The quest for greater data availability and use in Australia

28 June 2017

Sylvia Ng, Steph Baker, Cameron O'Sullivan, Rohan Shukla, Priyanka Vennelakanti

In brief

The Australian Federal Government recently released the Productivity Commission's (Commission) much anticipated final report on *Data Availability and Use* (Report), which analysed the benefits and costs of increasing the availability and use of data in Australia across the private and public sectors.

The Commission's recommendations seek to transform Australia's current risk-averse regulatory frameworks and protections for data collection and use to realise the value of data in today's digitised society. The Report recommends comprehensive reform of Australia's data infrastructure (including legal, policy, and cultural components) with the goal of building public confidence and trust in data use, and foster community perceptions of data as an asset rather than a threat. It explains that a shared understanding of the costs, risks, and benefits associated with data is the key to driving commercial value and potential innovations. It also seeks to uplift Australia against comparable jurisdictions in terms of open data policies and skills, and to capitalise on the rapid growth of data generation and usability.

If fully adopted, the recommended framework for open and transparent data sharing and management in Australia will require legislative and structural support, and include the following key reforms:

- a new Commonwealth *Data Sharing and Release Act* (DSR Act) to govern data access, sharing and release, and establish a new statutory office holder, the Office of the National Data Custodian (NDC), to guide and monitor the new data system,
- creation of a new 'Comprehensive Right' giving consumers (including both individuals and small-medium businesses) greater control over their own digital data through increased access and transferability, and
- creation of a scalable, risk-based institutional regime for data sharing and release, thereby recognising the different risks and benefits associated with different data sets, uses and environments across the public and private sectors. This would involve the establishment of Accredited Release Authorities (ARAs) as independent entities within particular sectors to oversee the curating, linking, sharing and releasing of data across and between sectors.

In this paper, we summarise the Commission's key findings and evaluate potential implications of the Commission's recommendations.

In detail

Australia's data regulatory framework

The Report identifies that Australia's complex, piecemeal privacy law regime as a contributor to Australia's risk-averse approach to data usage. Financial penalties, reputational damage, combined with confusion about the scope and applicability of State and Federal laws (particularly in the case of third party data transfers), has led to Australian governments, public and private sector entities, and individuals to err on the side of caution when dealing with data (even if de-identified).

The Commission recommended an ambitious and realistic timeline to reform, in order to adequately address the issues identified. It identified certain matters (such as collation of public data set registers) which should commence immediately, through to 2020 for matters which can reasonably be expected to take greater time to implement. We set out a summary of this timeline at Attachment A**.**

A new regulatory framework

Australian data framework

The Commission's key regulatory recommendation is the implementation of an overarching data regulatory framework (Framework), including the introduction of a new, technology-neutral DSR Act intended to complement the existing *Privacy Act 1988* (Cth), State-based legislation (which would continue to apply), and community consultations.

The DSR Act aims to clarify regulation over data sharing, access and risk management, and will:

- establish a 'Comprehensive Right' of consumers to access and control their data (see below),
- empower a new, independent statutory office holder within the Commonwealth portfolio, the Office of the NDC, with responsibility for changes to data risk management, accreditation of ARAs and the issuing of guidance including as to best practice for sharing non-sensitive public sector data sets;
- establish ARAs (which could be existing suitable organisations, or new organisations, accredited by the NDC), under the NDC, with power to share or release certain public sector data sets, provided privacy safeguards are sufficiently applies to the data set (to the extent possible, in compliance with the Privacy Act); and
- prescribe that non-sensitive data held by agencies and ARAs should be explicitly presumed to be made public, subject to guidance issued by the NDC, with risk-based provision of data to trusted users in a secure environment and subject to the five safes principles.

A detailed description of the proposed new regulatory bodies is set out at Attachment B. In addition to these new regulators, the Commission recommended greater involvement of the Australian Competition and Consumer Commission (ACCC), Ombudsmen and other relevant agencies. Whilst separate bodies responsible for data release, information privacy and consumer protection might create complexity, the Commission recommended that the bodies cooperate so that there is 'no wrong door' for individuals where they have privacy concerns.

