office of the privacy commissioner
new south wales

Submission to the Productivity Commission Inquiry into Data Availability and Use

Issues Paper
July 2016

information and privacy commission nsw

office of the privacy commissioner
new south wales

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

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

Dear Mr Harris

Submission to the Productivity Commission's Inquiry into Data Availability and Use

Thank you for providing the opportunity to comment on the Productivity Commission's Inquiry into Data Availability and Use, which examines the cost and benefits of increasing the availability of public and private sector data for individual and organisational use.

The NSW Privacy Commissioner (OPC) is an independent statutory officeholder that administers NSW privacy legislation, including the *Privacy and Personal Information Protection Act 1998* (PPIPA) and the *Health Records and Information Privacy Act 2002* (HRIPA). The Office of the Privacy Commissioner plays a strategic role in promoting privacy compliance with NSW public sector agencies and private sector persons regulated under HRIPA.

The NSW Government has established a data analytics capacity for the NSW public sector and, separately, a number of initiatives in the open data field. Importantly in both of these initiatives, the NSW Government has recognised community expectations and legislative compliance requirements to ensure that personally identifying information of NSW citizens, including health information, is not disclosed unlawfully. For example, the NSW Open Data Policy provides a separate category of 'protected data'. Protected data includes, amongst other considerations, personal and health information. This distinction is not reflected in the Issues Paper released. This is an unfortunate gap which, if addressed, would be a significant progression facilitated by the Productivity Commission.

The other key point I make in relation to the Issues Paper is that an area which needs to be considered comprehensively is international alignment. It is disappointing that this very important aspect has received scant attention. Examination of the reports of the United Nations Special Rapporteur to Privacy will provide further guidance to the Productivity Commission in achieving international alignment with data obligations.

As the regulator of privacy in NSW, I have responded to a number of privacy concerns regarding the use of data by public sector agencies and private organisations. The Inquiry into Data Availability and Use provides an opportunity for the Productivity Commission to examine these issues in further detail and build a privacy respectful approach for data use which will have the trust and confidence of the public.

This submission is composed of the following parts:

1. a covering letter outlining the NSW approach and need for consideration of international developments;
2. discussion of the points raised by the Productivity Commissioner's Issues Paper; and
3. a summary of the critical points raised in relation to each of the Terms of Reference of the Inquiry.

Please find comments regarding the Issues Paper below. I request that the Productivity Commission redact my signature if this submission is made publically available.

Yours sincerely

Dr Elizabeth Coombs
NSW Privacy Commissioner

office of the privacy commissioner
new south wales

SUBMISSION TO THE INQUIRY INTO DATA AVAILABILITY AND USE ISSUES PAPER

I. Comments on the content of the Issues Paper

The Productivity Commission's Inquiry into Data Availability and Use provides an opportunity to discuss data availability and use by the public and private sectors. The shift towards a knowledge economy and the capacity to store and transmit large quantities of data has placed considerable demand for debate. The use of data for policy and planning purposes which respects citizens' concerns for their privacy has my support.

From a privacy perspective, the law and community expectations are that any datasets which contain personal or health information will be handled in accordance with privacy legislation. Under NSW privacy legislation, personal information held by public sector agencies can only be used for the purpose in which it was collected unless an exception applies. This is a legal requirement and the repurposing of personal or health information for uses not known to the individual could be a breach. Such provisions are the building blocks for trust which facilitate the development of accurate and complete data.

The release of public or private datasets which contain personal or health information for other uses to which consent or a choice is not provided is not supported. The Inquiry into Data Availability and Use must address these issues in order to maintain public confidence in increasing the use of data supplied by citizens.

Increasing the availability of data creates both risks and opportunities. A central theme of this submission is that the future of data sharing depends on embedding respect for individual privacy and privacy legislation, and the implementation of risk management strategies to address the potential risks to individual privacy associated with increased data availability.

