The Federal Government's Bold Vision for Data Availability and Use

Partner Gavin Smith, Senior Associate Jessica Selby and Lawyer Claudia Hall consider the Federal Government's response to the Productivity Commission's report on data availability and use, released 1 May 2018.

Introduction

The Federal Government's response on 1 May 2018 to the Productivity Commission's report on Data Availability And Use (2017) (**PC Report**), outlines a bold vision but has a surprising lack of detail, suggesting implementation is likely to be some way off. If legislation is introduced, the new regime will result in a fundamental change to the way Australian consumers, businesses and government agencies interact with and think about data.

How does it affect you?

The Federal Government's Response has adopted most, if not all, of the recommendations in the Productivity Commission Inquiry Report on Data Availability and Use and confirmed the government's commitment to adopt a systems-wide approach to implementing an open data agenda. But it also leaves a huge amount of detail to be determined about the rights, obligations and governance framework under both the new Consumer Data Right (**CDR**) and data sharing and release (**DSR**) regimes.

The Response fails to replicate the PC Report's ambitious timeline for implementing the CDR and DSR regimes. The Federal Government has, historically, been slow to pass privacy legislation. Given the substantial amount of detail that remains to be determined, and a legislative road jam ahead of the next federal election (likely to be held in early 2019), we think it is unlikely that legislation codifying the CDR and DSR regime will be passed imminently.

If and when the government introduces legislation for the CDR and DSR regimes, there will be a ground-shift in the approach to data governance and valuation and the understanding of the utility of data in Australia. We predict the key impacts will be:

- **Private sector**
  - Businesses subject to the CDR will need to implement processes to identify what consumer data they hold and to enable consumers to access or transfer consumer data that is subject to the regime to themselves or third parties. Businesses in the banking, energy or telecommunications sectors should be on high alert, as the CDR will be introduced first to these sectors.
  - It is unclear whether the government intends to designate certain private sector datasets as, or as a component of, high-value datasets or Designated Datasets. If so, these private sector datasets might be required to be disclosed to, or compulsorily acquired by, government agencies or the broader market.
  - Once the Data Sharing and Release Act contemplated by the Response (**DSRA**) is introduced, businesses can apply to become a 'Trusted User' to obtain access to specified datasets that are not released to the public.
  - If the National Data Commissioner's functions include developing de-identification standards, businesses can consider whether they want NDC certification that they are using best practice de-identification processes and/or require that their service providers obtain such certification.
  - Businesses will likely be provided with greater access to searchable and comprehensive public-sector datasets.
- **Public sector**
  - Government agencies will need to implement processes (in conjunction with stakeholders) in relation to data sharing and management and de-identification.
  - Government agencies are likely to be required to disclose all information they hold that is not personal, commercial in confidence or 'particularly sensitive', for example because it relates to national security.
  - Depending on the scope of the DSRA, government agencies may have a greater right to access and require the release of information held by the private sector.
- **Consumers**
  - Consumers (and potentially small and medium enterprises (**SMEs**)) will have broader rights to access information about themselves in certain sectors, and the right to have that information transferred to a third party in order to improve their ability to make decisions about, and to acquire, products and services. The Response anticipates that the introduction of data portability will increase competition among service providers.
  - Individuals will be provided with greater access to searchable and comprehensive public datasets.[1]

1. Productivity Commission 2017, *Data Availability and Use*, Inquiry Report, Canberra, pages 33-52.

Background

- In May 2017, following public consultations and submissions on its draft report, the Productivity Commission released its Inquiry Report on Data Availability and Use, which included 41 recommendations. The PC Report was a landmark investigation on access and use of data in Australia, which criticised Australia's existing approach and proposed a need for 'fundamental and systematic change'. The PC Report set out an ambitious timeline that proposed all the recommendations be in place by 2020.
- In November 2017, the Federal Government announced that in 2018 it would bring forward legislation to create a Consumer Data Right (***CDR***) based on the PC Report recommendations. The announcement proposed the CDR would grant consumers across all sectors open access to their data, as well as an ability to direct a business to transfer their data to a third party in a usable machine readable form.
- In February 2018, the Federal Government released its Review into Open Banking, which included a new regulatory framework for 'Open Banking' (ie a framework for CDR for the banking sector).