NIDs

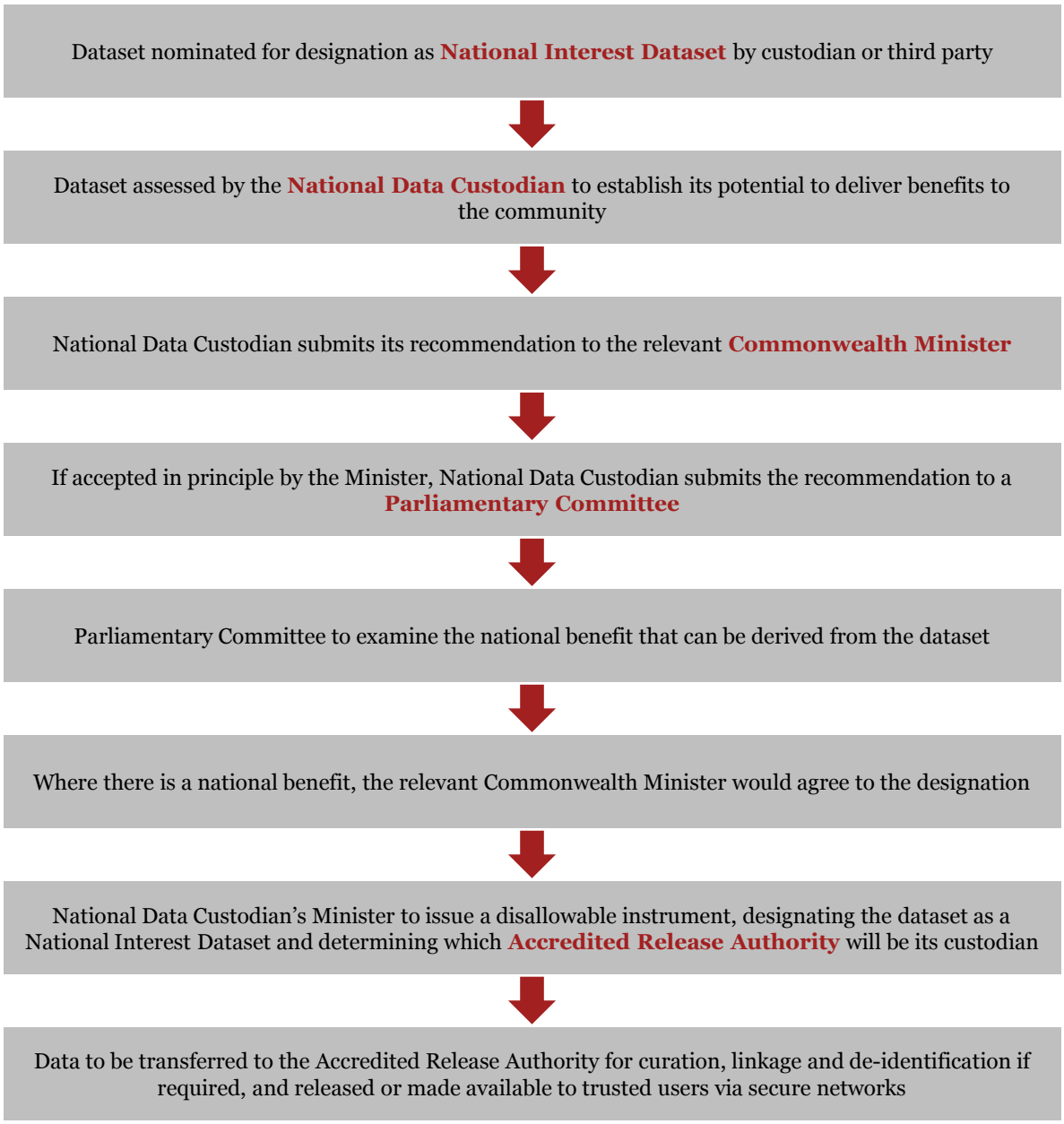
Figure 1 below illustrates how a dataset of significant national value would become designated as a National Interest Dataset (NID) and be released (or shared). The Commission recommended that this designation process be public whereby any third party may submit a nomination to the NDC, and then the NDC, Ministers and Parliamentary Committee would analyse each proposal.

