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

**Peter Leonard**
**Principal, Data Synergies and Professor of Practice, UNSW Business School**

## Open banking

On 21 December 2018, the Australian Treasurer announced[1] the following phased timetable for introduction of open banking:

- From 1 July 2019, the big four Australian banks (Commonwealth, NAB (National Australian Bank), Westpac and ANZ Bank) will be required to publicly share product data about credit and debit cards, deposit accounts and transaction accounts.
- From 1 July 2019, the ACCC and CSIRO Data 61 will launch a pilot program with the big four banks to test the performance, reliability and security of the Open Banking system.
- From 1 July 2019, the ACCC will begin formally engaging with parties interested in accreditation as accredited data recipients.
- Consumers and FinTechs will be invited to participate in these pilots and the ACCC and Data61 will also work closely with other banks (that is, banks that are not big four Australian banks) who have expressed an interest in participating in open banking earlier than may be envisaged for extension of the CDR to these other banks.
- On 1 February 2020, product and consumer data for mortgage accounts will be made available.
- Once the Australian Competition and Consumer Commission (**ACCC**) is comfortable with the robustness of the system, banks will publicly share consumer data about credit and debit cards, deposit accounts and transaction accounts, which will be no later than 1 February 2020.

The mechanism for introduction of open banking will be introduction of a new Consumer Data Right (**CDR**), a right of portability of designated consumer data that is exercisable by 'consumers', 'with consumers broadly defined to potentially include any customer of designated banks. The Federal Government has also stated its intention that the Consumer Data Right (**CDR**) will "be progressively applied sector by sector across the whole economy, beginning in the banking sector". The CDR is not limited to personal data, and it is not limited to data relating to individual natural persons. The CDR is potentially more interventionalist and impactful than the much-discussed right of data portability under Article 20 of the General Data Protection Regulation of the European Union. Creation of the CDR will be a remarkable, globally unprecedented legislative intervention.

[1] http://jaf.ministers.treasury.gov.au/media-release/077-2018/

The Treasury Laws Amendment (Consumer Data Right) Bill 2019[2] (**CDR Bill**) was introduced into the Australian Parliament on 13 February 2019. The CDR Bill is the culmination of political initiatives to introduce open banking. There has been a remarkably short period between inception (in late 2017) and likely implementation. Earlier drafts of the Bill had been released as exposure drafts for comment by interested stakeholders. Given the political imperative for both Liberal/National Coalition Government and the Australian Labor Party to be seen to be 'doing something about the banks' and 'about high energy prices' before the Australian Federal Election, it is likely that the CDR Bill will be pushed through the Australian Parliament. The CDR Bill may be passed with significant amendments and possibly limited in prospective operation to certain sectors (i.e. banking, energy and, but it is likely that the CDR Bill in some form will be enacted in Q2 2019, prior to an Australian Federal Election.

The current Federal Government envisages:

- A three-phase introduction of a CDR for certain retail banking products provided by specified classes of banks.
- 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.

**Policy rationale for the CDR**

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.

[2] Available at https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6281

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

- The CDR is being created to facilitate price and product comparison and lessen friction and inconvenience that is currently experienced by consumers when moving between service providers. The right of portability is not intended to be a right of ownership or control of relevant data by consumers: rather, it is a right of each customer to move (port) data about them and their transactions in a convenient electronic form, should the customer so wish. Although the right is principally a tool for consumer empowerment, creation of a CDR for an industry sector and product type may lead to profound supply side effects on the structure of that industry sector and strengthen cross-sector linkages, including (but not only) through facilitating growth of intermediaries and gateways to assist, guide or execute comparison and switching by consumers. The CDR may accordingly reshape the structure and competitive dynamics of supply side markets, even where it is created by Ministerial designation in a sector in order to empower consumers to compare offerings and switch between providers, rather than to further a policy objective of reshaping the supplier side competitive landscape.

