDJ *Research use of linked health data - a best practice protocol*. Australian and New Zealand Journal of Public Health 26 (3): 251-255, 2002.

- Ensures that only approved persons are provided with de-identified clinical/service information.

Overall SA NT DataLink strongly supports a nationally consistent approach to data access and availability. However, it is very aware that the value of the data and therefore the attitudes to it are strongly predicated on whether the discussions are about public or private for profit sector data and therefore the differing imperatives in regard to ownership and use, with the latter sector being strongly focussed on commercial gain.

The discussion paper questions also need to consider the different types of data and their purposes more particularly for the government sector where data relating to criminal justice and/or security may need to be considered separately from the range of health and human services data. That is, careful consideration should be given to the political and personal sensitivities of the data and therefore the impact of these on their release, and how to best balance these sensitivities and the public interest.

QUESTIONS ON HIGH VALUE PUBLIC SECTOR DATA

What public sector datasets should be considered high-value data to the: business sector; research sector; academics; or the broader community?

What characteristics define high-value datasets?

The value of a dataset lies in the commercial, policy or research questions that are part of a sector's interests and priorities.

Generally, in line with the later mentioned 'open government' policies, data that may be considered as high value by the community may be those that can be used to increase agency accountability and responsiveness, improve public health and wellbeing outcomes and create economic opportunities or respond to identified needs and demand in the range of areas for which governments are accountable.

Public sector datasets related to health, human services, education, transport, justice, and the environment would all be considered as high value, but the importance may also vary over time. While these datasets could be well-considered as high value, it is not as simple as listing these, since value is given by changing sector needs and priorities, particularly for the business and research sectors which need to meet commercial and funding imperatives.

A flexible approach to considering high value datasets is required. For example, even with in the research sector which includes the academic sector, there will be differing priorities in regard to how they assess what they consider to be high-value data based on the priories given to the areas of research by their particular for profit research organisation or universities.

Generally, the value of datasets can be considered in terms of combinations of the following:

- The level of demand for the information.
- The importance of the area for which they required.
- The quality and accessibility of the data.
- The priorities and needs of the organisation or sector requiring the data.
- Commercial/business imperatives.
- Popular/political interests.

In this age of 'Big Data' and the analytical capacities of data mining, increasingly a wider range of datasets are sought to make possible a greater refinement in the analysis and understanding of responses and outcomes which can be used to support an organisation's imperatives/interests.

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

There is growing demand for increased availability and use of public sector data which governments are responding to as evidenced by State, Territory and Australian Government policy responses that can be couched in key phrases such as 'open government data', 'open

access', etc. The justification for these policies is most often couched in terms of a 'public benefit'.

The value to the community, to government and other sectors from increasing the availability and use of public sector data is well recognised in the Commonwealth Government's own 2016 publication, *Open government data - and why it matters. A critical review of studies on the economic impact of open government data.*

While it is possible to make general comments about greater data availability and community benefits, the benefits should be more specifically considered in the context of the type of data being made available, the community (ies) being considered.

One of the often stated key benefits and the increasing availability and use of public sector data lies in the greater potential for sounder evidence based decision making, particularly for Governments. As data availability and access increases, it may be presumed that this benefit will become more evident.

Open access to data and the evidence provided from its analysis is also an important principle stated by governments to ensure that there is transparency and accountability for decisions related to funding and priorities. To enable this, it is important that the same data is available to other organisations to undertake an independent analysis.

Enabling open access (always assuming privacy is protected) can enable other organisations to provide alternative models and evaluations that may provide a wider range of options and thinking that are not constrained by particular agency (or government) bound thinking.

The above points are made in the Executive Summary of the *Open government data* publication:

> *Raw data collected in the course of usual government operations exhibits strong public good characteristics—it is non-rivalrous (use by one party does not reduce its availability to others) and non-excludable (once available to one party, others cannot be readily excluded from using it). This provides a strong rationale for governments to take a default position of making government data more accessible.*

In the private for profit sector there are likely to be considerable tensions between the data they hold and open access since this sector has commitments to shareholders to maximise profits and therefore open and freer access may conflict with this obligation.

Community benefits may also depend on the uses made from the data. For example, demonstrating the benefit for the use of health and medical data may be relatively easier than housing, traffic and road use data to inform the needs of transport systems and investments by private companies in building public roads where in the latter case, the cost of using the public roads to create a return to the investing company may offset the perceived community benefit. The use of health data by insurance companies for their commercial purposes in much the same way locational and/or demographic and accident data are currently used by insurance companies when determining premiums would raise considerable public objections.

It is worth noting the 2016 report prepared for the Wellcome Trust (UK*), The One-Way Mirror: Public attitudes to commercial access to health data*, which surveyed public attitudes in the UK about the topic as suggested in the title. The report suggested that most of those surveyed tended to accept the commercial use of health data, subject to there being, amongst other mechanisms, safeguards for public control. There was also a significant core group (17%) who did not support the use of health data for commercial gain under any circumstance and for whom the use of the data for insurance assessment and marketing was unacceptable as was third party access to the data.

Overall, where the question is about making public data available for the private sector, there are a number of other issues that need to be considered at the public policy level, and importantly consumer responses.

QUESTIONS ON COLLECTION AND RELEASE OF PUBLIC SECTOR DATA

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

There are at least four key factors stopping or limiting government agencies providing data. In summary, these are:

1. The lack of clear and consistent authorising environments (including legislation) that support the provision of data and protect individual privacy. This should be considered as one of the major issues and addressing this would also help address other issues.
2. Organisational cultures which are inherently conservative and cautious about the provision of their data outside of their agency, including to other agencies.
3. Leadership and support at senior agency levels that support an open data approach.
4. Leadership and support for an open data approach at mid-management agency levels as this is where senior support often stalls with functional custodian resistance.
5. Public attitudes and/or concerns about making their personal information more available.