Trusted data users

The Commission indicates that the Framework should incorporate a 'trusted user' model whereby ARAs assess and allow certain trusted users to access and use sensitive and/or identifiable data, on the basis of processes set by the NDC. ARAs would assess an entity's corporate governance structures and risk management processes, and whether the trusted user has signed a legal undertaking in respect of data safeguard and privacy obligations.

There appear to be tremendous opportunities for trusted users once datasets are nominated as NIDs (which may, for example, include credit reporting data, data on natural hazards, hospitals data, data on the Medicare Benefits Schedule and Administrative data such as drivers' licences).[1] Allowing only trusted users to access such data sets (if they are identifiable) will help maintain trust in society and ease related fears of 'big data'.

Figure 1: *Process to designate a NID*



[1] Productivity Commission 2017, *Data Availability and Use, Inquiry Report*, p. 286.

Policy amendments

The Commission identified that risk classifications on public sector data sets (at Commonwealth and State level) to be released would help define who should be allowed access to those data sets. For example, data with a low risk rating – e.g. which had been securely de-identified – could be released publicly, whereas data with a higher risk rating should only be available to trusted researchers in a secure environment and with monitoring and checks to ensure its security. The classifications should form part of existing policies[2] and acknowledge the processing of data – such as de-identification – can reduce its risk rating.

Government agencies should adopt data management standards and the private sector is encouraged to determine its own data sharing standards in line with this framework. Should cooperating with the framework fail to come about organically, the Commission encouraged the government to facilitate it through regulation or the ACCC's powers where failure may impact on the Comprehensive Right of consumers.

There is a clear need for cooperation between the Federal, State and Territory parties to develop a coordinated approach to data availability and use Australia-wide.

Community engagement and culture

The Commission emphasised the need for community engagement and education about the framework once implemented, to facilitate community trust and a culture that embraces the opportunity of sharing. Suggestions include the establishment of a National Data Advisory and Consultative Forum (including non-government experts that advise on public interest data needs, technology, governance and release authorities), community advocates and online engagement.

Potential implications

The DSR Act is intended to be an enduring, technology-neutral and principles-based statute, viewing data through a usability lens with the goal of overcoming current problems with data sharing and use, particularly in the public sector. The goal is honourable and certainly in line with the current need to improve data sharing in Australia whilst facilitating community trust in data usage.

However, the proposed framework risks contributing to an already complex regulatory web, because:

a) **The Framework does not address the problems caused by the Federal system:** It is widely recognised that the Federal system causes regulatory problems in the context of privacy law, causing legislation to be piecemeal. With data and privacy a State residual power under the Australian Constitution, the DSR Act will draw on the full extent of the Commonwealth's Constitutional powers - and States will need to opt-in to the legislation. The introduction of a new law without addressing the existing regulatory complexity may be challenging. Further, Federal-State cooperation is essential to the success of the Framework on a broader scale, and a strategy to achieve this must be determined.

b) **Number of regulators:** The Framework proposes the introduction of several new regulatory bodies. Importantly, appointing subject matter and jurisdictional or sectoral experts could aid the acceptance of the new Framework. However, the NDC and ARAs will not sit under the Office of the Australian Information Commissioner (OAIC), and it is not clear which ministerial portfolio will have responsibility for the new regulatory bodies (it appears, at first instance, that the Department of Prime Minister and Cabinet will have responsibility).

c) **The need for regulatory guidance:** Some elements of the Framework, for example, indication of what constitutes 'non-sensitive data' which is presumed to be available, are not presently clear and the NDC will need to issue regulatory guidance to improve stakeholders' understanding.

d) ***Red tape:*** The 2015 Belcher Red Tape Review (commissioned by the Commonwealth Department of Finance and the Secretaries Board in 2015) found key themes of over regulation and a culture of risk

[2] Such as the Federal Government's Protective Security Policy Framework, which is aimed at providing policy, guidance and better practice insights for governance, human capital, physical and information security.

