Deloitte.

Shaping the Future

Consumer Data Right

Deloitte Submission to the Inquiry into Future Directions for the Consumer Data Right

21 May 2020

Introduction

In March 2020 the Treasury released the Terms of Reference and an Issues Paper for its Inquiry into Future Directions for the Consumer Data Right.

Deloitte is pleased to provide our observations on future considerations for the Consumer Data Right in this submission. We continue to believe that open data has significant potential to enhance the Australian economy.

In our submission on the draft CDR legislation we noted that finding the balance between achieving a sound, stable system and encouraging competition and innovation is a continuing challenge and an evolving challenge in sectors being disrupted by technological change. This trade-off between stability and competition is only amplified in the current circumstances. Already we have seen calls by some for the introduction of the CDR to be delayed.

Our submission includes comments on the following matters:

1. The benefit of creating a more **consistent experience for consumers** and citizens in how data they provide is collected, used, shared and stored, together with consistent rights and protections.
2. The opportunity to **extend the CDR** principles to the **original collection and use** of data and not just data sharing.
3. The opportunity to **extend the CDR** principles to **data citizens share with government** agencies.
4. The importance of both **financial literacy and data literacy**, and ultimately financial and data consciousness, in addressing the behavioural biases that can constrain consumers' information gathering and decision making processes, and their role in enabling consumers to confidently and safely engage in the digital economy in a way that enables them to realise the benefits of greater competition and new propositions.
5. The benefits of allowing potential competitors from **jurisdictions with similar data sharing rights** and protections to operate in Australia.
6. The potential benefit of introducing a **'best interests' duty** for businesses using CDR data to operate as information intermediaries, including in particular comparator websites.
7. The **importance of trust** in creating the conditions in which consumers will confidently share data.
8. The potential that CDR has to blur industry boundaries, and the importance, wherever possible, of **aligning regulatory requirements** as the CDR is extended to other sectors.
9. The importance of ensuring that the **consent process is comprehensible** as potential data sharing arrangements increase significantly as additional sectors are added.
10. The opportunities presented by **write access** – both payment initiation and account opening – and the role it could play in addressing consumers' behavioural biases.
11. The importance of **aligning requirements**, including consent processes, enforcement and penalties, **across** all **payment mechanisms** and particularly **NPP**.
12. The potential **role of digital ID** in enabling consumers to more easily participate in data sharing under CDR.
13. The importance of **anticipating the consequences of an open data** economy on the **conduct** considerations of fairness, transparency, vulnerability and suitability and ensuring that the regulatory framework provides appropriate protection for issues which could emerge in an open data economy.

Future role and outcomes of the Consumer Data Right

The Inquiry invites submissions on the future roles that could be performed by the Consumer Data Right, the future outcomes which could be achieved, and what is needed for this to happen.

The original Productivity Commission Inquiry Report into Data Availability and Use noted how the exponential growth in data generation and usability 'has enabled a kaleidoscope of new business models, products and insights'.[1] In addition to the exponential growth in the number and size of data sets themselves, data sharing has the potential to see exponential growth in the linkages of data sets.

This brings significant opportunities for the creation of value for consumers, citizens and society, but also amplifies the risks to privacy from re-identification and from data breaches and has the potential to introduce new conduct issues associated with the use of these data sets.

At the heart of delivering the benefits from successful economy-wide data sharing is trust – trust in the data sharing framework, trust in the actions of data holders and data recipients, and trust in the government and regulators.

The Issues Paper correctly highlights that:

> *'By establishing a framework that introduces standardisation, systems which support trust between participants, clear liability and providing access to the data necessary to create innovative products and services, the Consumer Data Right has the potential to create the conditions for an Australian digitised ecosystem to grow.'*

Trust is enhanced where people, as both consumers and citizens, have a consistent experience with accessing and sharing data.

The UK Competition and Markets Authority noted that the benefits for consumers from providing their data will only be realised if consumers can trust the firms that collect and use it. The CMA outlined a range of practices for the collection and use of consumer data which support well-functioning markets: [2]

- *'Consumers should know when and how their data is being collected and used and be able to decide whether and how to participate. They should have access to information from firms about how they are collecting, storing and using data, so that they can select the firm that best meets their preferences.*
- *Firms should compete on the issues that matter to consumers, including the provision of clear and useable controls that enable consumers to manage data-sharing.*
- *Consumers and firms should share the benefits of using consumer data. Consumers may get a new or better service or lower prices because firms are becoming more efficient, or even trade their data for a direct financial reward. Firms may gain more sales or market share or become more profitable.*
- *The regulation of the collection and use of data should ensure the protection of essential rights such as privacy. The market can help achieve this goal where regulations encourage competition and choice, allowing a 'race to the top' by firms to offer consumers better services.*
- *Non-compliance with regulation should be tackled proportionately and effectively, so that firms and consumers can feel confident that the rules are being applied fairly.'*

[1] Productivity Commission, *Data Availability and Use, Inquiry Report*, Report No. 82, Canberra, 2017, page 2

[2] Competition & Markets Authority, *The commercial use of consumer data: Report on the CMA's call for information*, 2015, pp 7-8. See also: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf

In creating the future open data economy there are areas that could be enhanced in Australia:

1. Consistency of users' experience of the collection, use and storage of data by organisations to complement the consistent experience of data sharing that CDR enables.
2. Consistency of a person's experience as a citizen accessing and sharing data provided to government agencies with their experience as a consumer accessing and sharing data that they provide to organisations.
3. Developing consumers' financial literacy so that people are able to understand the potential benefits from participating in an open data economy.
4. Developing consumers' data literacy so that people are both able to participate in an open data economy and understand what they are participating in so they can do this safely.

Data Collection, Use and Storage

The Institute of International Finance (IIF) sets out three broad models which currently exist for data ownership, management, collection, use and storage:[3]

1. Individuals retain data ownership and consumer rights are given priority – this is the model adopted in the European Union (EU) with the General Data Protection Regulation (GDPR)
2. Large technology companies have access to and control over vast amounts of user data – this model is used in the United States with technology companies such as Facebook, Amazon and Google
3. Governments have more access to and control of user data – this state-backed technology model is used in countries such as China.

The IIF report notes that privacy concerns arise in the second and third models 'because individuals do not always know who has how much information about them, and how it is accumulated, stored, used or shared, leading to a loss of control over one's personal information.'[4]

Currently Australia's Consumer Data Right (CDR) is actually a consumer ***data sharing*** right. As CDR is implemented consumers will develop awareness that express informed consent is required for an organisation to share data about them with a third party, and that they can restrict the purpose and timeframe for which data they share with a recipient can be used.

However, to realise the full vision for an open data economy, the principles for consent set out in the CDR legislation could be extended to the original collection and use of data.

Some of the challenges that currently exist without this have been set out in the ACCC's digital platforms inquiry[5] and its review of customer loyalty schemes.[6] Others were set out in submissions on the CDR legislation[7] and the Rules Framework.[8]

These reviews and submissions highlighted a number of issues that risk undermining consumer confidence in how organisations collect, use, share and store data.