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

To make better use of their data, governments need to address at least the following key issues:

1. Developing whole of government policy directions supported by a legislative framework that enables data sharing and ensures that public privacy concerns are addressed.
2. The need for Governments to agree to standardised inter and intra agency technical capabilities and support the development of these where necessary.
3. Considering the cost of making data available as part of government core business and budget accordingly.

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?

Clearly a standardised approach to the sharing and release of data is ideal. However, such an approach also needs to be responsive to the sensitivities of the data. Overall though there should be a standard set of policies and approvals across government at least within in each jurisdiction and ideally, across jurisdictions. However, Australia's federal system militates against this.

There is a risk that in developing such an approach to the large range of data collected or available, that the collection and availability is based on a minimum dataset approach with the standards focussed on government reporting requirements. A consequence could be that other data considered valuable for research and evaluation purposes may not be considered within such a framework.

There would have to be extensive consultations with key sectors who may be users of the data to understand their needs and what they consider to be 'fit for purpose'. It is important to consider both immediate purposes and long term purposes and avoid the risk that the lowest common denominator in standardisation may only meet immediate needs for some users. For example, the data requirements of the research sector may well differ from that of the government or non-government sectors.

SA NT DataLink is not in a position to estimate the cost of standardisation, but it is very cautious about user charges for access to the data as part of a cost recovery principle. This is discussed later in this submission.

What criteria and decision-making tools do government agencies use to decide which public sector data to make publicly available and how much processing to undertake before it is released?

In South Australia, some of the key criteria for making public sector data available are visible in the conditions for the establishment of SA NT DataLink. SA NT DataLink was established in 2009 with the support of the SA Government on the basis that SA NT DataLink would only support projects that would provide a public benefit. Therefore, government agencies that provide data for linkage purposes through SA NT DataLink only support projects with this same purpose.

In addition, all projects seeking data must:

1. be approved by an accredited NHMRC ethics committee; and
2. be approved by each agencies data custodian; and
3. have an approved methodology that protects individual privacy and provides assurances and governance with regard to the appropriate use of the data.

As part of the process for approving the release of data, data custodians must be satisfied that the data do not contain identifying information or be readily suitable to re-identifying individuals. Data custodians (and data users) have significant responsibilities to ensure that they take measures to minimise this risk to privacy and enable a project to meet its objectives.

Apart from assessments made during the approval process, risks may also be managed by a general condition for all SA NT DataLink approved projects that a researcher must provide to data custodians a copy of presentation or submission for publication prior to the presentation or submission. The data custodian may review the information to ensure that individual privacy has been protected and that the findings are consistent with the information they have provided.

It is SA NT DataLink's experience that trust is a key factor in government agencies making their data available. Agencies should have confidence in the person and the organisation that the information provided will be appropriately held and managed. However, this confidence should be supported by well-established and agreed to security systems and protocols regarding the provision and use of the data.

What specific government initiatives (whether Australian Government, state, territory or local government, or overseas jurisdictions) have been particularly

effective in improving data access and use?

In SA, the Government's 'Open Data' policy is a positive initiative, but is still in the process of development and implementation. Therefore, effectiveness over the longer term is yet to be assessed.

Similarly, the Australian Government's initiatives in this area are also welcomed but the practical import of these are still being trialled and developed and the continuing reluctance of Australian Government agencies to provide more open access is still a notable factor. This may in part be the result of legislative barriers or more so of organisational cultural and/or policy barriers related to control of information, risk aversion and uncertainty about the level of security where the data may be held and later provided to a third party.

Some well-established overseas models that appear to have addressed these issues are discussed in response to later questions.

Overall, there has been a very positive response to the establishment of SA NT DataLink and the PHRN nationally and this research infrastructure has been particularly effective in improving data access use, albeit within the context of the limitations discussed in this paper.

QUESTIONS ON DATA LINKAGE

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

See previous response to question on high value datasets but in summary are:

- Research inquiries into the effectiveness of government initiatives and interventions, including outcomes, cost effectiveness and meeting policy objectives particularly where these can create greater accountability and transparency.
- Evaluations providing a robust evidence base to better inform potential planning and policy decisions that impact on communities.
- Public and clinical health interventions which are strongly supported by health consumers and consumer bodies.

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

The broad regulatory and/or policy areas which make accessing and linking datasets more difficult are:

- Variations across jurisdictions for multi or cross jurisdictional projects in meeting administrative and approval requirements that govern the provision of data can create significant delays, particularly where Commonwealth data is involved.
- Again for multi or cross jurisdictional projects, the need for multi-jurisdictional ethics applications can also create delays.
- Reluctance by Commonwealth Government agencies to make high value MBS, PBS and Centrelink and other data more readily accessible.
- Full cost recovery policies for provision of Commonwealth data create significant (sometimes impossible) barriers to accessing the data.
- Organisational inconsistencies between a public stance of making data available and the reality of inner-organisation custodian resistance at odds with the policy position.

How can Australia's government agencies improve their sharing and linking of public sector data? What lessons or examples from overseas should be considered?

As already suggested above, consistent regulatory, governance and authorising environments within and across jurisdictions would significantly improve the sharing and linking of public sector data. Potentially this may lead to:

- A more efficient governance process for decision making.
- Requiring the provision of data as a standard agency business process and therefore as part of 'core business' of agencies.
- Provision of adequate resources (financial and skill sets) for this process.
- Organisational consistency in provision of data.

Secure long term funding arrangements are needed to ensure the development of the required data linkage infrastructure and the embedding of these services as part of infrastructure and meeting government and other stakeholder long term expectations.

Given Australia's federated model of governance the differing jurisdictional legislated governance arrangements and authorising environments would also need to be addressed.

It is well recognised that Australia's jurisdictional arrangements are characterised by tensions between Commonwealth and State/Territory relations broadly in the areas of funding, accountability and program delivery. This is also reflected in the flow of data between these jurisdictions. For example, from a SA NT DataLink perspective the difficulties related to the timeliness for the authorisations and provision (and the cost of provision) of Commonwealth data (e.g. MBS, PBS and Centrelink) to researchers in States/Territories has been a significant barrier to state-based research that could be of value in the evaluation of their jurisdictionally based health service delivery and outcomes, as well as nationally.