aversion throughout government. It recommended taking steps to reduce the over-classification of information as a method of removing governmental red tape. The proposed Framework appears contradictory to this recommendation, adding layers of regulation and approvals to data access. Whilst this is intended to balance the needs for access and privacy, the Federal Government will need to evaluate the costs and benefits, including as applicable to red tape reduction, should it choose to implement the proposed Framework.

e) ***Unclear application to the private sector:*** Due to the split of some services across public and private sectors and the privatisation of others, the Commission maintains that some private sector datasets would need to be included within NIDs. This could lead to uncertainty over how NIDs may interfere with intellectual property rights or commercially sensitive information. The Commission has suggested the NDC consider paying the private sector for access or linkage, which is intended to provide some comfort. It further recommends that before designation as a NID, analysis should clearly note how the designation will deal with commercial sensitivity associated with information and costs.

Competition and consumer protection framework

The Commission identified that, despite rapid data production, increasingly sophisticated data analytics technologies and potential for data-derived innovations, individual consumers have few rights to the data about them and that economic opportunities derived from data often fail to reach the individual consumer. Consumers don't 'own' their data, and typically cannot authorise its transfer to third parties. Often, consumers aren't even aware of what data about them a firm or agency may possess.

This is overlaid with competition concerns - with asymmetric data availability in industries creating barriers to entry for new market participants and a lack of interoperability of technologies. These factors can create market inefficiencies and disincentivise competition and innovation.

Introduction of a consumer Comprehensive Right to data

One of the Commission's most significant proposals is to introduce a new 'Comprehensive Right' designed to give consumers greater control over data about them by amalgamating five distinct rights (some of which are currently recognised under privacy law, to the extent that the data would constitute personal information), being:

a) A right to access a copy of data which has been:
   i. provided directly by the consumer,
   ii. collected in the course of other actions (and including administrative datasets) and identifiable to that consumer (whether aggregated or not),
   iii. held by the data holder even though created by others – e.g. through screen-scraping or tracking, purchase of data about a consumer, or re-identification,

b) A right to request edits or corrections to data for reasons of accuracy,

c) A right to request a transfer of data held by an organisation about the consumer, in machine-readable form, to the consumer or to a nominated third party (the Transfer Right),

d) A right to be informed about the trade of any element of this data to third parties (the Disclosure Right), and

e) A right to be advised of disclosures of data to third parties (the Trading Notification Right).

Implementation

The Comprehensive Right will be a matter for Parliament to legislate and would cover both public and private sector data, and apply to 'consumers' (being single persons, family groups or other groups resident at a single address in the data holder's dataset, and any entity with an Australian Business Number and turnover of $3 million or less per annum). There would be no opt out rights, nor the right to appeal

automated decisions (although, consumers could still query the accuracy of data upon which a decision was based).

Scope of consumer data

For the Comprehensive Right to be effective, the scope of 'consumer data' must be clarified. The Commission envisages that industry participants will have the flexibility to negotiate a data-specification agreement, registrable with the ACCC, determining the scope of consumer data relevant to that industry; where no such agreement is reached, then a default definition provided by the Commission will apply.

The Commission's aim is to provide a broad default definition focused on the outcome of enabling consumers to access competing or complementary services or products, to help spur competition and innovation. Accordingly, the Commission proposes the following scope: consumer data is digital data, provided in machine-readable format, which is:

a) held by a product or service provider,

b) identified with a consumer, and

c) associated with a product or service provided to that consumer.

'Consumer data' will encapsulate personal information under the Privacy Act, information posted online by the consumer, data created by the consumer's online transactions and activities, and data purchased from a third party about the consumer. Importantly, imputed data (proprietary to the data holder, such as risk metrics based on raw data about the individual) and data collected for regulatory enforcement are excluded from being 'consumer data'.

Whilst 'consumer data' is broader than 'personal information' under the Privacy Act, there is clearly cross-over. Again, this raises concerns about regulation complexity.

The Transfer Right

The Transfer Right represents the most significant proposed legal and consumer development, and will likely form the bulk of increased compliance costs. The Transfer Right allows consumers to request that data held about them at the particular point in time of the request, be transferred to themselves or a third party. The application for transfer would be subject to a fee. In contrast to the United Kingdom, where consumers can request a transfer of data up to one year after creation, there is no time limit upon the proposed Australian Transfer Right: it would apply to all data that is reasonably accessible to the data holder of record (regardless of whether they hold it off-site or on restricted terms).

