Consumer Data Right, Open Banking and Federal Government Data Release and Sharing In Australia
A Status Report

Peter Leonard
Principal, Data Synergies

The Federal Government has stated its intention that the Consumer Data Right (**CDR**) is intended to be progressively applied sector by sector across the whole economy, beginning in the banking sector.

The Federal Government currently envisages the following:

- A three-phase introduction of a CDR for certain retail banking products provided by specified classes of banks. This is commonly referred to as 'open banking".
- A CDR for the retail electricity sector, but with the Government not yet deciding the categories of retail electricity data (other than household metering data), or the classes of providers to be subject to this CDR, or whether there would be stages or phases for implementation.
- Possibly, a CDR for the retail gas sector, but with the Government not yet determining the retail gas categories of data (other than household metering data) or classes of providers to be subject to this CDR, or whether there would be phases or stages in implementation.
- Possibly, a CDR for the retail telecommunications services sector, but with the Government not yet determining the categories of data or classes of telecommunications service providers to be subject to this CDR whether there would be phases for stages in implementation.
- Perhaps in the future and having regard to learnings and outcomes of the above implementations, other sector specific CDRs.

There will be a phased implementation of open banking from July 2019. The Government intends to require the four major trading banks to make data available on credit and debit card, deposit and transaction accounts by 1 July 2019 and on mortgages by 1 February 2020. Data on all products recommended by the Review will be available by 1 July 2020. All remaining banks will be required to implement Open Banking with a 12-month delay on timelines compared to the major banks. The Australian Competition and Consumer Commission (ACCC) will be empowered to adjust timeframes if necessary. Other banks will need to comply with these standards by 1 July 2020.

The Australian Treasurer has confirmed that the Council of Australian Governments (**COAG**) will consider the early application for CDR to the energy sector. A consultation process as to a COAG Energy Council "Facilitating Access to Consumer Energy Data - Consultation Paper" has closed (http://www.coagenergycouncil.gov.au/publications/call-submissions-facilitating-access-consumer-energy-data). The Federal Energy Minister and State and Territories Energy Ministers endorsed the adoption of the CDR regime for the energy sector and indicated a preferred standards implementation target date of end of Jan 2020. A proposal to formally consider this timetable will be discussed at the next COAG meeting in

November 2018. Data61 is to prepare and release a briefing/information package on how technical standards may be implemented across the energy ecosystem given the experience with the banking sector implementation. No timetable for this has been announced.

No timetable has been announced in relation to implementation of the CDR in the telecommunications sector or any other industry sectors.

The policy rationale for the CDR may be summarised as follows:

- The CDR will provide individuals and businesses with a right to efficiently and conveniently access specified data in relation to them held by businesses; and to authorise secure access to this data by trusted and accredited third parties.

- The CDR will also require businesses to provide public access to specified information on specified products they have on offer: that is, certain designated general product information. Accordingly, the CDR will also have an element of mandatory product disclosure.

- The CDR aims to facilitate 'apples with apples' comparison of products and portability of data to facilitate switching between providers. The Government's stated policy rationale for the CDR is "through requiring service providers to give customers open access to data on their product terms and conditions, transactions and usage, coupled with the ability to direct that their data be shared with other service providers, the Government expects to see better tailoring of services to customers and greater mobility of customers as they find products more suited to their needs".

- The CDR right may be exercised by any customer of any size in relation to designated DCR data relating to them.

There are now four key streams of work flowing from the Government's implementation of the recommendations of the Productivity Commission in its Data Access and Use Report (https://www.pc.gov.au/inquiries/completed/data-access#report).

1 Key Streams

The first stream is **development of the Treasury Laws Amendment (Consumer Data Right) Bill 2018** (**CDR Bill**) and the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2018, a process led by the Australian Treasury.

64 of the 65 submissions made on the First Exposure Draft of the CDR Bill were published on 25 September and are available at https://treasury.gov.au/consultation/c2018-t316972/.