There are two main pathways to address some of the issues related to data linkage from a national linkage perspective. Each presents challenges.

1. Providing for a comprehensive single national linkage capability that can make available Commonwealth data and/or undertake national or cross/multi-jurisdictional projects. To some extent AIHW is already undertaking this work, but on a project by project basis without enduring datasets. (Although SA NT DataLink is aware that AIHW is giving consideration to a single 'enduring master linkage' dataset for Commonwealth agency data, the provision of enduring data from State/Territory agencies would be carefully considered by these respective governments in terms of its policy implications.)

   This approach creates a single gateway through which Commonwealth data may be accessed. The risk is that this could create significant delays and also create a single point for controlling access to data which may militate against a more flexible approach to accessing data.

2. Providing for long term resourced State/Territory linkage capabilities. Again, these capabilities are established, but the nature and certainty of the funding can determine their priorities and the development of their infrastructure. For example:

   - predominant reliance on government funding and therefore primarily meeting government needs or as recently experienced NCRIS funding being used as part of a political bargain process; and/or
   - predominant reliance on relatively short-term funding (i.e. NCRIS) making it difficult for each to build their capabilities to suit their jurisdictional requirements and needs and to attract and hold staff with the required skills and experience.

Canada and the United Kingdom provide examples of good legislative and policy options that are instructive for Australia.

Canada, while also having a federated model, provides some Provincial models for reasonable legislation establishing the requirements for the provision, storage and use of data, the protection of privacy and the establishment of data linkage centres. These centres are supported by consistent government funding. That is, the models demonstrate what may be possible at the State/Territory jurisdictional level with reasonable government and regulatory support. (SA NT DataLink is aware that Canada is seeking to establish a more national approach that can accommodate its jurisdictional arrangements).

It should be stressed that what is central to all linkage centres is that their model of operating is based on the 'separation principle' as described previously.

CANADA

Manitoba, Ontario and British Columbia legislative models mandate the body to which information can be provided. They ensure that there can be proper controls over who may access the information and also mandate the responsibilities and obligations of that organisation. The legislative oversight requirements support public confidence and trust. They key provisions of the legalisation enable:

- A mandated privacy protecting framework to give confidence to businesses and consumers that the personal information provided is being properly managed. In particular, the 'separation principle'.
- Mandating agencies and their data custodians to make their data available; support for the provision of data from the non-government and private sectors; and providing protections when the former is undertaken.
- Establishing a trusted party to hold and manage the information provided.
- Providing for sanctions where privacy is violated.
- Provision of a sound evidence base to support government policy directions.
- Funding certainty. (Note that Farr @ Scotland (UK), although not a based on a mandated model, is also funded by Government.)

Manitoba

In Manitoba, the Manitoba Centre for Health Policy is mandated. To make best use of the Centre's resources and capabilities, senior level government officials meet on an annual basis to plan/review the strategic policies based on the government data provided for research through data linkage. The Manitoba *Personal Health Information Act 1997* is specific legislation governing the collection and provision of data and mandating the Manitoba Centre as the organisation responsible for the storage and provision of de-identified data. While the focus is on health, the health data can be linked to other datasets it holds such as housing, education and justice to more fully examine the social determinants of health. The Manitoba centre is funded by government.

Ontario

In Ontario, the Institute for Clinical Evaluation and Science (ICES) is designated as an entity under the *Personal Health Information and Protection Act 2004* to

receive government data. This designation is granted by the Information and Privacy Commissioner (IPC) of Ontario. ICES manage a health data repository for the province of Ontario, Canada. It plays a key role in supporting policymakers, managers, planners, practitioners and other researchers about the Ontario health care system.

British Columbia

In British Columbia, Population Data BC (PopData) provides government data for health related policy-making and investment decisions. PopData operates under the BC *Freedom of Information and Protection of Privacy Act 1996* and the *E-Health (Personal Health Information Access and Protection of Privacy) Act 2008* with the oversight of a public body, the *Data Stewardship Committee* responsible for approving the research data to be made available. PopData is funded by a number of government agencies.

UNITED KINGDOM

In the United Kingdom the *Data Protection Act 1998* provides general protections governing the provision and use of data. It is a large and complex Act which controls how personal information of living persons is used by organisations, businesses or the government and provides legal protection for authorised disclosure of personal and sensitive information.

The Act has broad purposes relating to the provision and access to information and is not restricted to health information as are the above Canadian models.

While not specifically dealing with data linkage, the Act underpins the Scottish and other UK Government's models for governance and privacy protection in data linkage and the Farr Institute for Health Informatics in particular, to which Farr @ Scotland belongs.

Scotland

Data linkage in Scotland, while underpinned by the above Act, is governed by the Safe Haven Charter. The Charter supports an environment for operating under an agreed set principles and standards for the provision of electronic data to support research when it is not practicable to obtain individual patient consent. It provides a good strategic and operational policy model for the provision and use of data. A central principle of the Charter is the protection of patient identity and privacy. The principles ensure researchers are working with data in an approved and trusted research environment, described as a 'Safe Haven'. Further information can be found at www.gov.scot/Topics/Statistics/datalinkageframework.

Each of these models demonstrate reasonable and effective legislative and policy principles that support greater availability and access to data in privacy protecting environments that should be considered in the Australian context.

QUESTIONS ON HIGH VALUE PRIVATE SECTOR DATA

What private sector datasets should be considered high-value data to: public policy; researchers and academics; other private sector entities; or the broader community?

In each case cited, what characteristics define such datasets?

What determines high value private sector datasets should be considered similar to the previous responses regarding public sector data (that valued data is related to their policy and commercial imperatives, etc.).

What would be the public policy rationale for any associated government intervention?