- Consumers have little meaningful control over how their data is collected used and disclosed. [9]
- There is a gap in privacy notice practices and data protection in Australia when compared with consumer expectations. [10]

[3] Institute of International Finance, *Digital Identities in Financial Services, Part 2: Responsible Digital Identities*, October 2019. See also: https://www.iif.com/Publications/ID/3596/Digital-Identities-in-Financial-Services-Part-2-Responsible-Digital-IDs

[4] Institute of International Finance (October 2019), page 7

[5] ACCC, Digital platforms inquiry, July 2019. See also: https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platforms-inquiry

[6] ACCC, Customer loyalty schemes review, December 2019. See also: https://www.accc.gov.au/focus-areas/market-studies/customer-loyalty-schemes-review

[7] For example, Consumer Policy Research Centre, *Submission to Treasury Laws Amendment (Consumer Data Right) Bill 2018 – Exposure Draft*, 7 September 2018

[8] For example, American Express, *Submission on the CDR Rules Framework*, October 2018, page 5

[9] ACCC (December 2019), page 34

[10] Nguyen, P. and Solomon, L., *Consumer Data and the Digital Economy*, 2018, as cited in Consumer Policy Research Centre (September 2018), page 2

- The majority of consumers were not aware that the privacy policies and terms of use limited the extent of control they retain over their user data. [11]
- The terms and conditions of privacy policies can prevent consumers from making informed choices that align with their privacy and data collection preferences, exacerbated by 'broad consents' and 'vague disclosures'. [12]
- Some consumers were unaware that agreeing to privacy policies and terms of use meant that they relinquished control over their personal information and organisations could use data to the extent outlined in that privacy policy. [13]
- It was very difficult for consumers to predict the long-term costs of data collection and factor these costs into their decision on whether to use a service. [14]
- Consumers are concerned about the sharing of their data with unknown third parties, with limited insight and control over how their data is shared. [15]
- Consumers may be confused about what data is moving through which regulatory framework.[16]
- Practices, such as direct marketing, may be permitted for consumer data that is initially collected, but not for the same data when it is shared with another organisation resulting in inconsistent outcomes for organisations and their ability to compete.[17]
- Data can be automatically transferred to digital platforms when consumers use some third-party apps, regardless of whether the consumer had an account with the digital platform or whether they were logged into the digital platform. [18]

The ACCC digital platform inquiry highlighted that even the term 'privacy policy' was a misnomer as these policies 'tend not to outline privacy protections for users but rather tend to set out the extent of permissions granted to digital platforms'. [19]

It is notable that during the Hayne Royal Commission a financial institution's "client protection" policy was described as 'Orwellian', 'entirely misleading' and 'nothing more than an elaborate attempt to exclude [the entity's] liability for the acts of its authorised representatives'. As we move towards an open data economy it will be important that privacy policies do not have the same fatal flaw that some "client protection" policies have been shown to have.

The ACCC's digital platforms inquiry noted that 'The volume of consumer data collected as well as the opportunities to interrogate and leverage such data, are expected to increase.' [20] The issues noted will be amplified as the CDR is extended to other sectors of the economy and more data is shared. As the ACCC noted, 'The combining of data from multiple sources can allow digital platforms or advertisers to build a profile that can be used to provide de facto identification of a consumer.' [21]

The ACCC recommended that the Privacy Act needed to be reformed 'in order to ensure consumers are adequately informed, empowered and protected, as to how their data is being used and collected.' [22]

These reforms would strengthen Australia's data rights, data protection and privacy legislation, and more closely align them with those set out in the EU's GDPR regime. These reforms would also provide a stronger foundation for the future of the CDR.

[11] ACCC (July 2019), page 383
[12] ACCC (December 2019), pp vii, 34
[13] ACCC (July 2019), page 383
[14] ACCC (July 2019), page 384
[15] ACCC (December 2019), pp vii and 34
[16] Consumer Policy Research Centre (September 2018), page 3
[17] American Express (2018), page 5
[18] The ACCC quoted research by Privacy International that at least 61% of third-party apps tested automatically transferred data to Facebook the moment a consumer opened the app. Privacy International, *How Apps on Android Shared Data with Facebook (even if you don't have a Facebook account)*, 29 December 2018, as cited in ACCC (July 2019), page 391.
[19] ACCC (July 2019), page 383
[20] ACCC (July 2019), page 3
[21] ACCC (July 2019), page 392
[22] ACCC (July 2019), page 3

Giving consumers confidence and clarity in all aspects of how their data is collected, used, shared and stored will help build people's trust, a critical enabler for a digital and open data enabled economy and an important element in enabling greater competition.

Recommendation 1

The CDR principles which allow consumers to share data should be extended to the collection, use and storage of their data to allow a consistent consumer experience and to help build consumer data literacy.

Citizen access to data provided to government

In September 2019 the federal government issued a discussion paper on Data Sharing and Release in Australia.[23] In Deloitte's submission on the discussion paper we noted that it excluded the release of information that a citizen has provided to a government organisation to that citizen or to a recipient with which the citizen chooses to share it.

The extension of data rights to include data on individuals held by government agencies was noted in the Productivity Commission's review of Data Availability and Use[24] and the extension of the CDR to include this data was explicitly recommended in submissions on the draft CDR legislation.[25]

The exclusion of a citizen's right to access and share information that they have provided to a government is also inconsistent with global data policies such as the EU's GDPR. The same data rights that apply to individuals under GDPR extend to data that a government agency collects about a citizen (as well as other individuals and data subjects that are not citizens).

The GDPR allows for exceptions which permit a government organisation to refuse to share certain data sets or to refuse to share data with certain individuals for national security and law enforcements reasons. Similar restrictions could be included in citizen access provisions which could be included in either or both the future of CDR and the federal government's data sharing legislative agenda.

The citizen access provisions could also note that the requirement for express informed consent before a citizen's data is shared with a third party does not apply to data which is shared with an accredited recipient under the data sharing provisions of the proposed federal Data Accountability and Transparency Act (DATA) legislation.

Recommendation 2

The CDR principles could be extended to data which consumers as citizens share with government agencies.

[23] Australian Government, Department of Prime Minister and Cabinet, *Data Sharing and Release Legislative Reforms Discussion Paper*, September 2019.
[24] Productivity Commission (2017, Finding 3.1, page 33
[25] For example, Business Council of Australia, *Submission: Response to the Treasury Laws Amendment (Consumer Data Right) Bill 2018*, September 2018, page 3

Financial Literacy

One of the potential impediments to the future of the Consumer Data Right and the creation of an open data economy is the low levels of financial literacy in Australia.

