THE CONSUMER DATA RIGHT

And What it Means for the Private Sector

SIMON BURNS AND CLARE HARRIS

2018

GTLAW.COM.AU

KEY TAKEAWAYS

1. The Consumer Data Right (CDR) will confer a right on consumers (both individuals and business customers) to access particular data and have that data transferred to either themselves or to a third party.
2. The impact to private sector organisations is likely to be significant as both competition and regulatory compliance costs increase.
3. Despite a planned economy-wide rollout being announced, it is likely we will only see consumers provided with access to their banking, energy, phone and internet data in the short to medium term. Although, the reciprocity principles may see other datasets from other industries shared earlier in some instances.
4. Lawyers, particularly those in the energy and telecommunications sectors, should consider advising their private sector clients to engage with the Treasurer's consultation process for the draft legislation implementing the CDR.

BACKGROUND

In May 2018, the Australian Government announced that it would legislate a CDR to allow consumers to harness the power of their data and provide consumers with greater control over their data.

The CDR and its implementation will be based on four key principles:

- Consumer-focused: it is for the consumer and about the consumer.
- Encourages competition: it seeks to increase competition for goods and services to allow consumers to make better choices.
- Creates opportunities: it seeks to provide a frame- work to foster new and creative goods and services.

Efficient and fair: it should be implemented with security and privacy front of mind, without being unnecessarily complex or costly. The government's announcement largely reflected the Productivity Commission's recommendation in its *Data Availability and Use: Inquiry Report*[1] (the Report) to create a "Comprehensive Right for consumers" that would give consumers the right to be provided with, or to direct the transfer to a designated third party of, their consumer data in a machine-readable format.[2]

Since the government's announcement, the Treasury who is leading the implementation of the CDR — released guidance[3] providing more information on cer- tain aspects of the CDR (Treasury Guidance). Despite this, as it stands, much of the detail surrounding the scope of the CDR and its implementation remains unknown and will be determined through a public consultation process to be conducted by the Treasury.

What is known is that the CDR will be implemented progressively, beginning in the banking sector, then energy and telecommunication sectors, before being rolled out economy-wide on a sector-by-sector basis.

The CDR will be rolled out in the banking sector under the guise of "Open Banking" as contemplated by the Treasury's *Review into Open Banking: Giving Customers Choice, Convenience and Confidence*[4] (the Open Banking Review). Open Banking will have a phased implementation from July 2019 (based on current time frames). To achieve this time line, the Treasury will be consulting on draft legislation, the Australian Competition and Consumer Commission (ACCC) will be consulting on draft rules and Data61 will be consulting on technical standards.[5]

In relation to the energy sector[6] , the Treasury and the Council of Australian Governments Energy Council (COAG EC) are currently working together, with the COAG EC expected to consider recommendations from this consultation process later this year.

The Treasury has stated that it will not conduct a full sector assessment of the telecommunications sector.6 Instead, the ACCC will consider which datasets will be made available by reference to the costs and benefits of making each dataset subject to the CDR.

For all other sectors, the ACCC will conduct a public consultation process with potential future sectors in due course.

WHAT IS THE CDR?

The CDR is a right for consumers to access certain data about themselves that is held by businesses, and to direct that such data be transferred to an accredited third party of their choice.

WHO IS GRANTED THE CDR?

The short answer is probably everyone. While the Report recommended that the right be limited to individuals and small and medium businesses, current guidance and recommendations from the Treasury indicate that the right will also be granted to large businesses.

This enhanced scope of "consumers" is one of the few areas where the CDR is broader than the initial recommendations from the Report. It is also an area where, particularly for banking, questions have been or will be asked regarding the cost–benefit analysis associated with granting large businesses this right.

WHAT DATA IS COVERED?