Key points a public policy rationale for government intervention should consider in improving access to data or in creating regulatory frameworks are:

- The need to make the data available for a demonstrable public good in the evaluation of delivery of services or the translation of research into better service delivery and outcomes.
- The need to provide an acceptable balance of the public benefit against the risk to privacy.
- Related to this, the need to support public confidence by regulations that provide for sanctions where there is a breakdown in privacy or confidentiality of information.
- The potential for commercial gain and under what circumstances, and how, a share of the gain is returned to a public good.
- Restricting the potential use of public data from purely commercial interests and its use particularly where the information may adversely affect the public (e.g. vetting or risk assessments of clients for insurance purposes).
- The level of public support.

QUESTIONS ON ACCESS TO PRIVATE SECTOR DATA

Are there any legislative or other impediments that may be unnecessarily restricting the availability and use of private sector data? Should these impediments be reduced or removed?

The private sector and persons more familiar with the relevant laws are better placed to address legislative impediments that restrict access to private sector data. In addition to legal impediments, there are likely to be contractual impediments, since the data are often the intellectual property that underpins the commercial viability of a company.

The question of what is a necessary restriction and what is not would have to be considered in consultation with the relevant private sector businesses and other stakeholders who have interests in private sector data. For example, public concern about the use and/or on selling of private information obtained online or as part of software downloading/purchases. Generally, there is a growing concern and debate about the uses made of personal information collected by the private sector. Whether and how this should be addressed though legislation are significant policy questions and can truly be described as a wicked policy problem that is also ideologically driven. Note too, that government's also make use of this data for their purposes.

A current example of private sector access to personal and sensitive health data which is of current interest is the contract signed between the Commonwealth Government and Telstra Health regarding the establishment of a national cervical and bowel cancer screening registry. To date the contract has been classed as 'commercial in confidence' and therefore its content in relation to the security of the data, access to the data and also the uses to which the data may be applied are not known. There is also a significant question of public transparency and accountability in relation to the establishment and on-going costs of the registry which will hold public health information. More particularly, there is some anxiety about Telstra Health, since this is public health data that will be provided to a for profit private sector company. The government had drafted a bill for the establishment of the registry (lapsed when parliament was prorogued) but the bill as drafted may not adequately address significant areas of public concern. The anxiety about private for profit corporations accessing personal and sensitive information is evident in the government's initiative. While the adequacy of the proposed legislative protections is yet to be debated, the lack of transparency and public consultation with key stakeholders (apart from those with the immediate commercial interest) suggests government has yet to develop a sound public policy approach in making sensitive information available to the private sector.

Whether legislation is or should be an impediment may depend on the interests being considered. Regulatory frameworks supporting the provision of data may serve community and government interests when issues arise that require governments to address and, as has most often been demonstrated, addressed at the government's and/or the community's cost.

What are the reasonable concerns that businesses have about increasing the availability of their data?

See responses (p4) regarding business and commercial impacts and intellectual property rights.

What principles, protocols or legislative requirements could manage the concerns of private sector data owners about increasing the availability of their data?

This is difficult to answer because of the conflict of the interests between business imperatives and community and public imperatives. While a set of principles may be of value, they are most likely to require a regulatory framework to have wider public acceptance and for them to operate effectively. It is relatively straight forward to develop high level principles and protocols for which there may be agreement and about which useful rhetoric may be developed. However, all principles that are accepted must also have practical effect and able to be supported to the satisfaction of the stakeholders. What is also essential is the support of the particular private sector businesses.

The provision of data (particularly if mandated) would have to be carefully considered so as not to run counter to the commercial competitive interests of the companies. And, as already mentioned, the information when linked to other publicly or privately available data should not be used to disadvantage individuals or communities. There is likely to be considerable public protest about the use of personal information for such purposes.

Whether a regulatory framework is required to give effect to the principles is one consideration. As part of this, the cost of the regulatory burden would have to be considered against the public benefit in ensuring that there is mandated accountability and transparency.

Should the collection, sharing and release of private sector data be standardised in some way? How could this be done and what would be the benefits and costs? What would standards that are 'fit for purpose' look like?

As suggested previously, the standardisation of government data within and across jurisdictions presents significant challenges. If this were to be attempted in the private sector, the support of the various private industry interests in this sector is required. They would need to be convinced of the need and practicality and by a positive cost/benefits analysis supporting standardisation and release of data, and if mandated, the cost of compliance to legislation.

Overall, significant further work would be required to undertake a strategic analysis of the benefits in terms of the public good (to justify the work and expected outcomes) and the commercial benefits on an industry by industry basis.

To what extent can voluntary data sharing arrangements between businesses / between businesses and consumers / involving third party intermediaries — improve outcomes for the availability and use of private data? How could participation levels be increased?

SA NT DataLink is an example of an organisation acting as an intermediary between the data holder (the data custodian) and a data user. SA NT DataLink through the application of the separation principle ensures that the user does not have access to the identifying information of the data custodian. The effectiveness of this model has created trusted relationships between data custodians and SA NT DataLink enabling other parties to make

valuable use of the data custodians' (de-identified) information for research purposes. However, it should be noted that SA NT DataLink, as do the other PHRN linkage units, also operate in regulatory and authorising environments (albeit in a multiplicity of these) that support the provision of data and the protection of privacy.

To date nearly all data provided have come from the government sector. This same trusted relationship is yet to be built with the private health sector. There is work underway in this area and SA NT DataLink has successfully been involved in a project with the private pathology sector, and through its location and relationship with the South Australian Health and Medical Research Institute (SAHMRI) also building positive relationships with some of the private health sector.

Would such voluntary arrangements raise competition issues? How might this change if private sector information sharing were mandated? Is authorisation (under the Competition and Consumer Act 2010 (Cth)) relevant?

Discussion with those proficient in this area of law is required. Other legal issues regarding contract law and commercial in confidence provision also need to be considered.

As part of the first steps, clarity is needed as to what may be expected from voluntary or mandated arrangements and then discussions with peak bodies representing the various private sector interests is required to determine their willingness to participate.

What role can governments usefully play in promoting the wider availability of private datasets that have the potential to deliver substantial Report prepared for the Wellcome Trust 2016 benefits?