The most effective approach for government and the private sector is a proactive 'privacy-by-design' approach which designs data availability and use, and privacy requirements, at the outset. Implementing preventative measures which remove privacy risks is more effective to containing costs, managing community expectation and realising the benefits than developing legislative exceptions. The community expects that exceptions, such as the exceptions listed under Part 2 Division 3 of PPIPA, only apply in extraordinary circumstances rather than the day-to-day operations of government and the private sector.

A balanced assessment of the claims supporting increased data availability

Increasing the availability of data has received considerable acclaim for its potential to drive innovation and economic growth. It is presented as an important resource as both public sector agencies and private organisations possess the technological capacity to harness high value datasets in order to develop new products, discover efficiencies and promote policy innovation.

Yet despite the number of benefits attributed towards big data, evidence for such claims is asserted rather than proven. There is a diversity of views as to whether data can deliver on its claims of economic growth and improved efficiencies for both public and private sectors.

Houghton, who was referenced by the Productivity Commission, noted:

> 'Some forms of PSI (public sector information) underpin major industries and contribute to their growth and prosperity. Other forms of PSI may have an important influence on policy decisions, but the economic impacts may be more limited or difficult to trace'.[1]

The view that the economic benefits associated with data are at risk of being overstated was also expressed by van Eechoud:

> 'A lack of hard data on the actual size of effects persists – or on the size of public sector information markets for that matter. Grand claims about the enormous benefits in terms of new products and services, growth in data driven jobs and efficiency savings in the public sector should therefore be taken with proper amounts of salt'.[2]

The OPC has been at the forefront of witnessing the ebb and flow of emerging technologies, and its varying levels of impact on individual privacy. As with any emerging technology, much caution must be exercised in giving weight to claims that greater availability and use of data presents a panacea for a lack of efficiency, innovation or economic growth across public and private sectors.

The Issues Paper notes that there are caveats to the benefits associated with data. However, the Issues Paper provides insufficient detail of these so that the reader can derive a balanced assessment as to the public benefit of data.

It is **recommended** that:

1. the Productivity Commission provides all evidence, including evidence which does not support the claims made for big data and open data, that was relied upon in its evaluation of the benefits associated increased data availability and use.

Recognition of privacy as a fundamental human right

Privacy is a fundamental human right. Although Australian privacy legislation concerns the regulation of personal and health information, the International Covenant on Civil and Political Rights (ICCPR) provides that:

> 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation'.[3]

Recent high profile cases, such as the NSA mass surveillance scandal, demonstrate that the failure to respect this personal privacy can result in a significant loss of public confidence in government, and moreover between governments. As data practices are underpinned by this confidence, it is vital that any proposed sharing of data respect personal privacy and work to take the community willingly along this path.

---

[1] J Houghton, *Costs and Benefits of Data Provision*, Report to the Australian National Data Service (Centre for Strategic Economic Studies, Victoria University, 2011) V.
[2] Mireille van Eechoud, 'Open data values: Calculating and monitoring the benefits of public sector information re-use' in T Drier et al, *Informationen der offentlichen Hand – Zugang und Nutzung* (Baden, 2016) 107, 140.
[3] *International Covenant on Civil and Political Rights*, 16 December 1966 [1980] ATS 23 (entered into force generally on 23 March 1976) Article 17.

Although no human right is absolute, the starting point to a privacy respectful approach is acknowledging the status of privacy as a fundamental human right. By doing so the Productivity Commission has an opportunity to build privacy by design approaches that can achieve concurrent goals of increased efficiencies, international alignment and a framework which facilitates broader societal, commercial and individual benefits.

It's unfortunate that the Issues Paper does not recognise the intrinsic value of an individual's right to privacy, and adopts a narrow interpretation of privacy as informational privacy. The Issues Paper also places the discussion of privacy issues as a cost associated with increasing the use of data, rather than an enabler.