The principles regarding exactly what data will be covered by the CDR is still to be confirmed. So far, the government has stated that the CDR will allow consumers to access "particular data, including transaction, usage, and product data, in a useful digital format."[7] The Treasury Guidance goes on to clarify that the type of data that will be available to consumers under the CDR will be determined on a sector-by-sector basis.

The areas of discussion in respect of excluded datasets are essentially anything which is not raw data. For example, "value-added data", "aggregated data", "derived data", "imputed data" and data subject to intellectual property rights. Determining what should and should not be "excluded" will require those drafting the enabling legislation to weigh innovation and investment against promotion of competition.

Over the past months, the recommendations from the government have evolved to reduce the scope of the data which is subject to the CDR to now, under Open Banking, carve out value-added datasets and aggregated datasets. The precise definition of these terms is still to be formulated, but organisations will need to consider how they can protect their more valuable data assets by ensuring they fit within the relevant categories of excluded data.

In relation to the banking sector, the Open Banking Review has determined, and the government has accepted, that the CDR will apply to transactional datasets based on product type. For example:

+ deposit products, including:
  - savings accounts
  - term deposits
  - debit card accounts
  - mortgage offset accounts
+ lending products, including:
  - mortgages
  - personal loans
  - credit and charge cards (both personal and business)
  - consumer leases

In relation to the energy sector, the COAG EC is currently conducting a consultation process as to what classes of data the CDR should be applied. The Treasury Guidance emphasises that retail electricity metering data will be included as a minimum.

A similar analysis and assessment of which datasets will be made available under the CDR will be under- taken for the telecommunications sector.

According to the Treasury Guidance, data may also be made available under the CDR through a reciprocity mechanism to be incorporated into the enabling legislation.[8] While the details of the reciprocity mechanism are yet to be settled, the mechanism will act as a term or condition for accreditation, under which businesses to whom data is transferred following a request by a consumer must provide "equivalent data"[9] to the consumer. As part of the accreditation process, the ACCC is expected to adopt a principles-based approach to determining what constitutes equivalent data on a sector-by-sector basis.

This approach is designed to avoid a "free-rider" scenario where organisations take from the CDR regime, but provide nothing in return. The net effect of this is that data holders outside of sectors which are subject to the CDR may have a disincentive to seek access to consumer data as it would mean their own data assets may become portable/shareable.

It will also be interesting to see how organisations in sectors which are not highly regulated (or at least do not have a regulatory need to retain transactional data) will manage their data practices so that they can participate in the CDR regime (ie, "take"), but have little "transactional data" to give. For example, data practices which perform analytics on or aggregate transactional data then purge the transactional data after a certain period of time may become more common depending on the type of business.

TO WHOM CAN DATA BE TRANSFERRED?

Presently, consumers may only direct their data be transferred to a trusted (ie accredited) third party. The accreditation regime is expected to be tiered based on the type and sensitivity of the data to be received.

Accreditation is naturally likely to focus on security and data controls and governance.
These requirements and standards will provide an additional overlay to the security standards under various privacy law regimes, including:

+ the Privacy Act 1988 (Cth)
+ the General Data Protection Regulation (GDPR) to the extent it captures an organisation in Australia,

and also various international standards and de facto standards, such as the National Institute of Standards and Technology's Cybersecurity Framework.

WHAT ARE THE SPECIFIC RULES AROUND CONSENT?

As well as providing the original data holder with a direction to transfer, consumers will also need to provide the data recipient with explicit consent as to how such data may be used.

The enabling legislation for the CDR will specify robust requirements regarding the consent to transfer and the subsequent consent to use the data. There will be no implied consent for data transfers under the CDR.

The Treasury Guidance foreshadows certain high-risk uses by the data recipient that may require separate consents, including:

+ use of the data for marketing purposes
+ on-sale of the data
+ transfers of the data overseas
+ transfers of the data to a party who is not subject to the CDR privacy and accreditation requirements.