The Second Exposure Draft was published on 24 September 2018 (https://treasury.gov.au/consumer-data-right/), together with the first draft of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2018 The consultation period closes on Friday 12 October 2018. The Designation is the draft instrument giving effect to Open Banking as a designation of certain data sets held by the four largest Australian trading banks. Australian Treasury is consulting on this Designation in parallel with consultation as to the draft Bill.

The second stream is development of the initial (in the words of the ACCC, "minimum viable product") **CDR Rules for open banking** (https://www.accc.gov.au/focus-areas/consumer-

data-right/accc-consultation-on-rules-framework). This process led by the ACCC. The ACCC has started with consultation on a draft "Framework" document ()https://www.accc.gov.au/system/files/ACCC%20CDR%20Rules%20Framework%20%28final%29.pdf) which will guide development of the actual CDR Rules. The consultation period for the Rules (also) closes on Friday 12 October 2018.

The criteria for accreditation of accredited data recipients (**ADRs**) is to be addressed in these Rules. Developing criteria for accreditation requires the ACCC to address complex technical (including data security) concerns. Resolving these concerns requires the ACCC to strike a careful balance between assuring sufficient transparency and security as to data flows and data use within the CDR data ecosystem, so as to mitigate risk of data crises and incidents that might undermine potentially fragile customer trust in the CDR system, while also not undermining timely deployment of new services. It is not yet clear whether and to what extent a regulatory sandbox might be used to evaluate new service offerings and facilitate beta or controlled testing of new data flows. The ACCC will need to evaluate competing claims as to security vulnerabilities and complexity in information management and governance. This is new territory for the ACCC. The ACCC will need significant independent technical input, which is currently difficult to source (because these technical skills are in heavy demand and therefore scare). The ACCC process also needs to be tightly entwined with development by CSIRO/Data61 of CDR data standards for open banking.

The third stream is **development of CDR data standards for open banking**.

Data standards will prescribe the format of data, method of transmission and security requirements for data to be provided by a data holder or accredited data recipient to a consumer or to one another. If a data holder or an accredited data recipient is unwilling or unable to provide the designated data set in a format that is consistent with the data standards, then the party who is seeking the information is able to seek redress.

The development of CDR data standards is being led by CSIRO/Data61 (https://data61.csiro.au/en/Who-we-are/Our-programs/Consumer-Data-Standards), "working closely with the ACCC as lead regulator of the Consumer Data Right, supported by the Office of the Australian Information Commissioner (OAIC)".

An Advisory Committee and a number of working groups are being established to support Data61 designing and testing the open standards that Data61 develops. Input provided by the Advisory Committee and working groups, alongside draft guidance materials, API specifications and implementation materials is to be openly shared.

As at late September 2018:

- the following "decisions" have been reviewed by the Advisory Committee and confirmed by the Chair of the Data Standards Body, Mr Andrew Stevens:

  Decision 001 - API Principles

  Decision 002 - URI Structure

  Decision 003 - Extensibility Model

  Decision 004 - Versioning Strategy

- the following “decisions” had been exposed for comment and a finalised position has been created in working groups, for review by the Advisory Committee and subsequent endorsement by the Chair.

  Decision 005 - Authorisation Granularity

  Decision 006 - KYC Status

  Decision 007 - Purpose Of Product Info

  Decision 008 - Use Of Pluralisation

  Decision 009 - ID Permanence

  Decision 010 - Standard HTTP Headers

  Decision 011 - Error Handling

- there were four proposals open for feedback:

  Decision Proposal 012 - Payload Naming Conventions And Structures

  Decision Proposal 013 - Primitive Data Types

  Decision Proposal 014 - Handling Of Union Types

  Decision Proposal 022 - Paging

The fourth stream is **development of a Data Sharing and Release Bill**, a process led by the Data Legislation Team of the Office of the National Data Commissioner (**NDC**) This Team is currently situated within the Department of Prime Minister and Cabinet (**PM&C**) and led by the new National Data Commissioner (https://www.datacommissioner.gov.au/).

PM&C released the “New Australian Government Data Sharing and Release Legislation: Issues paper” (https://www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation) for consultation in July 2018. 108 submissions were received in response. Non-confidential submissions were published on 4 October 2018 (https://www.pmc.gov.au/public-data/data-sharing-and-release-reforms/submissions).