**How will a CDR be created in each sector and how will it operate?**

The CDR Bill establishes a framework to enable the CDR to be applied to various sectors of the Australian economy over time. The framework relies on four key participants: consumers, data holders, accredited persons and accredited data recipients, and designated gateways. However, the system is flexible and may also provide, through the consumer data rules, for interactions between consumers and non-accredited entities.

CDRs will be regulated, initially, by the Australian Competition and Consumer Commission (**ACCC**) and the Australian Privacy Commissioner within the Office of the Australian Information Commissioner (**OAIC**). The OAIC will have primary responsibility for complaint handling under the CDR framework, with "particular attention to the privacy of individuals and the confidentiality of small businesses". The ACCC will oversee the CDR from a consumer and competition perspective with particular focus on systemic enforcement. The ACCC is also responsible for establishing the consumer data rules, in consultation with the OAIC.

If the sector is to have a gateway the Minister will designate this person in the instrument. A gateway is a person whose role it is to facilitate the transfer of data between certain participants in the CDR regime.

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. 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.

Accreditation by the ACCC will be based on criteria established in the consumer data rules about accreditation. Accreditation will initially be managed by the ACCC, which will be the 'Data Recipient Accreditor'.

The Government previously 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, but it is expected that will be addressed in the CDR rules.

A 'consumer data right' 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 relevant Minister (currently 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, designated data. The Minister may designate an industry sector by specifying classes of information and those classes for which a fee can be charged, and relevant data holders.

The designation instrument will also set out the earliest day that the CDR will apply. Certain information may be subject to the CDR even though it was generated and collected prior to the commencement of the CDR, but the instrument cannot specify a day earlier than 1 January two years before the instrument is made.

The CDR Bill places a number of obligations on the Minister, the ACCC and the Privacy Commissioner about factors that must be considered prior to the designation instrument being made. The CDR Bill also requires that the ACCC undertake consultation, including public consultation and consultation with the primary regulator of the sector proposed to be designated. "However, in the banking sector and energy sector these obligations do not apply because this consultation has already taken place."

Within a designated sector the types of data the CDR will apply to will be outlined via the designation instrument as well as the consumer data rules and, broadly speaking, the manner of making that data available will be established by the consumer data rules and the data standards.

The Explanatory Memorandum to the CDR Bill provides the following examples:

> Example 1.1
>
> EVBank is a major Australian bank with many customers. It collects transaction information for each of its customers reflecting the debit and credits on accounts.
>
> The designation instrument lists transaction information generated from providing a service or good related to a banking business as a "class of information".

The designation instrument also lists authorised deposit-taking institutions as a person holding such information.

EVBank is a data holder for the data it generates and collects that is listed in the designation instrument.

Example 1.2

LendMeMoney is an accredited data recipient. It holds an Australian credit licence and provides credit to its customers. As part of this service it generates and holds lists of the transactions for each consumer.

For the data that it holds about its own customers which reflects the credit services it provides its customers, LendMeMoney would be a data holder and potentially subject to access rights under the consumer data rules.

Example 1.3

EVBank became an accredited person so that it is able to receive CDR data.

Martin switches to EVBank. He uses the CDR to transfer his historical data from Bank A to EVBank. EVBank receives this data comprising banking information of the type EVBank ordinarily holds. EVBank collects that data about Martin as an accredited data recipient.

The consumer data rules provide that if a CDR consumer transfers their banking business, the recipient bank is able to treat banking information transferred under the consumer data rules as if the recipient bank was the data holder of the information.

EVBank will be considered a data holder for Martin's historical banking information and this information will be subject to the APPs.

Example 1.4

EVBank became an accredited person so that it is able to receive CDR data.

Sean switches to EVBank. EVBank offers an energy consumption monitoring and alert service. Sean uses the CDR to monitor his energy usage data from Energy A.