Governments should have a clear role in:

- Communicating the benefits and the risks to the public and gauging and respecting their views.
- Adherence to the key principle of the public benefit.
- Ensuring that sound governance, authorising and transparent reporting environments are in place to ensure the protection of privacy.
- Mandating requirements where necessary.
- Ensuring secure environments for the data are in place with appropriate controls and management of the data.
- Ensuring mechanisms for sanctions and redress are applicable.
- Taking note of and incorporating successful international models and practices to inform Australian model(s)

How can the sharing and linking of private sector data be improved in Australia? What lessons or examples from overseas should be considered?

See previous responses (p9) to questions related to this area.

Who should have the ownership rights to data that is generated by individuals but collected by businesses? For which data does unclear ownership inhibit its availability and use?

Ownership rights to information collected by private businesses may be complex and governed by varying legislative requirements and by business contracts. Three key issues requiring consideration include ownership rights:

- Related to Intellectual Property (IP).
- About information concerning them by agreeing to an end user license agreement (EULA) Ownership rights.
- Specified in contractual agreements.

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?

Public access to data about themselves is often restricted by the organisation itself either through difficulties in gaining access to the appropriate persons, bureaucratic processes or business policies or legal restrictions which inhibit or block access.

There is no simple response as to how to streamline processes governing individual's access to their data. The processes would need to consider:

- The nature of the data and its value to consumers.
- If it is private sector data what, if any, agreements exist between the individual and the organisation regarding access or what legal or contractual restrictions prevent its provision.
- If it is public sector data what, if any, legal or policy restrictions may apply to accessing it. For example, law enforcement and security information.
- What cost impediments may exist.
- What technological impediments there may be, including access and conversance with the technology.

Nevertheless, there are models of legislation that enable consumers access to private company information, with the law enabling consumers to view and amend their credit information is one such example. Creating public awareness of consumer rights and access and uptake by consumers will be an issue to determine effectiveness of such laws. Access and technological literacy in particular may become significant equity issues.

Are regulatory solutions of value in giving consumers more access to and control over their own data?

While private sector organisations may offer some pathways to better access, regulatory solutions may be required since organisations (public and private) may be unable to provide the information needed and/or have historically been more predisposed to not making the data available than the converse.

A further risk is that these providers become another organisational sector that has access to consumer information, perhaps without sufficient regulatory oversight or protections for them.

The European Union's General Data Protection Regulation has just come into effect, the main purpose of which is *to give citizens back control over of their personal data, and to simplify the regulatory environment for business*. While the Regulation is in response to EU's Digital Single Market Strategy it recognises with its implementation that organisations (public and private) will (or already) have considerable information about individuals over which the individuals have little or no control in regards to its content and use. Both the *Digital Single Market Strategy* and the *Regulation* present a sound model responding to the capacities and potentials of Big Data and data sharing, and how to balance these drivers with the need for consumer protections. How applicable they may be to the Australian political context needs to

be considered, nevertheless they demonstrate the importance of regulatory frameworks for addressing the issues.

Are there other ways to encourage greater cultural acceptance amongst businesses of consumer access to data about them?

Perhaps because of a culture of resistance to data access (often supported by legal and contractual obligations) it may be that a mandated approach is needed to shift the balance towards greater consumer access to their data. Industry self-regulation may be a preferred approach of the industry concerned, but industry failure in self-regulation and in publicly acceptable standards of transparency and accountability should also be noted as a significant concern with many examples of obfuscation and the unscrupulous use of personal information for personal or corporate profit. The role of industry in determining processes and standards for itself without a strong independent public interest representation also needs careful consideration in the context of the real differences in the power and influence that industry may have vis-à-vis the public generally or a particular community

The Wellcome Trust findings mentioned previously gives support to a view that consumers do not welcome, or only cautiously so, access to their information particularly where there is to be commercial gain made from its exploitation, either individually or more generally.

What role do third party intermediaries currently play in assisting consumers to access and use data about themselves? What barriers impede the availability (and take-up) of services offered by third party intermediaries?

There is a significant role (especially if underpinned by a principle of equity) for third party intermediaries to assist consumers to access data about themselves. The capacities, accessibility, affordability and diversity of third parties may be significant factors in determining the success of third parties, particularly where consumers are from culturally and linguistically diverse backgrounds who may not be aware of their rights. How such parties may be established and/or funded is important. There are many examples of private organisations acting as information brokers to consumers by providing information already publicly available, but at a much greater cost than what the originating agencies my charge. While a successful private sector business model, the practice may rely more on taking advantage of the lack of consumer awareness in accessing the information, than an informed choice by the consumer about cost alternatives.

What datasets, including datasets of aggregated data on consumer outcomes at the product or provider level, would provide high value to consumers in helping them make informed decisions? What criteria should be used to identify such datasets? What, if any, barriers are impeding consumers' access to, and use of, such data?

The range of consumer interests would need to be considered to identify the datasets. For example, where consumers are making commercial consumption decisions, responses to a product or market information may be valued. Where they are health decisions more specialised information would be valued. Consumer attitudes about which data sources they value or give credence to is also a consideration. Given the major part of consumers'

information is web based, efficient and reliable internet access and the technical literacy to effectively navigate IT systems are also important considerations.

QUESTIONS ON RESOURCE COSTS OF ACCESS

How should the costs associated with making more public sector data widely available be funded?

If greater availability and access to public sector data is to positively implemented, then the provision of data should best be regarded as a core cost of the ongoing business of government.

Full cost recovery is justifiable where the data provided will lead to a commercial gain for a person or body. Outside of this, given the expense of government business, cost recovery (and partial cost recovery) may significantly reduce the capacity of individuals and/or organisations such as researchers and/or their universities to afford to make use of the data. Should this occur, the data is more likely to be unused or only be affordable for larger private interests and there is a risk of creating monopolistic structures and organisations within which data analysis and research is concentrated. That is, it would work against a stated government commitment to openness, transparency and accountability.