Development of the Data Sharing and Release Bill is likely to run to a different timetable to development of the CDR Bill and related CDR materials.

2 The CDR Bill

The CDR Bill as now available as an ‘Exposure Draft’ for public comment will likely be amended and then introduced by the Australian Treasurer in some form into the Federal Parliament before end Q1 2019.

The CDR Bill might then (subject to many political uncertainties) be enacted to enter into operation from Q3 2019.

Given the political imperative for both Liberal and Labor to be seen to be ‘doing something about the banks’ and ’about high energy prices’, it is likely that the CDR Bill will be pushed

through the Parliament, although possibly with significant amendments and possibly limited in prospective operation to certain sectors (i.e. banking, energy and telecommunications).

CDR and accredited data recipients

A 'consumer data right' (**CDR**) is a right for a customer of any size of a particular service provider that is within a class of service providers of a particular class of products as may be designated by the Australian Treasurer to require that service provider to make available to (a) that customer, or (b) an accredited data recipient nominated by a customer.

In order to have CDR data relating to a consumer disclosed to an entity, the entity must hold an accreditation as a accredited data recipient.

Accreditation will initially be managed by the ACCC, which will be the 'Data Recipient Accreditor'.

An 'accredited data recipient' might be (by way of some examples) (1) a comparison service provider such as iSelect, (2) a new service provider (i.e. another bank), (3) an unconventional service provider such as a service aggregator or a fintech, wither onshore or offshore, (4) another customer representative or agent.

Accredited data recipients are entities holding CDR data as a result of CDR data being disclosed to them at the direction of a CDR consumer under the consumer data rules.

CDR data held by accredited data recipients can also include data derived from consumer CDR data (including de-identified or aggregate data which is derived from CDR data).

The Government announced that in some circumstances CDR consumers will be able to direct that their CDR data be provided to a non-accredited entity: in effect, 'out of the CDR system'. Data that has been derived from CDR data, such as financial reports compiled from transaction data, may also be transferred by a CDR consumer 'out of the CDR system'. The Government explained that CDR data might be directed by a customer to be provided 'out of the CDR system' to a customer's accountant or to an accounting service provider such as Xero, Quicken or MYOB. It is not yet clear how 'out-of-system' transfers will be permitted and controlled. The relevant permissions and controls are expected to be addressed in the CDR rules.

Other data that could be transferred to a non-accredited entity could include CDR data that does not relate to the CDR consumer, such as general product information.

Accreditation by the ACCC will be based on criteria established in the consumer data rules about accreditation.

While common criteria may be set to allow accreditation to be valid across sectors, the legislation provides flexibility for criteria to vary on a sector by sector basis.

Consumer data rules may (among other things):

- state criteria to be applied to persons applying to be accredited;
- state ongoing conditions which accredited entities must meet after accreditation has been granted;

- allowing for accreditation to be provided at different levels taking into account the different risks associated with the kind of activities undertaken within a designated sector or the kinds of applicants.

The ACCC may randomly audit accredited data recipients to ensure that the recipient's use of data is in accordance with consumer consents and that security protections are in place.

Derived (including value added) data

The draft CDR Bill does not provide clear guidance as to what data sets may be subject to the CDR Bill and what data is not. One suggested approach is:

- No value-added data about customers which is created by data holders using their own intellectual property and resources (e.g. data that is created by a data holder to infer the likelihood of interests, behaviours, or preferences of its customers) should be subject to the CDR Bill. This is because value-added data is valuable proprietary information of the data holder/custodian, with such value created through significant investment in data collection, enrichment and analytics.

- Data that is volunteered by a customer could be included as a CDR data set under the CDR Bill, but only where the information provided by a customer is consistently collected by, and volunteered to, all data holders in that sector. By contrast, where an individual data holder has made a significant investment in the capture, checking and maintenance of more detailed customer data, this more transformed data might not be within the CDR.