A key transfer concern is the interoperability of data, so as to ensure efficient access and transfer with minimal friction costs. Despite this, the Commission rejected suggestions in some submissions to implement application programming interfaces (APIs, which are sets of routines and tools specifying how software components should interact); concluding that so long as data is transferred in a machine-readable form, industry should be free to determine *how* it is transferred.[3]

The Transfer Right was particularly controversial in submissions, and there are enduring concerns in relation to:

a) liability - where inaccurate data is transferred to third parties who suffer subsequent financial loss,

b) data security risks during- or post-transfer, and

c) exploitation of consumers that are unaware of the risks of sharing data with different parties.

Risk allocation and liability in such circumstances are unclear. The Commission suggested third party accreditation to promote security, however this has the downside of further increasing barriers to market.

[3] Productivity Commission 2017, *Data Availability and Use, Inquiry Report*, pp. 224.

The Commission also dismissed concerns raised regarding the cost of compliance finding that compliance would not be costly where firms have access processes in place under the existing privacy law.

Disclosure and Trading Notification Rights

The Commission recommended implementation of Disclosure and Trading Notification Rights as follows:

a) all holders of consumer data should include in their privacy policies, terms and conditions, or on their websites a list of parties to whom consumer data has been traded or otherwise disclosed over the past 12 months, and

b) on the windup of an entity that holds consumer data, consumers should be informed if data to which they hold joint rights has been traded or transferred to another entity.

The intention is to provide consumers with greater information about where their data goes, without imposing a significant compliance burden (i.e. organisations are not required to notify consumers upon each instance of disclosure or trade). What remains unclear is the extent and frequency with which such notifications or disclosures should be made (e.g. annually). Insolvency practitioners will also need to be aware of the updated data notification requirements in the context of windups.

The Commission recommended that best practices for disclosure should not be legislated, but allowed to develop organically on a business-by-business and industry-by-industry basis.

Regulatory oversight

Interestingly, the Commission was of the view that the ACCC, and not the OAIC, should be the key regulator in the context of the Comprehensive Right, with power to 'name and shame' non-compliant entities. Specifically, the ACCC would be responsible for:

a) approving and registering industry data-specification agreements and standards,

b) handling consumer complaints,

c) educating consumers, and

d) monitoring the validity of fees charged for transfer requests.

Comprehensive credit reporting

Comprehensive credit reporting (CCR) is a voluntary system of credit reporting that, in contrast to negative credit reporting, provides more details than simply negative spots on a credit history with the goal of providing a more balanced assessment of a borrower's credit risk. The Commission identified the value of the voluntary CCR regime and recommended that, if sector participation is less than 40 per cent of active credit accounts provided by ASIC-licenced credit providers by 30 June 2017, government should legislate for mandatory CCR participation.

Transformation and pricing of data

The transformation of data beyond raw form into more sophisticated products, and sharing or applying transformed data with others, continues to create opportunities for structural change and innovation both within firms and within industries. A key component of a competitive market is pricing and, typically, private sector entities identify a purpose for the data, value it, and make business decisions in relation to transformation and pricing. This is more challenging in the public sector, where data presents significant opportunities but valuation is difficult and transformation costly.

Transformation of public sector data

There is an inherent tension between the timeliness of data release and the transformation of data. In distinguishing between basic data and transformed data (see Figure 2 below), the Commission recommended that public sector agencies should release basic data in a timely manner, and only look to transform data in limited circumstances.

Figure 2: Basic and transformed data[4]

Basic Data	Transformed Data
Data to which an agency has undertaken minimal level of curating or processing to make the data fit for sharing or release	Data to which an agency has undertaken more extensive curating or processing effort, often with the purpose of targeting the data at a specific set of users, rather than general release.

Government agencies should focus on efficient release of basic data. The data should be machine-readable, readily linkable, understandable and de-identified (unless the data set is already publicly accessible in identifiable form).