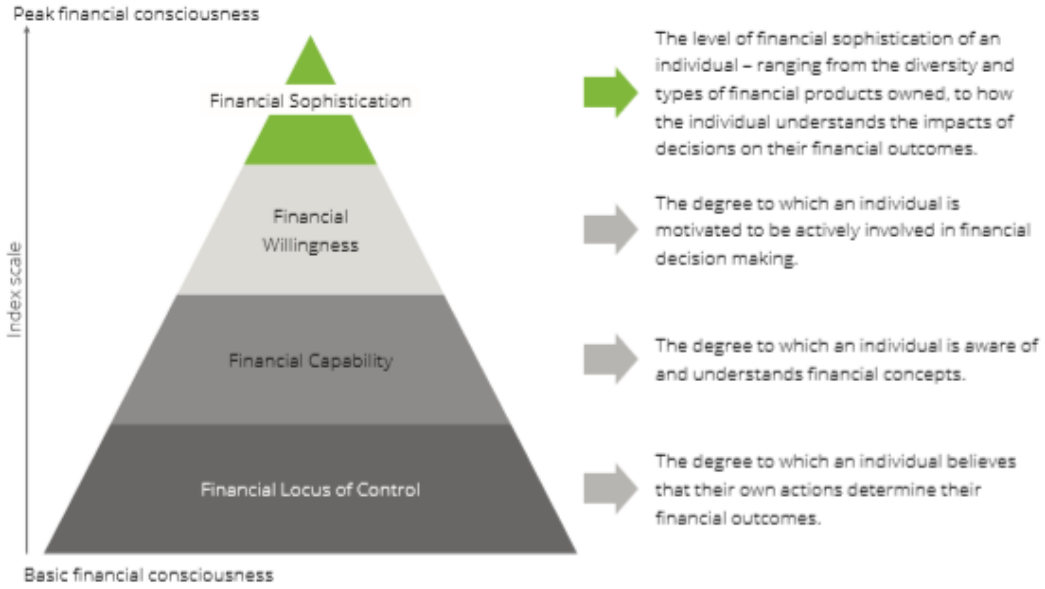
In Open Banking: Switch or Stick, Deloitte's report on the results of our survey on open banking and consumer behaviour, we highlighted the role of *financial consciousness* in creating the conditions where people were motivated to make informed decisions and act on them based on their understanding of their financial position.[26]

Deloitte developed the Financial Consciousness Index (FCI) which measures the extent to which a person is not just financially literate and capable, but whether they are able to affect their own financial outcomes.[27]

Financial Consciousness is comprised of four 'building blocks': the degree to which a person believes they have ***control*** over their financial outcomes, their financial ***capability*** to understand their finances, their financial ***willingness*** to be involved, and ultimately their financial ***sophistication*** (Figure 1).

These building blocks are a measure of not only how people *feel* but also how they then *act*.

Figure 1 Financial Consciousness Building Blocks



Source: Deloitte Access Economics, Dollars and sense: Compare the Market's Financial Consciousness Index, 2019

[26] Deloitte, Open Banking: Switch or Stick, October 2019. See also: https://www2.deloitte.com/au/en/pages/financial-services/articles/open-banking-survey-2019.html

[27] Deloitte was engaged by Compare the Market in 2018 to develop the Financial Consciousness Index (FCI). Deloitte Access Economics, *Dollars and sense: Compare the Market's Financial Consciousness Index*, 2018. See also: https://www2.deloitte.com/au/en/pages/economics/articles/dollars-sense-financial-consciousness-index.html)

People need to be ***financially literate*** to be able to understand their current financial position. But in a recent study by Deloitte less than half of Australians met the basic threshold for financial literacy. [28] In addition, we highlighted that there is growing evidence that the link between financial literacy and positive financial behaviours is weak. Financial literacy it seems has only a marginal effect, at best, on financial behaviours.[29]

If financial literacy changes people's ability to understand, ***financial capability*** changes people's capacity to act. Financial capability enables people to be actively engaged in the competitive process by searching for financial information and considering changing providers. But financial capability is not enough either.

As well as having the capability to act, it is also important that people are willing to make decisions and take actions. And that they understand the consequences of those decisions. It is important that they are ***financially conscious***.

Ultimately it is financial consciousness that influences whether a person searches for information, their ability to understand the information obtained, their willingness to act on this information, and the extent to which they are able to participate in sophisticated financial matters in a way that enables them to understand the potential benefits of their decisions, including a decision to change the provider of their banking or other products and services.

If consumers are going to take advantage of the benefits of open data as the CDR is applied to other sectors of the economy, it will be important for both government and industry to continue to build financial literacy, financial capability and financial consciousness in Australia.

Recommendation 3

The government should work with industry to further improve financial literacy and financial consciousness to support the realisation of benefits from data sharing and the CDR.

Data Literacy

Consistent data experiences can contribute to a data literate society. In charting the future of CDR and its role in building a digital, open data economy, enhancing Australia's data literacy is likely to be as important, if not more important, than improving financial literacy for Australia to realise the benefits of greater availability and use of data.

People need to be ***data literate*** to be able to understand what data they generate and with whom they are sharing it. But as the ACCC's digital platform inquiry seems to highlight, the link between data literacy and positive data protection and sharing behaviours appears to be weak.

This is not helped by lengthy terms and conditions on data usage and privacy, particularly when these are not read, let alone understood. Nor is it helped by a range of data practices, some of which are noted above, which are not consistent with community expectations.

---

[28] In recent surveys Deloitte asked respondents the 'big three' questions developed by researchers Annamaria Lusardi and Olivia Mitchell in 2014 to test financial literacy:

1. Suppose you had $100 in a savings account and the interest rate was 2% per year. After 5 years, how much do you think you would have in the account if you did not withdraw from the account? (More than $102, Exactly $102, Less than $102, Don't know)
2. Imagine that the interest rate on your savings account was 1% per year and inflation was 2% per year. After 1 year, how much would you be able to buy with the money in this account? (More than today, Exactly the same, Less than today, Don't know)
3. "Buying a single share from a company usually provides a safer return than an index fund." Is this statement true or false? (True, False, Don't know).

Deloitte's Financial Consciousness Index (FCI) prepared for Compare the Market noted that 40% of respondents answered all three questions correctly. (Deloitte Access Economics (2018)). In a survey in 2019 for the Australian Banking Association only 18% of respondents answered all three questions correctly. (Deloitte Access Economics (2019))

[29] A meta-analysis in the US of nearly 190 research studies showed that financial literacy and positive financial behaviours "are only slightly" related. Daniel Fernandes, John G. Lynch, Jr., and Richard G. Netemeyer, *The Effect of Financial Literacy and Financial Education on Downstream Financial Behaviors*, Working Paper, June 2, 2013. See also: https://www.nefe.org/What-We-Provide/Primary-Research/Effect-of-Financial-Literacy-on-Financial-Behavior as cited in Srinivas, Val, *Making financial literacy effective: How banks can help*, 12 September 2018. See also: https://www2.deloitte.com/us/en/pages/financial-services/articles/how-banks-improve-financial-literacy.html

The open data economy will be more effective, and consumer protection enhanced, if improved data literacy changes people's capacity to act, their ***data capability***. Data capability enables people to be actively engaged in the competitive process by searching for information and sharing information in an informed way when considering alternative products, services and providers. But like financial capability, data capability is unlikely to be sufficient either.