- Data that is provided by a data holder to a customer (e.g. via invoices, statements or transaction records) might reasonably be regarded as CDR data, to the extent that this information does not comprise value-added data of the data holder. So this might include basic aggregations or representations of data, and other basic transformations of data through data cleansing to reconcile inconsistent entries or to format data in a way that the customer may find easier to understand or use. Contrast where a data holder has used significant intellectual property and investment to provide additional, value-added data to the customer: this value-added data might not be within the scope of the CDR Bill.

The currently proposed procedural safeguards in the draft CDR Bill do not ensure that value-added data sets are not designated as CDR data for a particular sector.

Reciprocity

One of the most unclear aspects of Australian open banking proposals is the discussion as to "reciprocity" and application of that principle to "equivalent data".

The problem partly arises because the authors of the Open Banking Review Report appear to have accepted views that 'reciprocity' of 'equivalent data' is required to ensure 'fairness' as between banks and intermediates holding customer transaction data. The Open Banking Review Report stated (Recommendation 3.9 – reciprocal obligations in Open Banking) as follows:

> Entities participating in Open Banking as data recipients should be obliged to comply with a customer's direction to share any data provided to them under Open Banking,

plus any data held by them that is transaction data or that is the equivalent of transaction data. (pp44-45)

The context of that recommendation was the preceding recommendation that obligation to share data at a customer's direction should apply to all Authorised Deposit-taking Institutions (ADIs), other than foreign bank branches phased in and beginning with the largest ADIs (p43).

This then led the authors of the Open Banking Review Report to make the following propositions:

- Once banking data is transferred by the customer's bank to a data recipient the notion of it being still banking data becomes strained. At best it is data that met the description while it was in the hands of the bank, but in the hands of the third party it is not a record of banking transactions with them.

- However, it would seem unfair if banks were required to provide their customers' data to data recipients such as FinTechs or non-bank credit providers, but those data recipients were not required to reciprocate in any way, merely because they were not banks and therefore did not hold 'banking' data.

- An Open Banking system in which all eligible entities participate fully — both as data holders and data recipients — is likely to be more vibrant and dynamic than one in which non-ADI participants are solely receivers of data, and ADIs are largely only transmitters of data.

- This proposal is essentially about banking data. A concern for fairness that leads to a principle of reciprocity should not be allowed to unduly extend the scope of the system by stealth.

Recommendation 3.9 appears to have been intended to empower a customer to direct an accredited data recipient (ADR1) to provide "equivalent data" to a bank (e.g. B2) or an other accredited data recipient (ADR2) in circumstances where the customer had earlier directed a bank (B1) to provide regulated (open banking transaction) data sets to ADR1.

However, "equivalent data" is not only that customer's transaction data as first provided by B1 to ADR 1 (at the request of that customer): it also includes any customer data volunteered and provided by the customer to ADR1, (subject to some exclusions); data relating to the lending of money on credit; and data relating to the payment of monies to which "they" [ADR1] are either a party or that they [ADR1] are facilitating (p44).

Note that a direction can only be initiated by the customer, and that customer could specify in its direction to ADR1 the categories of equivalent data that ADR1 is directed to make available to ADR2/B2.

The reason for description of this proposed obligation as 'reciprocity' and the suggestion that it is required to effect 'fairness' appears to stem from an argument that because ADR1 gets the benefit of use of customer data at least initially provided by one of the regulated banks, it is 'fair' that ADR1 must 'reciprocally' make available equivalent data to be available to ADR2/B2 at the request of the customer. But it is not clear why 'fairness' as between the largest ADIs and other ADRs should be a relevant consideration for a framework that is allegedly intended to give consumers an improved ability to switch between financial services

providers. In any event, implementation of the proposal would create substantial complexity 'within the system' and might significantly increase barriers to entry of ADRs, which otherwise need to be able to ingest data but do not need to implement an outward facing capability for identity verification, data ordering-up and provisioning.

The meaning of, and need for, 'reciprocity' continue to be in spirited debate.

3 Is Australia out of step?

There are three important comparable (but quite different) regulatory initiatives underway in other jurisdictions:

- Implementation of open banking in the United Kingdom, with implementation currently administered by the Financial Conduct Authority.
- Implementation of PSD2 in the European Union.
- Implementation in the European Union of portability of personal data under the GDPR.