Ordinarily, the incentive for an agency to transform data is outweighed by the cost of doing so, with the private sector better placed to identify, execute, and distribute valuable data transformation. The Commission suggests that the public sector should only transform data prior to release in two circumstances:

Pricing of public sector data

Pricing considerations of public sector data are different to those of the private sector. For instance, agencies can be incentivised by public interest benefits that that do not directly provide a return to the agency. The Commission assessed three pricing structures: cost recovery, marginal cost pricing and commercial pricing.

Ultimately, the Commission determined that basic data release should be marginally costed or free, so to maximise the opportunity for direct and spillover effects. However, it is noted this recommendation, if implemented, will result in little agency revenue. There is potential to increase price where a public sector agency has engaged in value added transformation of data, but the Commission noted any price adopted should not undermine the public interest of release.

Funding for public sector data release

The Commission recommended no additional funding be provided to agencies to release data, except:

[4] For further detail, see: Productivity Commission 2017, Data Availability and Use, Inquiry Report, pp. 345.

a) where a dataset held by a public sector agency is determined to be of high value with a strong public interest,

b) for the NDC, for functions undertaken by ARAs and, in some cases, for the purchase and ongoing maintenance of NIDs, and

c) for the ACCC, to cover their new data regulation responsibilities.

The Commission recommended an independent review on the pricing of public sector datasets for public interest research purposes.

Transformation and sale of private sector data

To accommodate innovative business models (particularly for new entrants), the Commission recommended the enforcement of existing regulatory arrangements with a 'technology neutral'[5] approach. There were no detailed recommendations or findings with respect to the private sector. However, the Commission recommended the Australian Government make provision, in select circumstances as approved by the funding Minister, for the NDC to pay for access or linkage to private sector datasets, especially where identified private sector datasets would deliver significant private spill-over benefits and the nature of charging will likely be consistent with the public interest designation of the NID in the first place.

The takeaway

The Commission has undertaken a holistic review of data availability and use in Australia, having regard to the range of information available (including personal, commercial, demographic and government sector information; raw and transformed data) and the various issues that arise in this context (including community, privacy, consumer, commercial and other concerns).

Its key finding is that Australia is behind the eight ball, from a regulatory, cultural and therefore, innovation perspective as regards to data availability and use. Ultimately, the Commission proposes new data regulatory and competition and consumer frameworks to address the issues identified.

From a data regulatory perspective, the goal is to implement secure frameworks and facilitate community trust in data usage. How this will be implemented in an already-complex regulatory framework will be a challenge.

From a competition and consumer perspective, the Commission proposes to provide consumers with much-needed power over their own data. The empowerment of the ACCC to enforce these rights will mean greater cooperation between the ACCC and the OAIC will be required.

A cross-portfolio Data Availability and Use Taskforce has been established to prepare the Government's response to the recommendations in the Report. It therefore remains to be seen whether and to what extent the proposed Framework will be adopted.

Let's talk

In the meantime, for a deeper discussion of how these issues might affect your business, please contact:

Tony O'Malley, Partner, Legal
+61 (2) 8266 3015
tony.omally@pwc.com

Peter Malan, Partner, Risk Assurance (Digital Trust)
+61 (3) 8603 0642
peter.malan@pwc.com

Sylvia Ng, Director, Legal
+61 (2) 8266 0338
sylvia.ng@pwc.com

Cameron Whittfield, Partner, Legal
+61(3) 8603 0140
cameron.whittfield@pwc.com

Grace Guinto, Director, Risk Assurance (Digital Trust)
+61 (3) 8603 1344
grace.guinto@pwc.com

Steph Baker, Solicitor, Legal
+61 (2) 8266 5054
steph.baker@pwc.com

[5] Productivity Commission 2017, *Data Availability and Use, Inquiry Report*, pp. 344.