Consumer Data Right

The Response accepts the PC Report's recommendation to introduce a CDR for the access and transfer of consumer data, administered by the Australian Competition and Consumer Commission (***ACCC***). The implementation of this recommendation was foreshadowed by the Federal Government's announcement in November 2017 and the recent Open Banking Review. The CDR will be rolled out progressively on a sector-by-sector basis, commencing with the banking, energy and telecommunications sectors and then moving to other sectors designated by the Treasurer.

Scope of the CDR

The Response provides that the CDR will empower consumers to:

- access particular data, such as transaction, usage and product data, in a useful digital format (***consumer data***); and
- transfer that data to themselves or third parties.

This is a more limited right than that set out in the PC Report, which also proposed allowing consumers to have the right to be informed of an entity's intention to disclose, exchange or sell data about that consumer for commercial gain.

Notably, the Response does not clarify whether the CDR is limited to individuals or whether it will extend to SMEs, although we note the Open Banking Review recommended that all consumers - that is individuals, small business *and* large business - be entitled to exercise the CDR, given the difficulties in delineating between small and large businesses.[2]

The PC Report provides that the type of consumer data required to achieve 'choice and competition benefits' under the CDR will be determined by government in consultation with the relevant sector and consumers. As with the remainder of the Response, this explanation lacks a lot of the detail contained in the PC Report, which proposed a wide definition of consumer data.[3] We believe the approach under the Open Banking Review is likely to be indicative of how the government will approach the CDR in practice for future sectors.[4] For example, the scope of consumer data under the Open Banking Regime is relatively limited being:

- digitally held customer-provided data (such as payee lists);
- data generated as a result of transactions made on a customer's account or service in relation to specified deposit and lending products; and
- product and service information that banks are already required to publicly disclose.[5]

The PC Report expressly excluded certain data from the scope of consumer data, for example, data subject to intellectual property rights or 'imputed data' about a consumer (ie data that has been created by the entity or a third party where it is merely probable that the characteristics are associated with an individual consumer).

The Open Banking Review excluded 'value-added data' (which results from material enhancement by the application of insights, analysis or transformation) from the scope of consumer data. This approach conflicts with the PC Report, which clearly distinguished between value-added data (data that has been made more useful) and imputed data, and proposed that value-added data *would* be considered consumer data and subject to the CDR.

The proposal that value-added data would be subject to the CDR was heavily criticised by the private sector (on the basis that it would reduce incentives to clean and organise data or invest in data analysis and transformation). We think it is unlikely, given the requirement to consult with sector groups, that the government will require that value-added data be subject to the CDR moving forward, and expect the government's ultimate approach will align more closely to the Open Banking Review's approach.

In addition, we predict that the implementation of the CDR in the

2. The Australian Government the Treasury 2017, *Review into Open Banking: giving customers choice, convenience confidence*, pages 41-42.
3. Productivity Commission 2017, *Data Availability and Use*, Inquiry Report, Canberra, page 207.
4. The Australian Government the Treasury 2017, *Review into Open Banking: giving customers choice, convenience confidence*, page vii.
5. Ibid, Recommendations 3.1 and 3.2.

energy and telecommunications sector will draw on the 'reciprocity' concept set out in the Open Banking Review. This approach could allow the government to ensure the CDR is adopted within the sector by mandating that the main telecommunication carriers, internet service providers and retail energy providers comply with the CDR, and requiring that any entities to whom telecommunications or energy consumer data is transferred under the CDR must provide *equivalent data* to consumers under the CDR regime.[6]

Governance

The CDR framework will consist of:

- legislative amendments to the *Competition and Consumer Act 2010* (Cth) (**CCA**), enabling the development of sector-specific binding rules by the ACCC in consultation with other relevant regulators; and
- sector-specific access, transfer, data and security standards to be developed by the new Data Standards Body in consultation with industry.

The Response contemplates that responsibility for overseeing the CDR will be split between the ACCC and the Office of the Australian Information Commissioner (**OAIC**).