REGULATORY FRAMEWORK

The CDR will be implemented primarily through amendments to the Competition and Consumer Act 2010 (Cth), as well as the Privacy Act. The ACCC will be the lead regulator for the CDR, with responsibility for developing rules and an accreditation scheme, as well as ensuring compliance with the CDR.
The ACCC will be supported by the Office of the Australian Information Commissioner (OAIC), who will oversee privacy protections, complaint handling and a new Data Standards Body, which will develop technical data standards.
CSIRO's Data61 is performing the role of the Data Standards Body, who will be responsible for collaborating with industry sectors, the technology community, consumer groups and privacy advocates on the applicable data access and transfer standards.

IMPACT ON THE PRIVATE SECTOR

Since the government's announcement in May, much has been written about the benefits of the CDR for consumers, for example, better value for money and tailored products and services. Weighing against these benefits are the impacts on businesses that are data holders subject to the CDR.

RAISING THE BAR

Generally speaking, the enabling legislation for the CDR is expected to place additional layers of regulatory requirements on how data received through the CDR system must be handled. The additional security controls and enhanced consent requirements referred to above are just two examples of this and are expected to be coupled with rules around data deletion, transparency, and complaints and remedies.

This two-tiered regulatory regime will mean that organisations will either need to:

+ have in place strong data provenance, consent management and data governance regimes to enable the organisation to manage and govern their data practices based on the different regimes or
+ adopt the "high-water mark" and uplift their operations to comply with the most stringent requirements
+ These enhanced data governance regimes can already be seen, to a degree, in Australian organisations due to the extraterritorial reach of the GDPR, and the new CDR is set to add even further complexity.

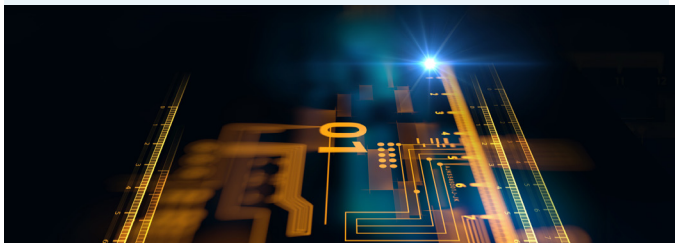
CORPORATE INFORMATION

One area yet to see significant discussion is data sharing organisations seeking to protect their own confidential corporate information which may be embedded within consumer data.

Consumer transaction data, particularly when pooled together and aggregated across large sets of customers, provides a wealth of information, not just about consumer behaviours but also about corporate behaviours and other market or business information. While much of this information can be generated from data which is already shared or accessible by third parties (for example, through the existing screen scraping mechanisms implemented today), the volume, velocity and, to a degree, variety of data available will be dramatically increased. This will better enable data analytics to be applied to learn corporate information about the relevant data holder.

This type of data use should be subject to the consumer's specific consent. However, despite the proposed controls around consent in the CDR, it may be that consents are still relatively broad and it may also be that data is permitted to leave the CDR system, for example by on-sale or disclosure by data recipients.

It will be interesting then to see what controls (if any) will be incorporated in the enabling legislation or alternatively in any direct data access and sharing agreements, or application programming interface (API) terms which may be put in place between data holders and data recipients.



COST IMPLICATIONS

The CDR is likely to have a significant cost impact on businesses. This cost impact will arise from the dual factors of additional costs of ensuring compliance with the new legislation and through increased levels of competition driving down prices for goods and services, which may in turn see an increased cost on marketing and other activities to retain market share.

The compliance costs will depend to a large extent on the breadth of the definition of "consumer data" and the size of the business's customer base. As the CDR is rolled out, there is likely to be repeated calls from sector advocates to limit the types of datasets subject to the CDR.

There may also be potentially disproportionate impacts on smaller businesses which have a smaller customer and revenue base to cover the cost of compliance. To support these businesses, new service offerings may emerge, including the supply of "off-the-shelf" solutions, particularly around identity, consent and data request management.