Data consciousness would enable people to provide express consent when deciding to share information; to provide informed consent based on an understanding of how the data recipient will be using the information shared; and to be able to understand the value that they are receiving in exchange for the data they are providing.

In Deloitte's report on open banking and consumer behaviour we asked people about their attitude to keeping up with technology.[30] We have classified those who saw this as extremely important or very important as Technophiles and those who saw it as extremely unimportant or very unimportant as Technophobes. These attitudes to technology can be used as a proxy for data literacy.

As the charts below highlight, greater data literacy is associated with higher education, greater levels of employment (particularly full-time) and higher household income.

Figure 2 Attitude to keeping up with technology: Education

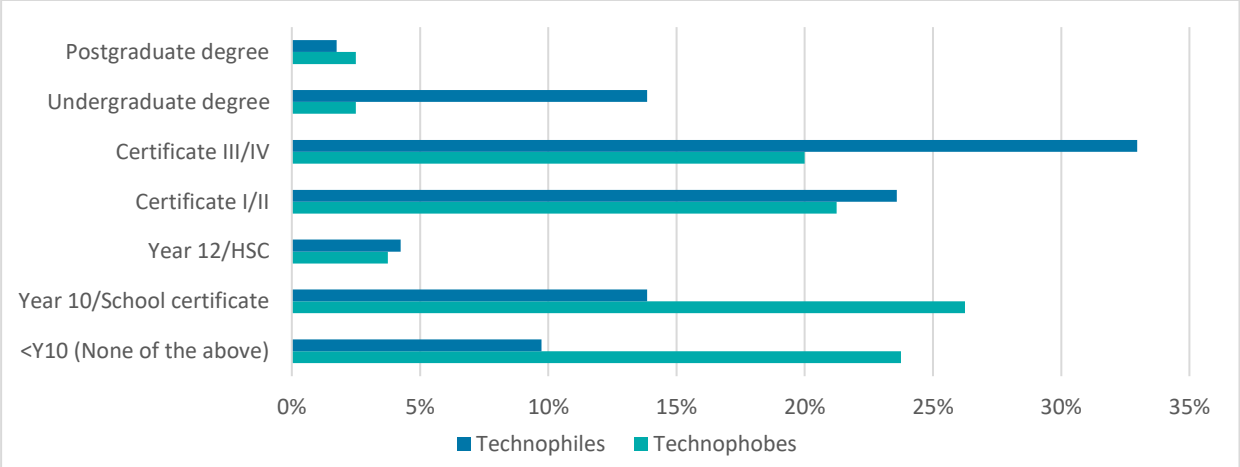
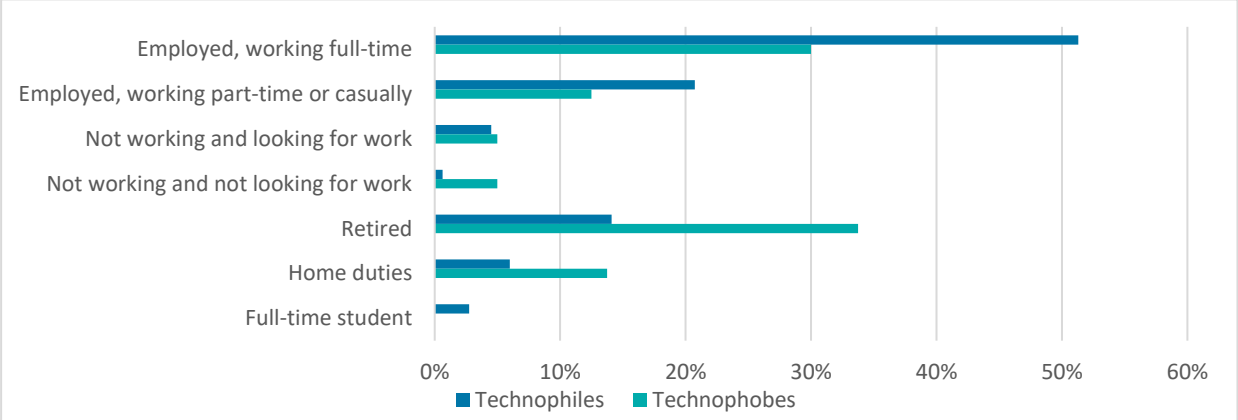
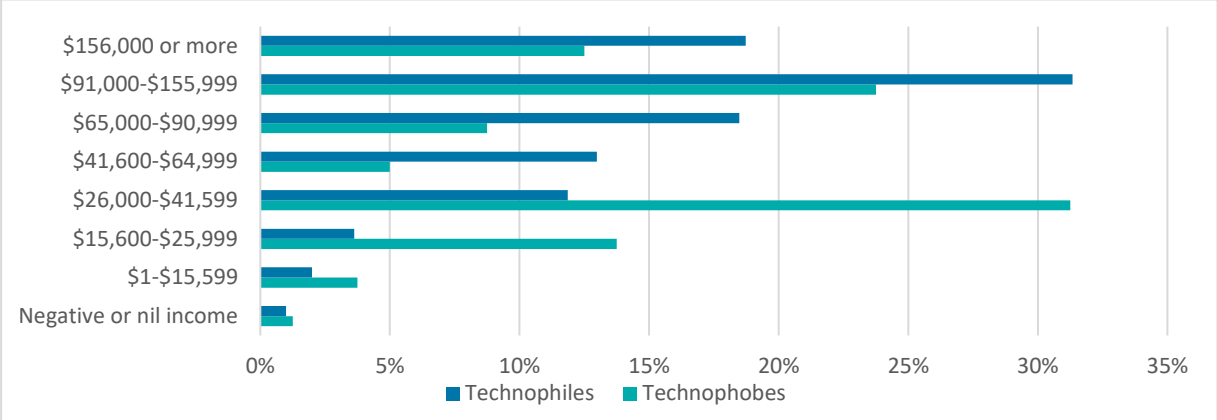


Figure 3 Attitude to keeping up with technology: Employment



[30] Answers were provided on a sliding Likert scale which varied from 'Keeping up with new technology is extremely unimportant' (1) to 'Keeping up with new technology is extremely important' (7) where 4 is the midpoint ('Neither important nor unimportan'). We classified responses of (1) and (2) as Technophobes, (3)(4) and (5) as Neutral, and (6) and (7) as Technophiles.