The OAIC will be given responsibility for ensuring the CDR framework contains strong privacy protections[7] and for handling consumer complaints (with the justification that such complaints are likely to relate to privacy).[8]

The ACCC will have a significantly increased remit and will be responsible for:

- ensuring that the CDR system operates as intended and supports competition and consumer outcomes;
- investigating breaches and enforcing the CDR, including breaches that raise systemic competition issues, other than enforcement of privacy or confidentiality;
- determining the criteria for, and method of, accreditation for entities to whom consumer data can be transferred under the CDR; and
- potentially, monitoring and reviewing any costs reasonably incurred by entities in providing access to, or transferring, consumer data under the CDR.[9]

New Data Sharing and Release Regime

In addition to the new CDR system, the government has also proposed introducing a new legislative and policy regime to increase access to, and sharing of, data. The regime would apply in particular to public sector data. As with the CDR above, the Response does not clarify the details of the Data Sharing and Release Act or the roles of the National Data Commissioner (**NDC**) or Accredited Data Authorities (**ADAs**) (discussed below). In particular, the Response does not:

- clearly set out whether, or to what extent, the regime will apply to the private sector, although it appears to suggest that it might; or
- address the PC Report's recommendation that the government's template contracts be amended to include the right for government agencies to access or purchase the data under the contract.[10]

Data Sharing and Release Act

The Response proposes introducing a new Data Sharing and Release Act (**DSRA**) to underpin the data sharing and open access regime. In line with the PC Report, the Response suggests that the DSRA will be principles based and not overly prescriptive, suggesting that restrictions on use of or access to data be contained in contractual 'data use agreements' (discussed further under Accredited Data Authorities below).

The DSRA will:

- establish institutional and governance arrangements, including establishing an accreditation process and governance framework for ADAs and the 'Trusted User' framework; and
- set out rules and expectations around data sharing and release, and relevant safeguards for sensitive information (such as personal information, commercial in confidence information or information relating to national security).

The Response provides that the DSRA will not affect existing protections of particularly sensitive information (such as national security and law enforcement data) or secrecy provisions in relation to identifiable information. This expressly rejects the approach put forward in the PC Report, that the DSRA might authorise the sharing and releasing of data *despite* the provisions of other legislation, such as privacy legislation.

National Data Commissioner

The NDC will be established as an independent statutory authority. The Response indicates that the NDC's functions will be to monitor the integrity of and oversee the DSR regime and the DSRA, in particular the data sharing and release activities of Commonwealth agencies, and to provide guidance on technical best practice and ethical access to and use of data.

The scope of the National Data Commissioner's remit is not clearly expressed in the Response. The PC Report suggested that the National

6. Ibid, Recommendation 3.9.
7. Ibid, page 18.
8. Ibid, page 17.
9. Productivity Commission 2017, *Data Availability and Use*, Inquiry Report, Canberra, page 19.
10. Ibid, Recommendation 6.3; Ibid, page 241.

Data Commissioner be given broad scope to deal with both private and public sector access to, and sharing or release of, data. However, the Response repeatedly refers to *public data* and the *government's* use or management of data. This suggests to us that the NDC's remit might in fact be limited to the administration of the DSR regime *only* in respect of the public sector. This leads to a broader question about whether the government intends for the DSR and 'open access' regime to govern the private sector, as recommended in the PC Report.

It is not clear whether the NDC's functions will also include additional activities that were set out in the PC Report, for example:

- developing standards for the de-identification of data and guidance on re-identification risks;[11]
- developing guidance on how to manage risks in sharing identifiable data between entities;[12] or
- setting prices for organisations to access datasets.

The Response further provides that the NDC will receive guidance from the Australian Bureau of Statistics (**ABS**) in respect of technical issues, and a new National Data Advisory Council in respect of ethical data use, technical best practice and industry and international developments.

Accredited Data Authorities

The Response commits to accrediting bodies with particular expertise as Accredited Data Authorities. The Response provides that the accreditation and governance process for ADAs will be similar to that for ABS and the Australian Institute for Health and Welfare as 'Integrating Authorities'. Accordingly, it is likely that each ADA will be a Federal Government agency, or otherwise a 'secure and trusted institution' bound by the *Privacy Act 1988* (Cth), and that they will have sole responsibility for administration and management of a number of datasets, including the provision of access to relevant Trusted Users (discussed further below).

As set out in the Response, two of the ADAs' key responsibilities will be:

- determining whether a dataset is made available for public release or otherwise for limited sharing with Trusted Users; and
- entering into data use agreements with Trusted Users, data custodians and data users. These agreements will outline the conditions of, and restrictions on, access to data, risk management arrangements, as well as permitted actions in respect of the shared data (for example, integration of the dataset with other data or release of a non-sensitive version of the dataset).[13]

Trusted Users

The PC Report contemplated that Trusted Users would be individuals who are approved by an ARA to access and use data that is sensitive or is otherwise not publicly available. The Response does not clarify the government's approach to Trusted Users, apart from acknowledging that it will be based on the UK 'five safes' model. While the Response does not specify who might be entitled to be a Trusted User, we believe it is likely to consist of the entities identified in the PC Report, namely government agencies, universities, not-for-profits, corporates and research bodies (where bound by the Privacy Act).