The previously referred to 2016 publication *Open government data - and why it matters*, states that as part of openness in government and increased access and to availability of data, costs to accessing data should not inhibit a general practical capacity for accessing the data, by creating cost barriers.

> *For open government data to provide maximum public benefits through improving welfare and significantly encouraging its use and re-use, it should be provided at no cost, or at the most, priced at the short-run marginal cost of making it publicly available. It should not be generally taken as an opportunity by government agencies to recoup costs that would have been incurred in normal operations.*

The issue of the cost of accessing data needs careful consideration since prohibitive costs will effectively negate access to data and therefore work against the potential benefits of increasing availability and access. If governments are committed to this, then it is reasonable to expect governments to provide data as part of its core services, the cost of which it must provide for in its budget, or have costing models based on the nature and capacities of organisations or individuals seeking the information to pay.

To what extent are data-related resources in agencies being directed towards dealing with data management and access issues versus data analysis and use?

Management of data to align with reporting requirements is a reasonable expectation of agencies. However, there may be a risk that as part of this management, only the data required for reporting are considered and/or only access to these data is provided. Therefore, data outside of these requirements, which can be added to analysis to provided richer and more accurate information, may not be included at the time of collection or data quality processes are not as well applied.

Researchers accessing agency health and human services data through SA NT DataLink,

although sometimes frustrated by data quality or availability, more generally are satisfied with the data that are available to them.

What pricing principles should be applied to different datasets? What role should price signals play in the provision of public sector data?

See previous response (p18) on costs and cost recovery implications associated with data provision.

Is availability of skilled labour an issue in areas such as data science or other data-specific occupations? Is there a role for government in improving the skills base in this area?

There is an accepted recognition of the shortage (nationally and internationally) of persons with the high level analytical skills needed to undertake complex data analysis, particularly of integrated or linked complex data.

There is a role for government to provide ongoing and long term support for the infrastructure that will attract persons with these skills. When looking at international models such as those previously mentioned, they have a better capacity to attract, hold and build the skill sets required because the can provide long term employment certainty.

QUESTIONS ON PRIVACY PROTECTION

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

Most obviously, data that hold personal identifying information create the greatest threat to privacy. It is for this reason that this class of data must be managed with the highest level of security both within the government and private sectors.

The separation principle and other security controls as utilised by SA NT DataLink for data linkage provide for a high level of privacy protection for the personal information it holds. While there can be a high level of confidence in the protection of privacy using this model for data linkage, privacy risks may be different for other data and data applications where personal information is voluntarily put in the public domain or required as part an agreement to use certain applications.

However, loss of privacy is an ongoing issue of concern. In the UK for instance, there are numerous examples of accidental and deliberate breaches of privacy or loss of sensitive information which suggest that the measures in place were not adequate.

Data breaches leading to loss of privacy (including in Australia), have involved areas such as financial information including credit card or bank details, immigration details, personal health information, personal information, trade secrets of corporations or intellectual property.

Because data breaches are may not be publicly reported or understated or causes not publically identified it is difficult to know what measures have been put in place as a result of these breaches.

The adequacy of data breach notification laws requiring an organisation that has been subject to a data breach to inform customers and to immediately take steps to remediate the situation should be considered. Perhaps a body such as the UK's Information Commissioner's Office, an independent authority set up to uphold information rights in the public interest, and which appears to more proactively promote openness and transparency by public bodies and data privacy for individuals, is a model to be considered that would augment the role of the Office of the Australian Information Commissioner.

Apart from personally identifying information (including addresses) other categories of data that may create concerns (generally described as sensitive information) should it become publically available include information about a person's:

- Criminal history
- Political affiliations
- Religious beliefs
- Sexual preferences
- Health history or status
- Financial history or status
- Protected identities

The implications and responses of revealing sensitive information may vary from person to person but generally there should be protections related to this information unless it is has been made public by the person or is already in the public domain. This also raises questions of the legal rights about persons who have died and legal remedy where the information is revealed without consent.

The above responds mainly about data that has been legally collected by agencies as part of the course of their business. Data that are captured as part of other consumer activity and then mined for commercial purposes can also reveal much about consumer behaviour and therefore information that may be considered as personal. While consent may be provided, there is room for argument as to whether it is properly informed and/or leveraged as part of the conditions of use for data products the consumer is wanting to acquire. How this area should be addressed is an area of law that requires careful consideration by those expert in this area, but should be done through public consultations.

How can individuals' and businesses' confidence and trust in the way data is used be maintained and enhanced?

Much of this has been addressed in previous responses, but in summary the key principles for building and maintaining trust are:

- Consumer need to be involved in decisions in relation to risks to individual privacy and that concerns are always properly considered and managed. Consumers should have a voice where decisions of privacy vs public good are made.
- Mandated requirements for the protection and use of data and appropriate sanctions where data are misused.
- The 'separation model' is a core best practice in the data linkage using health and human services data.
- Consumers should have greater levels of control over the data they provide and specifically how their data may be used.
- Robust security measures and protocols should be in place that protect the privacy of individuals.
- Models of transparency and openness in the use of the data and demonstrating public benefit where personal information is required. Transparency in reporting and accountability is also required.

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?

Much has been written about purported changing public attitudes towards privacy, with some viewing this as all but lost and therefore should not be valued as highly. However, the findings of the Wellcome Trust may contradict some of this view. In either case the nature of the information revealed or kept private needs to be considered.

The weight given to privacy protection relative to benefits is largely governed by the current public attitudes and commercial and political sensitivities and the value attributed to the benefits. It would not be unreasonable to suggest that private companies seek to

maximise the benefits of accessing and using data for their interests as much as permissible under law.

The security of privacy using the separation principle for data linkage supports a high level of confidence in the protection of privacy underpinned by this methodology. It therefore also supports positive public attitudes about the provision of data and its greater use, particularly for a public benefit.

As technological capabilities progress, the legal and policy frameworks governing privacy protection, if robust, should in principle, enable the management of privacy as technological capabilities and data availability increases.