LIABILITY AND DATA BREACHES

At a time when data breaches are questions of "when" not "if" for businesses, the government has emphasised that the CDR will be underpinned by strong privacy and information security protections, together with a regime to attribute liability for data breaches to the appropriate party.

It will be interesting to see just how effective the liability regime will be in directing compensation claims between participants in the CDR ecosystem. It is easy to envisage circumstances where consumers will look to their bank for compensation or redress, rather than a start-up, regardless of where statutory liability may rest for a data breach. This will particularly be the case in circumstances of identity theft and fraudulent transactions where the impact of a data breach will be felt within the banking relationship regardless of whether or not the data breach occurred at the bank or some other third party.

While data holders may find it difficult to negotiate additional risk allocation regimes with data recipients, the offer of value-added services or enhanced data access regimes may provide some leverage to negotiate these types of terms.

OPPORTUNITIES

While there is no doubt that there are costs and risks associated with the CDR for private sector organisations, there are equally significant opportunities for all organisations (including data holders) which implement solutions and platforms to leverage existing customer relationships and expand them based on data received through the CDR regime.

For many organisations, the CDR may be the push which is needed to both enhance their data governance regime, and also focus on new digital solutions and ways to better serve their customers.

Forward-thinking organisations, particularly in the banking sector, may also look to ways to leverage their head start over other industry sectors so that by the time combined data across sectors is available, they have mature solutions and service offerings.

Further still, it would be prudent for the banking sector to structure their assets and solutions with an eye to the possible expansion of Open Banking to include write, and not just read, APIs. The inclusion of write access, which enables payment transactions to be initiated by third-party service providers, would follow the UK approach. This would be a fundamental shift in the banking sector and have the potential to materially alter the nature and scope of a bank's relationship with its customers.

CONCLUSION

Together with other reforms announced by the government, such as the introduction of a National Data Commissioner and new legislation to improve the sharing, use and re-use of government data, the CDR represents a seismic shift in the government's attitude towards the use of data in Australia.

While we are yet to see the scope of the draft legislation implementing the CDR, it is clear that it will significantly change the data landscape in Australia.

SIMON BURNS

Partner

T +61 2 9263 4776

E sburns@gtlaw.com.au

CLARE HARRIS

Lawyer

T +61 2 9263 4189

E charris@gtlaw.com.au

ENDNOTES

1. Productivity Commission Data Availability and Use: Inquiry Report Report No 82 (31 March 2017) www.pc.gov.au/inquiries/ completed/data-access/report/data-access.pdf.
2. Above n 1, at 197.
3. The Treasury "Consumer Data Right" Booklet (9 May 2018) https://static.treasury.gov.au/uploads/sites/1/2018/05/ t286983_consumer-data-right-booklet.pdf.
4. The Treasury Review into Open Banking: Giving Customers Choice, Convenience and Confidence (December 2017) https:// static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open- Banking-_For-web-1.pdf.
5. Above n 3.
6. Above n 3, at 9.
7. Department of the Prime Minister and Cabinet (Cth) "The Australian Government's response to the Productivity Com- mission Data Availability and Use Inquiry" (2018) 6 http:// dataavailability.pmc.gov.au/sites/default/files/govt-response-pc- dau-inquiry.pdf.
8. See above n 3, at 4.
9. Above n 3, at 4.

SYDNEY
Level 35 International Towers Sydney
200 Barangaroo Avenue
Barangaroo NSW 2000
Australia
T +61 2 9263 4000
F +61 2 9263 4111

MELBOURNE
Level 22
101 Collins Street
Melbourne VIC 3000
Australia
T +61 3 8656 3300
F +61 3 8656 3400

PERTH
Level 16 Brookfield Place Tower 2
123 St Georges Terrace
Perth WA 6000
Australia
T +61 8 9413 8400
F +61 8 9413 8444

GTLAW.COM.AU