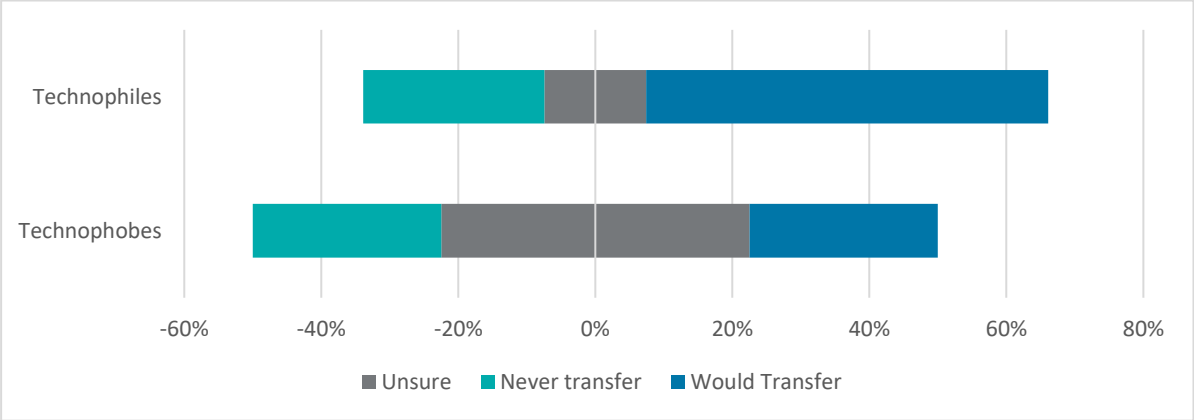
Figure 4 Attitude to keeping up with technology: Household income



In considering the future of the consumer data right, a future in which data literacy is going to be increasingly important, those with lower education levels, retirees and those from lower income households are less likely to have the data literacy to be able to participate in data sharing. These are also the characteristics of those who lack the financial literacy, capability and consciousness to be able to understand their financial position and have the willingness to act to change it.

Data literacy directly impacts people's willingness to share information. Technophiles were more than twice as likely to be willing to share information in exchange for benefits provided by an organisation compared with Technophobes.

Figure 5 Attitude to keeping up with technology: Willingness to share information



People's attitudes to keeping up with technology were also correlated with whether they had changed their banking service provider. People who switched providers were 27% more likely to be a technophile and see keeping up with technology as extremely or very important.

As with financial literacy, capability and consciousness, in preparing for the future of the CDR, one in which the CDR is applied to multiple sectors of the economy, it will be important for both government and industry to build data literacy, capability and consciousness in Australia.

Recommendation 4

The government should work with industry to further improve data literacy and data consciousness to both support the realisation of benefits from data sharing and reduce the risks associated with poor data practices and fraud.

International context

The Inquiry invites submissions on how the Consumer Data Right can be leveraged with international developments ... to enhance opportunities for Australian consumers, Australian businesses and the Australian economy.

Open Banking approaches globally

In Deloitte's submission on the CDR legislation we had noted that as a design principle, Australia should seek to align Australia's regulations with international standards unless there is a strong rationale to do otherwise.[31]

However, while open banking is a commonly used term, there are almost as many unique versions of open banking as there are countries which have deployed it. While Europe might reasonably claim to be the 'cradle of Open Banking' – with PSD2 and the UK's Open Banking Standard – as open banking initiatives have been adopted in other countries they have not just replicated the approach adopted in Europe.

Jurisdictions are adopting their own approaches to open banking, reflecting their markets and policy objectives. The variations cross several dimensions, including implementation timelines, the range of products and services, and the type of institutions and third parties in scope.

However, they all fall broadly into one of two categories: regulatory-driven and market-driven.[32]

Open Data globally

Country / Region	Data Sharing (Read access)	Payment & account initiation (Write access)	Comments
			Regulatory Driven
European Union	Y	Y	The EU's General Data Protection Regulation (GDPR) introduced a broad range of consumer data rights and applies to a broad range of industries. The EU's second Payment System Directive (PSD2) applies only to payments processing data and requires banks, at the direction of a consumer, to share banking data and allow payment initiation. PSD2 allows third party providers (TPPs) to access all bank APIs through registering as an account information service provider (AISP) or a payment initiation service provider (PISP).
United Kingdom	Y	Y	**Open API standards** Requires nine identified banks to share banking data and allow payment initiation through open API standards. Third party providers are regulated by the Financial Conduct Authority (FCA). It also requires banks to provide product information and publicly available information on branches and ATM locations. The Open Data Institute's review of open banking in the UK in July 2019 recommended that the current UK approach be expanded to include all banks, be extended to other financial services sectors and be used as a model to extend data sharing to other sectors of the economy.[33]
Hong Kong	Phase 3 Yet to be implemented	Phase 4 Yet to be implemented	**Open API framework** The Hong Kong Monetary Authority issued an Open API Framework in July 2018, setting out a four-phase approach for banks to implement Open APIs, starting with information sharing on products and services (Phases 1 and 2), then sharing of transactional information (Phase 3) and ending with payment initiation services (Phase 4). Contrary to the EU approach however, while banks will be required to develop APIs, they will be able to restrict access to those TPPs with which they choose to collaborate.

[31] Deloitte, *Shaping the future, Consumer Data Right, Deloitte Submission on the Draft Consumer Data Right Bill*, 7 September 2018. See also: https://treasury.gov.au/consultation/c2018-t316972

[32] Deloitte, Open Banking around the World, 2018. See also: https://www2.deloitte.com/global/en/pages/financial-services/articles/open-banking-around-the-world.html

[33] Open Data Institute, *Open Banking, Preparing for lift off*, July 2019, pp33-34. See also: https://www.openbanking.org.uk/wp-content/uploads/open-banking-report-150719.pdf

Country / Region	Data Sharing (Read access)	Payment & account initiation (Write access)	Comments
			Market Driven
China	Y	Y	**Open API and Digital Platforms** China has opted for a market-led approach with platform and Open API based business models widely used.
India	Second stage Yet to be implemented	Y	**Unique Digital ID** Open banking is being implemented in two separate stages. The first stage is implemented through the Unified Payments Interface (UPI) developed by the National Payments Corporation of India (NPCI). This interface is built on a national identity platform (Aadhaar) and facilitates inter-bank transactions over a robust API framework. The second stage is customer data sharing and is yet to be implemented. It is intended that an RBI licensed entity intermediary will retrieve or collect the financial information of an individual from a data holder (financial information providers or FIPs) and consolidate, organise and present this information to a data recipient (financial information user or FIUs).
Japan	Y	Y	**Open API** Japan has opted for a primarily market-led approach, but one in which the Japanese regulator (the FSA) has encouraged banks in Japan to release APIs for deployment by 2020. The FSA has established legislation for 'Electronic Payment Intermediate Service Providers', an authorisation process for third party service providers. These services include sharing customer data to allow reporting and aggregation of information undertaken by AISPs, and PISPs. There are also no specific API standards. The FSA has introduced an obligation for banks to publish their Open APIs policies by June 2020 and encouraged banks to contract with at least one TPP. However, TPPs are required to register and establish contracts with each bank with which they wish to interact. In addition, and unlike other jurisdictions, Japanese banks are allowed to charge fees to TPPs for access to customer data which appears to be hindering the introduction of open banking.
New Zealand	Y	Y	**Open API** New Zealand's market-led approach is overseen by Payments NZ. Third parties need to register as an API Standards User with the Payments NZ API Centre and then enter into an open banking standard API agreement with each bank. This then allows the third party, with customer consent, to receive customer data and initiate payments.
Singapore	Y	N	**Open API** The Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore (ABS) have published an API Playbook to support data exchange and communication between banks and FinTechs, encouraging financial institutions to develop and share their APIs openly. There is no regulatory framework for open banking, and no standardisation of APIs which has resulted in low levels of utilisation.
United States	Y	Y	**Premium APIs** The US have opted for a market-led approach, without any material government initiatives to support the development of open banking products and services. Data sharing principles encourage banks to introduce APIs for data sharing. The major US banks are developing API-based offerings in contractual partnerships with third parties, as a way to attract new customers and maintain/ gain competitive advantage. However, in the absence of an industry-wide API strategy, screen scraping remains prevalent as a way for TPPs to provide innovative services to customers without having to enter into a contractual agreement with each bank. An API standardisation program was launched to focus on fraud reduction, data sharing and payment access. A US Treasury report[34] recommended developing regulatory approaches to enable secure data sharing in financial services. However due to the highly fragmented and state-based nature of banking and banking regulation in the US, as well as a cultural aversion to 'red tape', there is little discernible appetite currently for taking this forward and issuing a common federal policy on Open Banking.