While the technology required to ensure the principle of privacy protection can be maintained may keep pace with changing technological capabilities enabling data access, the implementation of the technology and protocols that protect privacy remains subject to the competence and willingness within an organisation to implement these.

More generally, there is increasing public discussion about current ethical and legal frameworks which are already significantly challenged and/or inadequate to deal with technological advances in for example areas such as genetics, pharmaceuticals, security and warfare. The same technological advances present significant privacy challenges and it is questionable how these will be managed especially as the perceived or claimed benefits may be strongly driven by the political and commercial priorities.

Are further changes to the privacy-related policy framework needed? What are these specific changes and how would they improve outcomes? Have such approaches been tried in other jurisdictions?

As has already been identified, there is no singular privacy related policy (or legislative) framework or authorising environment for approving and/or protecting data and privacy. The development of such would be of considerable benefit.

In relation to the above, considerable discussion about consumer privacy and data mining of consumer captured or provided information is required in the area of consumer law as to what may be required or desirable. Given the commercial value of this information, it would well be a contested area of legislation. More immediately, from SA NT DataLink's business perspective, what would be of greatest benefit are changes to Commonwealth government

While not directly part of the Productivity Commission's inquiry, some consideration should be given to intent where a breach is undertaken by a whistle blower and claimed to be in the public interest. The rights to legal protection for a whistle blower are well-recognised. The adequacy of legislation in regard to these rights is arguable and in more recent legislation denied, with significant penalties imposed. Much of this revolves around a debate of what is the public interest where this is interpreted as not meaning the same as the national (political/security/commercial) interest. For example, commercial interest may be argued by business to override public interest in the provision of certain information. *What the debates and legislations demonstrate is that the notion of public interest is always qualifiable*. Therefore, previous discussions using the public interest (or public benefit) as a policy justification must consider that public interest is not an unassailable principle where privacy of information (government or private) is concerned.

policies that currently unduly limit access individual record level Commonwealth data for linkage.

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

Coordination across jurisdictions requires sufficient high level cross government support for consistency in privacy legislation, data sharing and security. COAG would be the most useful body to support the processes required.

How effective are existing approaches to confidentialisation and data security in facilitating data sharing while protecting privacy?

As far as SA NT DataLink is aware, there have been no privacy breaches involving the PHRN and researchers which suggests that its technical security and privacy protecting procedures and protocols under which operates are effective in facilitating access and protecting privacy.

However, as discussed previously (p19) there are numerous examples in the government and private sectors that suggest that there are vulnerabilities in the existing approaches applied to other data management practices. It is important to note that an individual in a position of trust may almost always be able to circumvent privacy protecting measures should they have that intent. Again legislative protections and sanctions need to work to address these situations where they may not be justifiable.

What lessons from overseas jurisdictions can Australia learn from regarding the use of individuals' and businesses' data, particularly in regard to protecting privacy and commercially sensitive or commercially valuable information?

As mentioned previously, in the area of privacy protection there are a number of successful overseas models. In the Canadian model, there are unique personal health identifiers that are used for linkage and privacy protection. In addition to these, other countries (e.g. Denmark, USA) have unique universal personal identifiers that greatly simplify the processes for data linkage across a wide range of health and non-health data (much like the Australia Card proposed (but not established) in 1985 could have done). Greater access to and use the Medicare number could facilitate linkage, much in the way the personal health identifier does in the Canadian provinces.

What are the benefits and costs of allowing an individual to request deletion of personal information about themselves? In what circumstances and for what types of information should this apply?

This question in part goes back to the earlier one about who owns personal information. The answer to this will influence the responses and what may be required (e.g. enabling legislation). If a person does not own the information (e.g. their GP's medical records or information provided by the individual to other private companies) then such a request may be redundant. The capacity to review their information and request changes (e.g. credit assessment records) is however, considered extremely important. Again, the range of information where this can be requested would be circumscribed by other needs, (e.g.

government agencies such as law enforcement, justice, security).

Access to personal information and the right to amend this would be one of the important considerations in a privacy protecting regulatory framework to give confidence to the public about how their information may be used and which may provide for more accurate information when it is used. However, Parliaments have agreed that this is not an unfettered right and have circumscribed this under certain circumstances.

Company and commercial agreements may also restrict this right and require legislative amendments to ensure at least individual access to their information, where this is valued.

What competing interests (such as the public interest) or practical requirements would indicate that the ability to request deletion should not apply?

See above response and response p22.

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?

See previous responses relating privacy of information.

Is there need for a more uniform treatment of commercial-in-confidence data held by the Australian Government and state and territory governments?

While this may be question for government (and private) sectors, commercial in confidence should not be a blanket claim to disallow access to data that may have a public good value. Knowledge of commercial considerations may be important for understanding the value of government investments (utilising public monies) and the benefits derived from these.

Are there merits in codifying the treatment and classification of business data for privacy or security purposes? What would this mean in practice?

This may be best addressed by the relevant private and government sectors. However, any codification should also consider the above comments about not prohibiting legitimate scrutiny to ensure data has not been misused.

QUESTIONS ON DATA SECURITY

Are security measures for public sector data too prescriptive? Do they need to be more flexible to adapt to changing circumstances and technologies?

See previous comments about this area, but to summarise:

- Identifying information should be treated with very high and consistent standards for security, privacy protection and the circumstances under which it may be provided.
- It is important to distinguish between identifying data and de-identified or anonymised data when discussing data and privacy, but it must be recognised that all de-identified data is potentially re-identifiable. Hence de-identified data should also be treated with high levels of security and privacy protecting protocols and practices. As an example, geo-codes are de-identified but are re-identifiable data in many circumstances and especially when linked to other data. Therefore, the risks to privacy increase significantly, particularly as spatial data becomes more precise and more accessible and is a growing area of contention in the use of geo-codes.

Whether security measures are too prescriptive for public sector data would to some extent depend on the data being considered and also an individual's or organisation's values or interests; and whether from their perspective, the measures reasonably limit access to the data.