There is extensive commentary readily available in relation to each of these initiatives. Accordingly, they are not addressed in this status report.

By contrast, there is limited material available as to comparable regulatory initiatives in Asia. For this reason known regulatory initiatives in Asia are outlined below.

Hong Kong

The Hong Kong Monetary Authority (**HKMA**) published in July 2018 an Open Application Programming Interface Framework (**OAIPF**) with process and timetable for Open APIs. Implementation of OAIPF is proposed to be compulsory for HK's largest banks, with others funacial service providers to follow.

HKMA proposes to follow a four-phase approach, with data standards to largely follow new EU technical standards.

- Phase I: Product and service information to third party providers (**TPPs**) can access banks' product information (e.g. for product comparison sites) – by end Q4 2018
- Phase II: Subscription and new applications for products/services - banks will deploy core-banking open API functions to accept new account/product applications (eg, customer acquisition via TPPs) – by end Q3 2019
- Phase III: Account information - account information, retrieval by TPPs of account information, and other bank products such as bill payment history. Includes investments and insurance policies. Timetable for development over next 12 months.
- Phase IV: Transactions - allowing TPPs to process customer requests, such as funds transfers, bill payments, and investments and insurance. Timetable for development over next 12 months.

Singapore

The Monetary Authority of Singapore (**MAS**) supports a voluntary scheme, but no mandating and no timetable.

The "MAS API Playbook" provides guidance to financial institutions, FinTechs and other entities as to API-based system architecture.

The "MAS FI API Register" lists available open APIs, e.g. Transactional APIs (payments, funds transfer, settlements) and Product APIs (financial product details, rates and branch/ATM locations).

DBS claims to have 'the largest banking API platform in the world' with over 155 APIs for a range of services.

Malaysia

Bank Negara Malaysia (**BNM**) recently (18 Sept 2018) published draft specs for Open APIs and guidance 'encouraging' their use for data transfers to third-party providers (**TPPs**), starting with product info for SME loans, credit cards and motor insurance.

The current proposal is draft and voluntary, with no timetable.

Japan

The Government of Japan promotes adoption of open APIs by banks and credit card companies via policy measures, technical standards and a regulatory sandbox. There is a stated target of 80 banks to deploy open APIs by 2020.

The Banking Act of Japan was amended in June 2018 to facilitate open API architecture between financial institutions and regulated Electronic Payment Intermediate Service (**EPIS**) providers. Banks must publish interface standards for EPIS and must not cannot discriminate against EPIS providers that meet these standards. Financial institutions are to develop fully Open APIs for EPIS providers by June 2020.

Japan already has complex and restrictive data protection laws.

South Korea

The Government of South Korea is encouraging some open banking initiatives, including launch in 2016 of Joint FI Fintech platform for inquiry and transfers using standardised APIs and testbed for services using these APIs.

The scheme is currently voluntary, with no timetable.

Regulation facilitates of internet only banks, including K-bank and Kakao Bank.

South Korea has complex and restrictive data protection laws.

Thailand

The Bank of Thailand (**BOT**) professes support for fintechs including through regulatory sandbox and collaboration with Singapore MAS.

There is limited availability of bank APIs, no required or standardised open banking APIs.

BOT has announced that 14 Thai banks in 'Thailand Blockchain Community Initiative' will use Hyperledger Fabric blockchain technology for a shared trade finance platform including digitised Letters of Guarantee.

Indonesia

There is currently limited availability of bank APIs, no required or standardised open banking APIs.

There have been some relevant initiatives by Bank Indonesia (**BI)** include provision of regulatory sandbox and establishment of BI Fintech Office

Most fintech activity in Indonesia is by payment system operators, followed by P2P operators. There are currently 34 fintechs registered by BI, with one fintech in the regulatory sandbox

Indonesia has data localisation requirements and licensing restrictions that impede entry of foreign fintechs.

Peter G Leonard
Principal, Data Synergies
Professor of Practice, UNSW Business School
Consultant, Gilbert + Tobin Lawyers

pleonard@datasynergies.com.au

5 October 2018