Source: adapted from Deloitte (2018), Open Banking around the World

[34] United States Department of the Treasury, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation*, July 2018. See also https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf

Comparing Australia's approach

Australia's Consumer Data Right stands out globally for its innovative approach and scale of ambition. It is, arguably, currently unique in its design as an economy wide data sharing policy initiative.

Open banking in the EU and UK may have started, principally, as way to promote competition in the payments and banking industry. But it is clear now that its impact is much broader. Open banking promises to create a new data sharing infrastructure, which will form the basis of a much richer range of services and products across the whole of financial services, and critically, in other industries as well.

It is notable that the review of implementation of the UK's limited open banking initiative by the Open Data Institute recommended that the UK expand open banking to apply to a broader range of banking products, extend it to other financial products and services, and build on it to create a digital economy by extending it to other non-financial sectors of the economy.[35] The Issues Paper for this Inquiry highlights that the UK has announced that its 'Smart Data' model will be extended to the energy and pension markets and has set out a strategy for further extension.

If these recommendations are adopted the UK data sharing model would be similar to Australia's, particularly if Australia adopts write access.

Implications for Australia

Data Protection regulation

The starting point for greater harmonisation of cross-border data sharing frameworks is greater harmonisation of legislation on data rights including data sharing.

There are international regulations on data protection which can be used to guide the data protection regulation which would support the future of the CDR, most noticeably the EU's GDPR framework.

As noted in our comments on the future role and outcomes of the CDR and its interoperability globally, it will be important to ensure that Australia's CDR regime extends to give consumers data rights over their data when it is originally collected, not just when it is shared.

If CDR creates data protection rights together with a new data sharing infrastructure, this creates the conditions for, and forms the basis of, a much richer range of services and products across the economy.

Against this background data regulation will have a transformative impact on the shape and structure of industries. Above all else firms will need to recognise that from now on putting customers fully in control of their 'data lives' will be both a commercial and regulatory imperative.[36]

For entities operating in jurisdictions with a regulatory led approach with similar data rights and data sharing rights, specifically the EU and the UK, the consistency of these regulatory frameworks with Australia's CDR framework could be leveraged to allow faster regulatory approvals for them to operate in Australia.

This is more challenging for entities operating in jurisdictions which have adopted a market driven approach.

Regulatory regime

Globally, if it is clear that open banking and data sharing have the potential to blur the lines between financial services and other industries, what is less clear is whether collaboration between financial services regulators and data protection authorities is sufficient to respond to these challenges.[37] This challenge is likely to arise in other industries to which the CDR is extended.

[35] Open Data Institute (July 2019)
[36] Deloitte (2018), Open Banking around the World
[37] Deloitte (2018), Open Banking around the World

Australia's dual regulator approach for the CDR with responsibilities shared between the ACCC and the OAIC mitigates this risk. However, some submissions on the draft CDR legislation highlighted gaps in some of the regulators' capabilities.[38] It will be important that these regulators are appropriately funded so that they can build the relevant capabilities to enable them to execute their regulatory functions particularly as CDR is expanded to other sectors.

The growth of digitally delivered services also introduces new issues around consumer protection, privacy and confidentiality, financial crime, taxation and regulatory enforcement.

In addition, by changing the ways customers interact with organisations, the boundaries between industries blur, and ultimately, could break down.

While some aspects of Australia's regulatory regime are sector agnostic (such as competition regulation) other elements are sector focused (e.g. AEMC and AEMO in energy, APRA in banking). Many sectors which will be designated in the future are likely to be subject to existing regulation, industry codes and standards.

It will be important for other regulators – e.g. APRA, ASIC and AUSTRAC as well as possibly the Australian Energy Regulator, the Australian Communications and Media Authority and other sector specific bodies whose remit includes consumer protection, data and/or privacy – to be anticipating the consequences of adoption of the CDR across the financial services sectors and the implications for regulation of other sectors when the CDR is adopted across the economy.

Recommendation 5

The government should review how data sharing impacts other regulatory requirements and consider how CDR obligations interact with other legislative requirements, industry codes and standards in other sectors to which the CDR is expanded.

Passporting

The significant variations in open banking instances globally potentially make it more difficult to allow cross-border data sharing and passporting of new entrants into open banking in Australia and data sharing arrangements in other sectors.

However, imposing additional regulatory requirements on potential new entrants could reduce the potential for innovation and increased competition.

The UK-Australia FinTech Bridge in part recognises the similarity of the regulatory approach adopted in each country.[39] Under the Enhanced Agreement, the Regulator-to-Regulator Implementing Authorities have committed to facilitating the entry of FinTech start-ups from the other jurisdiction into their respective regulatory sandboxes (Section 3.2).

However the FinTech Bridge agreement is primarily focused on collaboration and information sharing including government-to-government (section 2), regulator-to-regulator (section 3) and business-to-business (section 5), awareness raising (section 4) and market entry support (sections 4.3 to 4.12).

By contrast, for example, the Asia Region Funds Passport is a multilaterally agreed framework to facilitate the cross-border marketing of managed funds across participating economies in the Asia region. It provides a framework which is more specifically focused on achieving defined outcomes allowing greater competition.

[38] For example, Financial Rights Legal Centre, *Submission by the Financial Rights Legal Centre and Financial Counselling Australia: Treasury Laws Amendment (Consumer Data Right) Bill 2018*, September 2018, page 38

[39] Australian Government, The Treasury, UK-Australia FinTech Bridge, https://treasury.gov.au/fintech/uk-australia-fintech-bridge

As part of the future of the consumer data Australia should consider which countries have sufficiently robust data sharing regimes, with effective and enforceable regulation, to support cross-border data sharing by entities in specific sectors.