Attachment A

Data Regulatory Reform – Proposed Timeline

In the Commission's view, an ambitious and realistic timeline is required to adequately address the issues identified. It suggests the following timeline for the Framework:

Immediately

- Improve data accessibility and quality:
  - create registries of public and publicly funded data holdings
  - public guidance for custodians on data sharing and release
  - government agencies to commence implementation of data standards
  - commence releasing all non-sensitive public sector data
  - designate agency responsible for introducing data policy reform
- appoint NDC administratively
  - Improve data usage:
  - accredit more data linkage units
  - abolish requirement to destroy linked data and linkage keys.
- *Data Sharing and Release Act*
  - commence exposure draft development
- Consumer rights:
  - begin industry negotiations on definition of consumer data
  - monitor progress towards target for Comprehensive Credit Reporting (CCR).

End of 2017

- Establish the NDC, which, at first instance, will be tasked with monitoring the effects of the new framework, engaging with States and Territories and producing an initial suite of NIDs (including identification of legislative restrictions on the sharing of such NIDs)
- Establishment of a central agency, different from the NDC and at each the Federal and State/Territory levels, with responsibility of implementing the new framework and publicly reporting on progress
- Government agencies release draft data management standards, addressing industry-specific matters relating to data availability and use, for public consultation.

By May 2018

- Draft Data Sharing and Release Act including an initial list of NIDs
- Appoint NDC Advisory Board and ethics advisor
- Streamline human research ethics committee processes
- Priority development of industry data specification agreements
- If required, introduce legislation to mandate comprehensive credit reporting
- Report on progress of implementation of new framework.
- Public funded entities to publish data registries

By End of 2018

Implement the DSR Act and supporting amendments for an initial suite of NIDs

2019 Onwards

- NDC to assume role of central agencies
- Establish clear lines of accountability to support the implementation and ongoing success of the framework
- ARAs to manage NIDs
- Data custodians to work with ARAs to improve data use
- Comprehensive Right enforced by ACCC.

By 2020

Government agencies to adopt data management standards

Attachment B

Proposed Regulatory Bodies

Regulatory body	Role	Composition	Powers/Responsibilities
Office of the National Data Custodian (**NDC**)	Overall responsibility for implementation of the data regulatory framework and data management policies, in consultation with all levels of government.	Independent statutory office holder within the Commonwealth Portfolio. The NDC should be an individual with significant expertise in data and the benefits of data use, but also have an understanding of community attitudes and the need for a 'social licence' to use data.	• Oversight, monitoring of and public reporting on the new Framework and DSR Act. • Assessment of and recommending designation of NIDs. • Accrediting ARAs and responsibility for ARA matters including cooperation and complaints. • Regulatory guidance for ARAs and data custodians on matters such as risk management, data curation and metadata, data security, data de-identification and trusted user models. • Regulatory guidance for government data custodians as to their data rights and responsibilities, to ensure that requests for data access are dealt with in an efficient manner, consistent with the ARA risk management approach.
State-based central government agencies	Agency with responsibility for overarching policy in respect of data.	As determined by the States.	• Offer a public process whereby data sets or combinations of data sets can be nominated for potential focus of private investment opportunity and public benefit.
Accredited Release Authorities (**ARAs**)	Public sector or public interest entity accredited by the NDC to be an accredited data release authority, at either a jurisdictional or sectoral level.	Public sector or public interest entity, which has a focus on release of data sharing, an existing base of technical and sectoral expertise, and social licence. Ideally, an ARA will be politically independent and an incorporated entity. The	• Improving access to data (including personal information, NIDs and other data sets) and determining whether a data set should be available for public release or limited sharing. • Acquiring, storing and processing the data sets of a

Regulatory body	Role	Composition	Powers/Responsibilities
		Commission envisages jurisdictional ARAs be appointed, plus sector-specific ARAs where sector responsibilities are split between the Commonwealth and States (e.g. healthcare). The Commission anticipates approximately 12-15 ARAs should be accredited nationally.	particular jurisdiction or sector (for which it holds primary responsibility for transformed - e.g. de-identified - data sets). • Provision of resources to other entities to assist with skills and policy development in the context of data availability and use. • Perform data linkage activities for their jurisdiction or sector. • Perform ongoing work after collection of data to ensure data accuracy and usability over time. • Perform fit-for-purpose de-identification and encryption of data as suitable for a particular data set, to help make such data available to trusted users • Publishing (and regularly review) formal risk management processes for the sharing of data under their control.