It is **recommended** that:

2. the Draft Report addresses the impact of data on the ordinary meaning of privacy, not just informational privacy; and
3. the Draft Report develops this discussion in a separate chapter on privacy matters that is not a subsection of 'Managing the costs' associated with the greater availability of data.

Clarification of key terms used in the Issues Paper

The discussion of increased data availability and use relies upon the use of several key terms which require some level of technical knowledge. The Issues Paper supports this discussion by providing definitions under Box 1, which use language provided by both the Office of the Australian Information Commissioner (OAIC) and PricewaterhouseCoopers (PwC).

Despite the explanation of terms in Box 1, there is uncertainty towards the relationship between 'open data' and 'big data'. Although open data may be subject to data analytics used by big data, big data is not necessarily open data.

As 'open data' and 'big data' present their own distinct privacy challenges, further discussion on distinguishing the two concepts is vital in order to generate informed debate surrounding open data use in Australia. Currently, the UN Special Rapporteur on Privacy is investigating this distinction between these concepts.

It is **recommended** that:

4. the Productivity Commission provide further investigation towards the differences between open data and big data within the Draft Report and to do this with an eye towards international alignment.

The Issues Paper needs more precision when using the term 'open data'. It is not interchangeable with the term 'big data', nor is it clear whether this term contains personal or health information. It is also not clear whether the term open data refers to data that is de-identified, anonymous or aggregated to ensure that individuals cannot be identified or re-identified. This clarification is required as both personal and health information is subject to privacy legislation.

It is **recommended** that:

5. the Productivity Commission clarify that the usage of 'open data' explicitly exclude personal information or health information.

Finally, the Issues Paper recognises a concept of 'personal data'. According to the Issues Paper, personal data is data that:

> 'identifies, or could identify, someone such as their name, address, medical records, bank account details, photos, videos, personal preferences, opinions and occupation – essentially, any data by which someone may be reasonably identifiable'.

This definition closely resembles the definition of personal information provided under NSW privacy legislation. The concept of 'identifiability' is also used to distinguish personal and health information from data under Commonwealth privacy legislation.

Both personal and health information attracts additional statutory protections under privacy legislation which may not be apparent when using the term 'personal data' to the reader.

It is **recommended** that:

6. the Draft Report uses the term 'personal or health information' instead of 'personal data'.

II. Public sector data

Existing legislative framework protecting personal and health information in NSW

Data which contains personal or health information must be handled in accordance with privacy legislation. In NSW, the Information Protection Principles (IPPs) and the Health Privacy Principles (HPPs) provide the framework for the protection of personal and health information held by NSW public sector agencies.

One of the key challenges presented by data use which contains personal or health information is the assumption that information can be repurposed for a use or disclosure that is not permitted under privacy legislation. This repurposing may come in different forms, such as 'function creep' that occurs as a result of using data for a different function or context to which it was originally collected.[4]

Under PPIPA section 17, a public sector agency is prevented from using personal information for another secondary purpose unless the individual:

- consented to the use of the information for the secondary purpose;
- the secondary purpose was for a use that was directly related to the primary purpose for collection; or
- to prevent a serious or imminent threat to human life or health.

Under PPIPA section 18, a public sector agency cannot disclose an individual's personal information unless the disclosure was for:

- a directly related purpose for which the information was collected;
- the prevention of a serious or imminent threat to human life or health; or
- the individual concerned is reasonably likely to have been aware that the information of that kind is usually disclosed to the other body or person

[4] See B Custers et al, 'Big data and data reuse: A taxonomy of data reuse for balancing big data benefits and personal data protection' (2016) *International Data Privacy Law* 1, 5.

Similar protections on the use and disclosure of health information also apply under the HPPs.

In addition to the limitations to the use and disclosure of personal and health information, the IPPs and HPPs provide protections regarding how public sector agencies collect personal information. NSW privacy legislation requires public sector agencies (and private sector persons under HRIPA) to collect personal information directly from the individual unless it is unreasonable to do so.