From SA NT DataLink experience in relation to accessing Commonwealth health and human services data, it appears that although SA NT DataLink is capable of meeting Commonwealth levels of security and privacy protection there exists a cultural and policy resistance to making data available for linkage to organisations outside of itself. While the Commonwealth appears to be developing some flexibility about this, the fundamental reluctance remains, with explanations in response to inquiries by SA NT DataLink based on the restatement of its criteria and policies.

While the Commonwealth is working with SA NT DataLink to make some of its data more readily available, by contemporary community standards which can see greater benefit in providing better accessibility, there does need to be a more adequate and flexible response in relation to the provision of Commonwealth information for data linkage purposes.

How do data security measures interact with the Privacy Act?

The Privacy Act offers a critical legislative and policy framework for the protection of privacy. However, because there are a number of exemptions to organisations that come under this Act it cannot provide for nationally uniform mandated protections.

The Privacy Principles central to the Act are also central to those organisations coming under the Act. However, it does not provide for more specific technical security, privacy protections and protocols for data linkage organisations which are required and for which nationally consistent standards would greatly assist in the provision of these services and support consumer confidence.

The Privacy Act provides the overarching legislative framework for privacy protection and drives the security measures to provide for this protection. All PHRN linkage capabilities,

including SA NT DataLink ensure that all measures for technical security and privacy protection are consistent with the Privacy Act, as well as meeting SA Government policy and agency requirements.

How other organisations security measures interact with the Privacy Act, SA NT DataLink is not able to assess and therefore comment.

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?

Breaches of privacy should in principle always be considered as serious. However, whether there has been some offense or harm physically, psychologically, financially and/or to a person's reputation needs to be ascertained. The severity of harm or offense would impact on the seriousness of the invasion and much of this may be decided by the courts under existing legislation. Whether new or amended legislation is required is a further question.

More generally, a data breach notification should be a necessary mandated response, but should not be considered as sufficient, since as discussed above, the right to redress is important, as is the need for reasonable penalties/sanctions against individuals and organisation that participate or enable a breach of privacy.

ATTACHMENT 1

BIG HEALTH DATA: AUSTRALIA'S BIG POTENTIAL

Recommendations of the

SENATE SELECT COMMITTEE INTO HEALTH SIXTH INTERIM REPORT

Recommendation 1

2.36 The committee recommends that Australia forms partnerships with other countries engaged in data linking to ensure that Australian data access and linkage policies and regulations are developed to world's best practice.

Recommendation 2

3.37 The committee recommends that the Department of Health, as a high priority, actively explore and then implement measures to advance cost-effective, evidence-based policy development through the use of data linkage.

Recommendation 3

3.38 The committee recommends that relevant government departments should include information in their annual reports which describes the processes and projects being undertaken to establish evidence-based policy based on data linkage as well as strategies they have adopted to contribute to the government's pubic data policy.

Recommendation 4

4.40 The committee recommends that given the changes in technology, and mindful of the capacity and moral obligation for governments to hold and strongly secure personal data and privacy, the government review the operation of section 135AA of the *National Health Act 1953*, with the aim of improving access to de-identified MBS and PBS data for the purpose of health policy evaluation and development as well as research undertaken in the public interest.

Recommendation 5

4.41 The committee recommends that the Australian Information Commissioner, in consultation with privacy advocates, data custodians, academics and healthcare consumers, review the *Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs* in order to ensure that the government:

- retains ownership and management of Australian MBS and PBS data and improves technological capacity to ensure the privacy of all Australians health data; and
- develops a strategy to improve access to de-identified MBS and PBS data for the purpose of health policy evaluation and development as well as research undertaken in the public interest, in ways that don't decrease privacy.

Recommendation 6

5.75 The committee recommends that each Australian Government agency develop and maintain on its website a list of datasets held by the agency along with the contact details of the data custodian. This list should be updated at least twice annually.

Recommendation 7

5.76 The committee recommends that all datasets held by the Commonwealth be listed on www.data.gov.au, identifying which agency is the data custodian.

Recommendation 8

5.77 The committee recommends that each Australian Government agency that is a data custodian develop and publish on its website guidance for researchers detailing its process for data requests and approvals.

Recommendation 9

5.80 The committee recommends that the government take a whole-of-government approach to streamlining the ethics approval process and the authorising environment in consultation with the Privacy Commissioner, privacy advocates, the NHMRC, data custodians, academics, consumers and the States and Territories. The government should also work with the States and Territories to establish a national accreditation system so that ethics approvals from accredited jurisdictions are recognised by the Commonwealth.

Recommendation 10

5.87 The committee recommends that relevant government agencies give greater priority to, and adequately resource their data custodians.

Recommendation 11

5.88 The committee recommends that relevant government agencies provide guidance to data custodians to assist them in their decision-making, with a view to making more de-identified data available on an enduring basis.

Recommendation 12

5.89 The committee recommends that the government adopt the Productivity Commission's proposed principle that open access to de-identified datasets should be the default position.

Recommendation 13

5.90 The committee recommends that the government should direct relevant agencies to release de-identified datasets on an enduring basis as the default position.

Recommendation 14

5.91 The committee recommends that departments that have data custodianship responsibilities must establish and publish realistic Key Performance Indicators for the timely consideration and approval of datasets requests. These departments must publicly report on their KPIs in their annual reports.

If after 5 years departments continue to delay the release of datasets, then the committee recommends that the government establish binding timeframes for processing applications for data. Failure to comply with the timeframe should trigger appeal rights similar to those found in other information access regimes.

Recommendation 15

5.93 The committee recommends that Government encourage collaboration on data linkage projects between government agencies, as well as academia and industry to provide for evidence-based policy development and facilitate research that is undertaken in the public interest.

Recommendation 16

5.98 The committee recommends that government consider accrediting State data linkage units to link Commonwealth data with State data collections, subject to comprehensive privacy and security protocols.

Recommendation 17

5.99 The committee recommends that the Government review the cost of data access and linkage work undertaken by Commonwealth entities with a view to facilitating research and innovation in the national interest.