EVBank receives this data comprising energy information of the type EVBank does not ordinarily hold. EVBank collects that data about Sean as an accredited data recipient. EVBank would be considered an accredited data recipient for the energy information it receives and would need to meet the associated Privacy Safeguards.

The data sets of CDR data can relate to natural and legal persons, for example a partnership or incorporated business of any size. However, the class of consumers on which the CDR is conferred may be narrowed on a sector by sector basis through the designation process and the rule-making process. The Explanatory Memorandum states by way of example "ïn the banking sector, it is expected that the access and transfer right under the rules will not extend to large customers who have bespoke arrangements", but then continues with the following example:

Example 1.6

TBM is a large corporation specialising in manufacturing bicycle parts. It obtains banking services from one of the medium sized banks operating in Australia, Stately Bank. Following the designation of the banking sector as a CDR sector, TBM is keen to send its banking data to a FinTech, McDanMoney, to check whether it is getting the best banking services.

The consumer data rules provide that large consumers have the right to access data and request a transfer of their data where the consumer receives services that are generally available.

Stately Bank has data about TBM that is covered by the designated data set applying to the banking sector, and TBM uses banking services that are generally available (and not bespoke), TBM is a CDR consumer and is able to participate in the CDR system.

**Which data sets may be designated as CDR?**

Designated data may, or may not, be personal information about individuals, and may, or may not, be value added, enhanced or transformed from basic customer details and formatted or statement summarised transaction data. The definition of CDR data includes data that is 'derived' from data listed in the designation instrument and accordingly "Privacy Safeguards" (as outlined below) continue to apply to CDR data that relates to a consumer even if that data is received and subsequently transformed in the hands of the accredited data recipient.

The definition of CDR data is therefore very broad. The scope of data to be included within a Ministerial designation limited only by criteria which the Minister is to be apply in determining a designation and processes that the Minister must undergo before finalising that designation. There are however some proposed statutory limits on the data sets that data holders may be required to give access to:

- For data that relates to a CDR consumer, a data holder can only be required to disclose that data to an accredited person, designated gateway or the consumer themselves. In this circumstance the data is also limited to data that is specified in the instrument and does not include data that is derived from data specified in the instrument.[3]

- For data about a product, good or service, a data holder can only be required to disclose data about the eligibility criteria, terms and conditions, price, availability or performance of the product, good or service. Disclosure about the availability or performance can only be mandated where this data is publicly available.[4]

**Who pays, for which CDR data sets?**

The Explanatory Memorandum states:

[3] Schedule 1, item 1, subsection 56BD(1)

[4] Schedule 1, item 1, subsection 56BF(1)

> It is anticipated that the majority of designated data sets would be made available for free. Only in rare circumstances, for example, where the marginal cost of disclosure would be significant, would it be appropriate for a data set to be designated as a chargeable data set.

The CDR Bill introduces the concept of 'chargeable data', where the Minister states in the designation instrument that specific persons can charge a fee for the use or disclosure of the data, in such circumstances as the Minister may state in that instrument. If data is not listed as chargeable data in the designation instrument the person cannot charge a fee for the data. Similarly, the person cannot charge a fee for the use or disclosure where the circumstances specified in the designation instrument have not been met.

The Explanatory Memorandum to the CDR Bill provides the following examples:

> Example 1.7
>
> Data holders in sector X are designated in respect of data set A. Data set A is intellectual property.
>
> There are strong competition, consumer, and privacy benefits to the designation of data set A.
>
> The Minister designates data set A as a chargeable data set for the use of data set A. Data holders are able to set their own reasonable fees for the disclosure and licence to use data set A.
>
> Example 1.8
>
> Data holders in sector Y are designated in respect of data set B. Data holders in sector Y are not legally required to collect or hold data set B, but choose to do so for their own reasons.
>
> There is a strong consumer welfare benefit to consumers being able to access data set B.
>
> There is compelling evidence that if data set B is designated, data holders in sector Y would stop collecting and holding data set B. If allowed to charge a fee for the disclosure of data set B, data holders in sector Y would continue to collect and hold data set B.
>
> The Minister designates data set B as a chargeable data set for both the disclosure and use of data set B. Data holders are able to set their own reasonable fees for the disclosure and licence to use data set B.
>
> Example 1.9
>
> Data holders in sector A are designated in respect of data set Z. Data holders incur initial costs of $100 million to meet their obligations under CDR, but their additional costs per disclosure of CDR data are minimal.