The direct collection principle may also apply to collections between NSW public sector agencies. In *APV and APW v Department of Family and Community Services* [2015] NSWCATAD 140, the collection of drivers licence information by the Department of Family and Community Services was found to be a breach of the direct collection principle.

The collection of personal or health information without the individual's knowledge undermines privacy protections and denies citizens the control of their own identifying information and therefore prevents individuals from exercising their privacy rights. The direct collection principle provides an important protection to enable individuals to ascertain who is collecting their personal or health information, and provide an important transparency mechanism for government.

One of the core obligations for public sector agencies is to ensure that they check the accuracy of personal information before use. Under IPP 9:

> 'A public sector agency that holds personal information must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading.'

In this context, IPP and HPP 9 serves an important function to improve data quality for data analytics. If the fundamental data at individual level is incorrect or inaccurate, it may lead to a significant loss of quality in data analysis and will reduce the benefits associated with increased data availability. Privacy law also allows correction of inaccurate information which serves as an important protection.

Exceptions to the restriction on the use or disclosure of personal and health information

In NSW, the IPPs and HPPs contain exceptions which allow NSW public sector agencies to use or disclose personal or health information in certain circumstances which would otherwise not comply with an IPP or HPP.

These exemptions include activities which relate to law enforcement, the performance of agency's investigative functions, where non-compliance is authorised by law or to engage in research activities. In terms of research activities, a similar exception is also provided under the Commonwealth *Privacy Act 1988* section 16B(3) in relation to health information.

However, any use or disclosure of personal or health information which can reasonably identify an individual cannot be published in a publically available publication, including datasets. This is an important safeguard as the publication of personal or health information for research can be highly prejudicial to the individual and in the case of health information, potentially to biologically related family members.

Any use or disclosure of personal information or health information for a research purpose also requires compliance with the PPIPA or HRIPA Statutory Guidelines on Research. Under these Guidelines, a research proposal that uses personal or health information requires approval from a Human Research Ethics Committee (HREC).

De-identifying personal information during a research activity remains an important activity in order to safeguard individual privacy. In the context of the application of the research exemption to data, the process of de-identification for a research activity does not, in itself, constitute research. Further information regarding the de-identification process when undertaking research can be found under our PPIPA and HRIPA Statutory Guidelines on Research.

Use of information access legislation to enable data transfers between public sector agencies and non-natural persons

Information access legislation, including the *Government Information (Public Access) Act 2009* (GIPA Act) provides a mechanism to enable members of the public to access government information where it is in the public interest to do so. The GIPA Act does not provide a mechanism to facilitate data sharing between public sector agencies.

There is some uncertainty regarding the application of information access legislation to facilitate the release of public sector data to non-natural persons. This includes other government agencies (such as Commonwealth and state governments) and private organisations. This uncertainty is based on concerns whether the use of GIPA access orders can be used as a mechanism to facilitate open data requests, and the application of processing charges to non-natural persons to facilitate cost recovery associated with such a request.

III. Private sector data

Unlike the Commonwealth *Privacy Act*, PPIPA only applies to public sector agencies in NSW although reserve powers enable the Productivity Commissioner to investigate, research and report on any privacy related matters. Under PPIPA section 4(4), personal information is also considered to also be held by a public sector agency if the personal information is under the possession or control of a person employed or engaged by the agency, such as contractors and non-government organisations.

My powers to issue Public Interest Directions or Codes of Practice – which can allow an entity to be exempt or alter the application of an IPP and HPP – can only apply to a public sector agency, and not a person or body employed or engaged by an agency.

Under HRIPA, private sector persons who provide health services or hold health information are regulated by the HPPs. This places private sector health service providers and organisations over a certain size that hold health information under both NSW and Commonwealth health privacy law.