Recommendation 6

The government should seek opportunities for mutual recognition of data sharing frameworks in other jurisdictions which have similar rights, obligations and legal protections.

Summary

There seems little doubt that markets believe that data sharing, starting with open banking and followed by the development of a broader cross-industry data sharing ecosystem, is the way forward.

To respond effectively regulators will need to break down their own sectoral and geographic siloes and put the protection and fair use of customer data at the top of their agenda. [40]

As Australia moves towards an economy wide consumer data right, it will be important that the regulatory environment is reviewed so that it continues to be appropriate and anticipates the delivery of services by global organisations.

So far Australia is leading the way with its vision and legislative framework for an economy wide CDR. While each country will choose a data sharing framework which reflects their markets and policy objectives, Australia has an opportunity to shape the development of global best practice in data sharing by fast-tracking the entry of new entrants from countries with similar or equivalent data sharing frameworks, data protections, and consumer protections.

[40] Deloitte (2018), Open Banking around the World

Switching

The Inquiry invites submissions on how the Consumer Data Right could be used to overcome behavioural and regulatory barriers to safe, convenient and efficient switching between products and providers, whether those barriers are sector-specific or common across industries.

Trust

The ACCC have noted that the future of the digital economy relies on trust, by both consumers and business users. [41]

Organisations seeking to encourage customers to participate in open banking and share their data need to be able to answer two questions:

1. Will consumers trust my ability to keep information about them and their transactions secure, and ensure their privacy?
2. Are the benefits that I offer consumers sufficiently valuable to them to encourage them to share their information?

Deloitte's report on open banking and consumer behaviour explored the role trust plays when consumers look at alternative providers for their banking services, and how trust influences people's willingness to share information.[42]

One clear finding was that trust is the starting point when looking at customer behaviour. Trust influences who we bank with. It influences our willingness to share information. And it is one of the reasons people change banks.

Following the Hayne Royal Commission much has been written about trust in banks and financial service providers. Although trust is a broad and complex concept there are three dimensions to trust that stand out:

1. **Prudential trust** - do I trust an entity to keep my money safe?
2. **Information trust** - do I trust an entity to keep information about me and my transactions secure?
3. **Relationship trust** - do I trust that an entity has my best interests at heart?

The results from our survey highlighted that the majority of Australians are satisfied with their current banking products and providers, or at least not dissatisfied enough to gather information about other banking products or offerings (let alone to make a decision to change banks).[43]

Our survey also highlighted that people bank with the type of organisation that they trust the most. For each type of bank - irrespective of whether you bank with a major bank, a regional bank, a mutual bank, a digital bank or a foreign bank - customers bank with the type of bank in which they have the highest level of trust.

This suggests that what each of these types of organisations offer, appeals to a particular type of customer. So levels of switching, can, in part, reflect people's level of trust in their current provider and their general satisfaction with the banking services they receive.

Deloitte's consumer privacy insights have consistently highlighted the importance that Australian consumers place on transparency, and the significant improvements that many organisations require in order to embed a culture of trust. Our 2019 submission to the ACCC's review into Customer Loyalty

---

[41] ACCC (July 2019)

[42] Deloitte, Open Banking: Switch or Stick (October 2019)

[43] Most consumers (81%) say they are very or fairly satisfied with their bank. In a separate survey we found that around four in five (79%) of transaction account holders are either 'satisfied' or 'very satisfied' with their existing provider. Similarly, three quarters of credit card holders and two thirds of mortgage owners reported being 'satisfied'. Conversely, only 5% to 9% of account holders said that they were dissatisfied with their account. Deloitte Access Economics for the Australian Banking Association, *Choice in banking*, 2019.

Schemes highlighted that trust has become the primary driver of consumer decision making and brand loyalty in Australia.[44]

Notably, 65% of consumers surveyed as part of the 2019 Deloitte Privacy Index rated trust as their first consideration when deciding whether to provide an organisation with access to their personal information. The 2017 Privacy Index found that only 32% of consumers felt that organisations had built meaningful trust with them, and that 91% of organisations believed that they could increase their transparency in relation to the use of consumer data.[45]

Consumers in Australia have also shown that they are more likely to interact positively with organisations that they trust, a factor that will be key to the future success of the CDR. The 2018 Privacy Index found that 69% of consumers chose 'trust that a brand will use data appropriately' as their primary consideration in deciding whether to share their personal information.[46]

Deloitte's open banking survey highlighted that lack of the third component of trust, relationship trust — concerns about ethics and mindset — was one of the top five reasons people changed banks.

Behavioural Biases and Barriers

Deloitte's open banking survey also highlighted that people's behavioural biases influence whether and how people search for information and make a decision to change provider. Research by Deloitte[47] together with a study on product innovation[48] identified six key behavioural biases that impact people's willingness to change providers:

Analysis paralysis: **"**There are too many options, I just can't decide."
Consumers freeze when too many choices are presented. Decision paralysis brought on by the inability to choose between options is typically the result of cognitive overload and fatigue. This state of choice overload tends to reduce consumers' confidence in a decision they have made and can prevent making one at all.

Facing an uncertain future: "I know I should…but that can wait."
Consumers strongly prefer present payoffs to future rewards. While the potential savings from a lower mortgage rate can be significant over 25 years, they may not create enough of a sense of urgency in people to offset the more immediate transaction costs of gathering information and switching now.

Cognitive research has shown that people often learn and make decisions using 'case-based reasoning'—solving problems by recalling previous situations and reusing that information.[49] With no personal experience, feedback, or a memory of past reference points, consumers feel ill-equipped to make the right call; even after gathering additional information to supplement their view, they are often left with the sneaking suspicion that important 'unknown unknowns' remain.[50] The behavioural tendency to explicitly or implicitly lean on anchors—trusted reference points—provides our brains with a place to start understanding what good looks like. Without these anchors, and with only tenuous confidence in their own ability to choose wisely, consumers stall and do nothing—sometimes indefinitely—rather than commit to the wrong option.

---

[44] Deloitte, *Submission on the ACCC Customer Loyalty Scheme Draft Report*, 3 October 2019. See also https://www.accc.gov.au/system/files/Deloitte%20-%20October%202019.pdf
[45] Deloitte, *Deloitte Australian Privacy Index 2017: 'Trust starts from within'*, 2017, page 6. See also: https://www2.deloitte.com/tl/en/pages/risk/articles/deloitte-australian-privacy-index-2017.html
[46] Deloitte, *Deloitte Australian Privacy Index 2018 'The Symbiotic Relationship'*, 2018 page 4. See also: https://www2.deloitte.com/au/en/pages/risk/articles/deloitte-australian-privacy-index.html
[47] Deloitte University Press, *Frozen: Using behavioural design to overcome decision-making paralysis*, 2016. See also: https://www2.deloitte.com/us/en/insights/focus/behavioral-economics/overcoming-decision-making-paralysis.html
[48] Gourville, John T., *Eager Sellers Stony Buyers: Understanding the Psychology of New-Product Adoption*, Harvard Business Review, June 2006 pp98-106. Refer https://hbr.org/2006/06/eager-sellers-and-stony-buyers-understanding-the-psychology-of-new-product-adoption
[49] Agnar Aamodt and Enric Plaza, "*Case-based reasoning: Foundational issues, methodological variations, and system approaches. AI communications*", IOS Press7, no. 1 (1994), pp. 39–59 in Deloitte University Press (2016)
[50] Doblin research, https://www.doblin.com/ in Deloitte University Press (2016)

The impact of emotion on behaviour: "I worry about failure, and I hate feeling dumb."
Consumers are often overcome by fear of failure when presented with an important choice. They hate the idea of being forced to live with a sub-par option, but, just as importantly, they worry about looking silly or stupid for having chosen poorly. [51]

Loss aversion effect: "I'm worried about what I'll lose… and not certain of the value of what I'll gain."
Consumers focus on what they'll lose by changing provider. The put three times as much weight on what they'll lose, compared to what they may gain.