> The Minister designates data set Z and does not specify that data set Z is a chargeable data set. Data set Z is a fee free data set and data holders are not able to set fees for the disclosure or use of data set Z. 1.

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.

Data relating to a consumer will be subject to privacy safeguards specified in the CDR Bill once a consumer requests its transfer to an accredited recipient. These safeguards are comparable to the protections for individuals contained in the Australian Privacy Principles under the Privacy Act 1988. The safeguards provide broadly consistent protections for consumer data of both individuals and business enterprises, with a few more restrictive requirements on participants than those applying under the Privacy Act 1988.

Consumer data rules, as determined by the ACCC, 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.

**Reciprocity**

One of the most confused areas of discussion in Australian open banking proposals to date has been "reciprocity". The authors of the Open Banking Review Report[5] 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[6] 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:

[5] https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf

[6] Recommendation 3.9 – reciprocal obligations in Open Banking

- 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.

In any event, the CDR Bill will empower the ACCC to write rules requiring certain accredited data recipients to provide consumers access to CDR data, or the ability to request transfer of CDR data, to accredited persons, when a consumer has made a valid request. Given that the CDR Bill itself not provide further detail, we must rely upon the discussion in the Explanatory Memorandum as the only currently available statement of the Government's intention:

1.127 The principle of reciprocity may apply in three circumstances. First where an entity is included in a designation instrument but there is not a consumer data rule requiring that data holder to disclose that information.

1.128 An example of this would be where a small ADI is not required to disclose banking information at a consumer's request before 1 July 2020. However, if the small ADI becomes an accredited data recipient before this date, the consumer data rules may require the small AD to transfer data at the request of the consumer.

1.129 Similarly, the principle of reciprocity may apply where an accredited data recipient is not included in the designation but holds data that it has generated or collected itself outside of the CDR. For example, a non-ADI lender would hold data that is included in the designation instrument. The consumer data rules may require the accredited data recipient to transfer data at the request of the consumer.

1.130 The final circumstance where the principle of reciprocity may apply is where the ACCC writes rules requiring accredited data recipients to disclose data that they have received through the CDR to another accredited person at the consumer's request.

1.131 If an accredited data recipient does not hold data that falls within a class designated in a designation instrument, reciprocity cannot apply. That is, reciprocity only applies to data included in the designation instrument. This is because the transfer of the data needs to be supported by data standards to occur efficiently. 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.

We can expect continuing, spirited and confused debate as to the circumstances in which there is a valid public policy rationale for 'reciprocity'.

**Related releases**

There were a number of related releases in late December 2018, including:

- A Privacy Impact Assessment (**PIA**) of the previous draft CDR Bill (the Exposure Draft Treasury Laws Amendment (Consumer Data Right) Bill 2018) and proposed implementation of the CDR in banking, which PIA was open for consultation and submissions until 18th of January[7].