As previously noted, both HRIPA and the *Privacy Act 1988* contain provisions which allow the use or disclosure of health information for research purposes where it is impracticable to obtain consent or de-identify the information. The definition of personal information which includes information relating to deceased individuals is an important distinction between Commonwealth and NSW privacy legislation which can provide greater utility to citizens.

IV. Consumer access to, and control over, data and managing the costs of open data

Under the IPP 7 and HPP 7, individuals have the right to seek access to their personal or health information, without excessive delay or expense, from a public sector agency. This applies to any personal or health information, regardless of whether the personal or health information is contained in a dataset or not. This is a very important right particularly as it is complemented by the provision enabling correction of inaccurate information. This is not provided by any other NSW law such as the GIPA Act or the *State Records Act 1998*, which also provide access to personal or health information.

Supporting the right of access is the limitation to how public sector agencies may use or disclose personal or health information. Public sector agencies cannot use or disclose an individual's personal or health information unless they have obtained their informed consent, or an exception applies. Both the rights to access personal and health information, and the restrictions in how such information is used or disclosed, are central features of NSW privacy legislation to enable individuals to retain control over who accesses their personal and health information and what that information accurately presents.

The most effective means to enable the expression of access, use and disclosure rights is to embed consumer data control mechanisms into data design protocols. This privacy by design approach creates a framework to enable timely access by the individual and thus build public confidence that data practices accord with community expectations towards privacy.

V. Managing the costs – privacy and data security

The premise that privacy protections impose a barrier to greater data availability and use is not supported by information handling practice. Data quality and the use of legacy systems remains a significant barrier for greater data exchange. Cai et al identifies that the diversity of data sources and difficulties and difficulties associated with integration, and the vast volume of data which restricts the ability to perform quality control prevents the increased adoption of data analytics.[5]

The existence of government silos and the lack of service coordination also present significant barriers to the adoption of effective information sharing arrangements. The NSW Standing Committee on Social Issues, which examined service coordination, noted the existence of silos as 'exacerbating difficulties' for information sharing and data collection.[6] The Committee also reported that a lack of understanding of regulatory requirements regarding information sharing also contributes to an 'organisational aversion' from effective information sharing arrangements.[7]

These issues present the most significant barriers to increased data availability and use. The Issues Paper does not give adequate weight to these concerns. By placing too much emphasis on privacy as restricting data sharing, rather than enabling, these issues remain obscured from informed debate.

Advances in technology have changed the threat environment in data security. According to the McAfee Labs Threat Assessment Report 2015, there has been a monumental increase in the number of major data breaches and the volume of records stolen in the last 10 years.[8] The increase accessibility of public

[5] Li Cai and Yangyong Zhu, 'The Challenges of Data Quality and Data Quality Assessment in the Big Data Era' (2015) 14 *Data Science Journal* 2, 2-3.
[6] NSW Standing Committee on Social Issues, *Service coordination in communities with high social needs* (NSW Government, Report 50, December 2015) 15.
[7] Ibid, 39.
[8] McAfee, *McAfee Labs Threat Assessment Report* (Intel, August 2015). See http://www.mcafee.com/au/security-awareness/articles/mcafee-labs-threats-report-aug-2015.aspx

and private sector data increases the risk of a data breach, be it as a result of a malicious attack or an accidental disclosure of personal or health information.

Privacy enhancing technology provides a critical role in identifying the risks associated with increased data availability and use. Advances in de-identification, the use of synthetic data and anonymization provide an opportunity to not only prevent privacy breaches, but also reduce the impact of a breach in the event that a breach does occur.

Recent high profile data breaches illustrate the potential impact of embedding privacy enhancing technology into information system design. In the 2011 Catch of the Day (COTD) data breach,[9] customer data, including financial information, was stolen by malicious hackers. The breach was compounded as COTD did not build financial infrastructure that was compliant with the Payment Card Industry Data Security Standards (PCI-DSS), which allows online payments through an authenticated third party. As a result, COTD customers were required to replace their credit cards and change their passwords.