We expect that Trusted Users will be classified on a scalable basis, with the level of trust the user has influencing the accreditation, reporting and compliance requirements. While private sector entities may be entitled to become Trusted Users, they are likely to be subjected to more stringent access and use restrictions, including controls on accessing potentially identifiable data about businesses in the same industry.

Designated Datasets – a special class of high-value datasets

In the Response, the government agreed to establish a framework to identify 'Designated Datasets' (***DDs***), being datasets whose availability and use would generate significant community-wide benefits. The Response classifies DDs as a 'special class of high-value datasets' whose release would complement work done about high-value datasets under the *Open Government Partnership National Action Plan 2016-2018* (**Action Plan**). Given that high-value datasets under the Action Plan only relate to public sector data, we think this suggests that DDs might similarly be limited to public sector datasets.

This approach would be at odds with the PC Report, which suggested that there could be situations where there is a national interest in including private sector information in a DD, such as data held and collected due to services funded or legislatively authorised by Commonwealth or State public policy (eg data held by banks, health insurance funds and energy providers).[14] This recommendation in the PC Report received negative backlash from the private sector, so it is possible that the government has reduced the scope of DDs such that they will only contain public sector data, or that the government has left the Response intentionally vague to give itself more time to determine whether it requires private sector DDs.

The government has also committed to publishing a register of available publicly-funded datasets and giving priority to the release, curation and streamlining of access to datasets

11. Ibid, page 320.
12. Ibid, Recommendation 8.2.
13. Ibid, Recommendations 6.9 and 8.3; Ibid, pages 269, 322.
14. Ibid, pages 305-306.

with the greatest potential to deliver social and economic outcomes for the country.[15]

Looking forward

The open access approach championed by the Productivity Commission and supported by the Federal Government's Response signifies a fundamental change in the attitude to the access and use of data in Australia.

The PC Report and the Government's Response propose a framework that will dramatically shift the way in which data is thought about and managed by government, the private sector and individuals. While greater access to public and private datasets is likely to improve the insights that can be gained about population trends and may improve the setting of public policy, it is also likely to impose a cost on private entities, both in relation to compliance and through increased levels of competition. It will increase the potential risk for data to be misused. It remains to be seen whether the government in weighing these costs has determined that they will only implement the open data framework and DSR regime in respect of the public sector.

Crucially, in attempting to implement the new DSR and CDR regimes, the government must ensure that data is provided in a meaningful and understandable way to consumers and the broader public and is not released in quantities that are overwhelming, and that personal and commercial-in-confidence information is protected.

The Response leaves all details of the proposed regime open to be determined. The proposed regime will need to be implemented through the drafting of the amending legislation to the CCA, the DSRA and through guidance issued by the NDC, ACCC and the Data Standards Body. Given that the NDC has not yet been established and legislation has not yet been put forward, it is unlikely that the new DSR and CDR regimes will be implemented until at least next year.

While big changes to Australia's privacy and data landscape appear to be on the horizon, until the detail and enabling legislation is settled, it is not possible to say with certainty what this brave new world will look like for the Australian public and private sector.

15. Commonwealth of Australia, Department of Prime Minister and Cabinet 2016, *Australia's First Open Government National Action Plan 2016-2018*, page 25.

Michelle Rowland MP:

Old media, new media, not media:

Rethinking policy for the public interest

"We need a coherent, principled and evidence-based approach to guide a transition where all players do their bit"

With recent developments in policy and regulation suggesting that Australia is barely playing catch-up, Michelle Rowland MP, Shadow Minister for Communications will provide a presentation on the role of Government in promoting public interest objectives and the need to adapt as the media ecosystem evolves.

To encourage openness and the sharing of information for the benefit of its members, unless specified otherwise, all CAMLA events are subject to the "Chatham House Rule" which provides that participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

Date and Time
17 May 2018
Registration: 5.45pm
Seminar: 6.00-7.00pm
Drinks and canapés: 7.00-9.00pm

Venue
Gilbert + Tobin
Level 35, Tower Two,
International Towers
200 Barangaroo Avenue
Barangaroo, NSW

Cost
$70 for members
$95 for non-members