- ACCC's Rules Outline[8], which sets out the ACCC's current position on development of the CDR Rules. The CDR Rules will be the key subordinate instrument addressing how open banking will be implemented in relation to designated products of the big four Australian banks. In line with the Treasurer's announcement on 21 December 2018, the Rules Outline reflects the commencement schedule with 1 July 2019 being the date for product reference (generic) data being made publicly available, and 1 February 2020 being the date by which the remaining obligations to share the first tranche of consumer data will commence. The Rules Outline also highlights a number of areas where the ACCC is further considering the implications of the revised timeline for the scope of version one of the Rules. The Rules Outline assumes that the CDR Bill will be passed in the first quarter of 2019 and is intended to provide guidance to stakeholders, including designated data holders, potential data recipients, and consumers, on what "version one of the Rules" will require of CDR participants. The policy positions in the Rules Outline will be reflected in the draft Rules which the ACCC intends to publish for consultation in the first quarter of 2019. After consultation on the draft Rules, the ACCC may make further refinements before submitting version one of the Rules to the Treasurer for consent.

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

[7] Available at https://static.treasury.gov.au/uploads/sites/1/2018/12/CDR-PIA.pdf

[8] Available at https://www.accc.gov.au/focus-areas/consumer-data-right/rules-outline

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 closely coordinated with development by CSIRO/Data61 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, "working closely with the ACCC as lead regulator of the Consumer Data Right, supported by the Office of the Australian Information Commissioner (OAIC)".[9]

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 being published. Draft work stream outputs from Data61 which will form the technical standards for the CDR include:

- Draft API Standards (v0.2.0)[10]
- A draft information security profile (v0.1.0)[11]
- An independent review of progress in development of standards[12].

**Extension of the CDR beyond open banking**

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" closed in 2018[13]. 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. Data61 had been commissioned by the Federal Government to prepare and release a briefing/information package on how technical standards may be implemented across the energy ecosystem, applying Data61's experience as to implementation in the banking sector. Having regard to the forthcoming Federal election and NSW State Election and the political sensitivity of energy policy, it is difficult to predict the likely scale and timetable for expansion of the CDR to the energy sector.

[9] Available at https://data61.csiro.au/en/Who-we-are/Our-programs/Consumer-Data-Standards

[10] https://consumerdatastandardsaustralia.github.io/standards/#introduction

[11] https://consumerdatastandardsaustralia.github.io/infosec/#introduction

[12] https://consumerdatastandards.org.au/christmas-2018-working-draft/

[13] http://www.coagenergycouncil.gov.au/publications/call-submissions-facilitating-access-consumer-energy-data

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

**Development of a Data Sharing and Release Bill**

The CDR workstreams as described above are the principal areas of current regulatory activity flowing from the Government's implementation of the recommendations of the Productivity Commission in its Data Access and Use Report[14].

A less publicised but important parallel workstream 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.[15]

The Productivity Commission had identified a "lack of trust by both data custodians and users in existing data access processes and protections and numerous hurdles to sharing and releasing data are choking the use and value of Australia's data", and recommended "the creation of a data sharing and release structure that indicates to all data custodians a strong and clear cultural shift towards better data use that can be dialled up for the sharing or release of higher-risk datasets". The Australian Government's response stated that Greater access to public sector data with a consistent approach to managing risk can improve research solutions to current and emerging social, environmental and economic issues" and stated the Federal Government's commitment to:

- "Establishing a National Data Commissioner to implement and oversee a simpler, more efficient data sharing and release framework.
- Introducing legislation to improve the sharing, use and reuse of public sector data while maintaining the strong security and privacy protections the community expects.
- Introducing a Consumer Data Right (CDR) to allow consumers to share their transaction, usage and product data with service competitors and comparison services."

The Data Sharing and Release Bill, when drafted and enacted, will address the first two commitments.

Although there have been consultations with interested stakeholders to inform drafting of this Bill, no Exposure Draft has been released. Further progress of this commitment remains unclear. In any event, development of the Data Sharing and Release Bill will likely to run to a different timetable to development of the CDR Bill and related CDR materials.

**Is Australia out of step?**

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

[14] (https://www.pc.gov.au/inquiries/completed/data-access#report

[15] https://www.datacommissioner.gov.au/

- 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**) in September 2018 published draft specs for Open APIs and guidance 'encouraging' their use for data transfers to third-party providers, 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

16 February 2019