The COTD data breach demonstrates that the benefits of privacy enhancing technology, and used within an appropriate risk management framework. Risk management, such as implementing privacy by design, represents the best form of managing privacy concerns associated with data.

Tools such as Privacy Impact Assessments (PIAs) have been extensively used by public and private organisations in managing privacy risks. A PIA is a systematic assessment of a project which identifies the impact that the project may have on the privacy of individuals and sets out a process or recommendations in addressing this risk.

PIAs are more than a 'compliance check' against privacy legislation. Critically, PIAs allow data custodians to gain an insight into information flows within their organisation, demonstrate corporate responsibility and provide the community with the confidence that a proposed project accords with community expectations towards privacy and appropriate information management.

It is **recommended** that:

7. the Draft Report examine how privacy by design, including the use of Privacy Impact Assessments, must be used by data custodians before releasing public or private datasets

Although data custodians are responsible for ensuring that personal and health information is handled in accordance with privacy legislation, end users of data play a key role in mitigating the risks associated with a data breach.

Mandatory data breach notification ensures that this risk is mitigated by notifying relevant parties that a data breach has occurred. By notifying the data custodian, the data custodian can undertake appropriate measures to address and contain the data breach, and implement appropriate measures to ensure that a breach does not reoccur.

[9] See OAIC, 'Catch of the Day data breach' (OAIC, 2015) https://www.oaic.gov.au/media-and-speeches/statements/catch-of-the-day-data-breach

In addition, data breach notification allows individuals to take appropriate steps to minimise the impact of a data breach. By informing individuals, in appropriate circumstances, that a data breach has occurred, individuals can request the issuance of new identifiers or change their security settings (such as passwords) with the data custodian.

It is **recommended** that**:**

8. the Draft Report supports the implementation of a mandatory data breach notification scheme.

office of the privacy commissioner
new south wales

SUMMARY OF KEY ISSUES AND RECOMMENDATIONS

I General comments

Key Issues

The Issues Paper raises general concerns regarding the:

A.1 critical assessment towards the benefits associated with increasing data availability and use;

A.2 recognition of privacy as a fundamental human right; and

A.3 clarification of key terms used by the Issues Paper.

Recommendations

That the Productivity Commission:

1. provides all evidence, including evidence which does not support the claims made for big data and open data, that was relied upon in its evaluation of the benefits associated increased data availability and use.

2. addresses the impact of data on the ordinary meaning of privacy, not just informational privacy;

3. develops a discussion on the human rights dimensions in a separate chapter on privacy matters that is not a subsection of 'Managing the costs' associated with the greater availability of data;

4. provide further investigation towards the differences between open data and big data within the Draft Report and to do this with an eye towards international alignment;

5. clarify that the usage of 'open data' is to explicitly exclude personal information or health information; and

6. uses the term 'personal or health information' instead of 'personal data' in the Draft Report.

II Public sector data

1. *Examine the benefits and costs of options for increasing availability of public sector data to other public sector agencies (including between the different levels of government), the private sector, research sector, academics and the community. Where there are clear benefits, recommend ways to increase and improve data linking and availability. The Commission should:*

   a) *identify the characteristics and provide examples of public sector datasets that would provide high value to the public sector, research sector, academics and the community to assist public sector agencies to identify their most valuable data; and*

   b) *examine legislation or other impediments that may unnecessarily restrict the availability and linking of data, including where the costs are substantial, and consider options to reduce or remove those impediments.*

Key Issues

Data which contains personal or health information held by NSW public sector agencies must be handled in accordance with privacy legislation. Increasing data availability and use raises concerns regarding the:

1.1. repurposing of personal or health information for a purpose not permitted under NSW privacy legislation;

1.2. compliance with the direct collection principle;

1.3. accuracy of personal or health information;

1.4. application of the research exemption under PPIPA and HRIPA, including compliance with Research Guidelines; and

1.5. use of information access legislation to enable data transfers between public sector agencies and non-natural persons.

III Private sector data

2. *Examine the benefits and costs of options for increasing availability of private sector data for other private sector firms, the public sector, the research sector, academics and the community. Where there are clear benefits, consider ways to increase and improve availability. The Commission should:*

   a) identify the characteristics and provide examples of private sector datasets that would provide high value to the private sector, public sector, the research sector, academics and the community in developing or providing products and services, undertaking research and developing policy;

   b) identify the concerns of private sector data owners and provide recommendations on principles or protocols to manage these concerns;

   c) examine legislation or other impediments that unnecessarily restrict the availability of data, including where the costs are substantial, and consider options to reduce or remove those impediments; and

   d) provide an update on existing data sharing initiatives in Australia, including the uptake of the credit reporting framework. Consider recommendations for improving participation in such initiatives.

Key Issues

Increasing data availability and use of private sector data raises concerns regarding the:

2.1 application of NSW privacy legislation to private sector entities, specifically the distinction of 'personal information' under Commonwealth and NSW privacy legislation; and

2.2 application of Public Interest Directions or Privacy Codes of Practice to facilitate increased data availability and use with private sector entities.

IV Consumers' access to and control over data about them

3. *Identify options to improve individuals' access to public and private sector data about themselves and examine the benefits and costs of those options. The Commission should:*

   a) *examine how individuals can currently access their data, including data about them held by multiple government agencies, and develop recommendations to streamline access;*

   b) *identify datasets, including datasets of aggregated data on consumer outcomes at the product or provider level, that would provide high value to consumers in making informed decisions and any impediments to their use. Develop guidance to assist in identification of other high value datasets; and*

   c) *examine the possible role of third party intermediaries to assist consumers in making use of their data.*

Key Issues

Under privacy legislation, consumers have a right to access their personal or health information. Increasing consumer access and control over data raises concerns regarding:

3.1 preserving rights to access of personal and health information;

3.2 obligations which limit how personal or health information is used or disclosed; and

3.3 embedding consumer access control mechanisms into data system design.

Standardising the collection of datasets

4. *Examine the options for, and benefits and costs of, standardising the collection, sharing and release of public and private sector data.*

Key Issues

The OPC does not raise any key concerns in relation to Term of Reference 4 at this stage.

V Managing the costs

5. *Examine ways to enhance and maintain individuals' and businesses' confidence and trust in the way data are used. Having regard to current legislation and practice, advise on the need for further protocols to facilitate disclosure and use of data about individuals and businesses while protecting privacy and commercial interests and, if recommended, advise on what these should be. The Commission should:*

   a) *balance the benefits of greater disclosure and use of data with protecting the privacy of the individual and providing sufficient control to individuals as to who has their information and how it can be used;*

   b) *benchmark Australia's data protection laws, privacy principles and protocols against leading jurisdictions;*

c) *examine whether there is adequate understanding across government about what data can be made openly available given existing legislation;*

d) *consider the effectiveness and impacts of existing approaches to confidentialisation and data security in facilitating data sharing and linking while protecting privacy; and*

e) *consider the merits of codifying the treatment and classification of business data.*

Key Issues

Individuals and business confidence and trust in increasing data availability and use raise issues regarding the:

5.1 role of privacy enhancing technology in facilitating increased data availability;

5.2 use of risk management strategies, such as privacy by design;

5.3 utilisation of tools such as Privacy Impact Assessments to support risk management strategies;

5.4 role of mandatory data breach notification in protecting individual privacy and mitigating risk to individual privacy; and

5.5 other information handling issues, such as data quality and a lack of understanding of regulatory requirements, which also impact on greater data availability and use.

Recommendations

That the Productivity Commission:

7. examine how privacy by design, including the use of Privacy Impact Assessments, must be used by data custodians before releasing public or private datasets; and
8. supports the implementation of a mandatory data breach notification scheme.