Endowment effect: "I value what I have more than something new."
Consumers value things they've previously made a decision to acquire.

Status quo bias: "I prefer to stick with what I have … even if there's a better alternative."
Consumers value stability, preferring to stick with what they already have.

The effect of these behavioural biases were evident in the switching results in Deloitte's open banking survey.

Behavioural biases mean that people tend to stick to what they have, even if a better alternative exists (status quo bias), and tend to value products they already possess more than those they don't have (endowment effect). These behavioural biases, together with our desire to believe we have made good choices (confirmation bias), may contribute to people's assessment of how satisfied they are with their current provider and how much they trust the organisation they bank with currently.

Because customers perceive that they are satisfied with their current banking product or provider, they do not gather information about other banking products or offerings. And because they have not gathered information, they are not aware of the benefits of these alternative financial services products from other providers, and so lack the information to re-assess their level of satisfaction with their current provider.

Although the CDR is likely to reduce some of the transaction costs associated with gathering information on alternative providers and changing provider, equally important will be reducing the psychological costs associated with behaviour change.

Behavioural biases will be amplified for consumers with low levels of financial and data literacy which can mean that they don't have the confidence or capability to share data, and lack the capability to understand the impact of information they gather about alternatives or the level of financial consciousness to make a decision to change provider.

Impact on the future of the CDR

It is notable that many of the behavioural biases can be addressed, at least in part, through improved financial and data literacy and consciousness. The CDR enables third parties – both product and service providers and, if extended, intermediaries – to help with the decision-making process by making sense of the range of options, or with making the potential benefits more tangible. In an environment where the CDR and data sharing are economy wide, it will be important that consumers seeking advice from intermediaries can be confident that the intermediary has a duty to have the consumer's best interest at heart – that the conditions for relationship trust exist. This would require a strengthened regulatory framework for intermediaries which includes a best interest duty.

The CDR makes product information available via APIs. Comparator websites potentially have an important role to play in using this product information to help consumers understand the options available to them. The potential value comparator websites can play increases as more sectors of the Australian economy are subject to data sharing under the CDR, and increases further, if the inclusion of write access allows comparator websites to seamlessly change providers on behalf of customers. However, while the ACCC's report in 2014 on the comparator website industry highlighted the benefits that PCWs provide it also highlighted a number of concerns about conduct in the industry. Write access

[51] Deloitte University Press (2016)

will amplify these concerns and the potential harm to consumers (see comments on Comparator websites and 'best interests' duty).

To successfully get customers to switch, organisations need to overcome customers' inertia. This is only exacerbated for more complex products, where customers possibly feel anxious about selecting the best product or service for them, overwhelmed by different product terms and conditions, and without an easy way to compare and assess options. The CDR helps overcome this intention-action gap by reducing effort and cognitive load on consumers by:

a. enabling aggregator and comparison websites to help consumers find and compare offers.
b. enabling contextualisation of offers through parsing other parametric data to enable personalised "what-if" analysis (e.g. electricity usage and typical usage times for an energy provider).
c. reducing friction involved in changing providers through enabling customers to automatically act on the insights generated by being able to enter and exit contractual arrangements. E.g. cancelling a service, signing-up to a new offer or triggering other desired actions such as obtaining a better rate. This is a critical aspect enabled by write access.

Deloitte's open banking survey also highlighted a significant difference in the level of prudential trust and information trust by consumers in foreign banks and digital banks compared to major, regional and mutual banks despite the common regulatory framework which applies to all ADIs. Consideration should be given to enhancing consumer trust in the prudential and regulatory frameworks applying to all classes of ADIs.

Recommendation 7

As the CDR is extended to other sectors policy frameworks that are currently primarily industry or sector based, should be reviewed to facilitate the potential introduction of competitors from other industries or sectors.

Recommendation 8

Given that the CDR has the potential to amplify the role of PCWs, particularly if CDR is extended to include write access, the concerns raised in the ACCC's report on the industry should be reviewed and resolved.

Read Access

The Inquiry will look at the scope of current 'read' access functionality and consider options to expand it. It has requested submissions in relation to:

- ***Consent - the potential to develop a 'consent taxonomy' using standardised language for consents across providers and sectors.***
- ***Consent fatigue – how best to enable consumers to keep track of, and manage, their various consents.***
- ***Voluntary data sets – the promotion of industry cooperation on standards for 'voluntary' data sets.***
- ***Tiered accreditation - the scope for use of tiered accreditation to promote broader access without increasing risk.***

Consent

A standardised consent taxonomy has the potential to reduce complexity and streamline consent requirements for participants and consumers under an expanded CDR regime, but must be balanced against the need to protect consumers, particularly in relation to their most sensitive information.

To protect privacy, the development of a standardised consent taxonomy should embed existing CDR protections requiring express consent that is voluntary, informed, specific, time limited and easily withdrawn. A standardised consent taxonomy that embeds consistent, simple to understand language across all industries is likely to benefit consumers, particularly those with lower data literacy, and enable them to better understand the different ways in which their CDR data will be used.

Standardised consent may also reduce the likelihood of consent fatigue as the regime is expanded to include a greater number of industries and services (see comments on Consent Fatigue).

To maintain effective privacy protections for consumers, the standardised consent taxonomy should be regularly reviewed as the CDR is extended to other sectors to ensure that all industries and associated data sets are accounted for in the language and form of standard consent.

Specifically, as new sectors are designated under the CDR, consideration should be given to the specific data sets that will be shared in the delivery of services in that industry, particularly where information would attract greater protection under the Privacy Act. This may include CDR participants which offer products and services requiring the collection of sensitive personal information, for example, health information.

A standardised consent taxonomy should also be reviewed if new functions are added to the CDR regime that carry an inherently greater risk to consumers, for example write access or the provision of payment scheme arrangements (see comments on Write Access).

CDR data recipients are required to segregate data sets between CDR data, which is afforded greater protection by the CDR Rules Framework, and other personal information collected outside of the CDR regime that is protected in accordance with Privacy Act 1988 requirements.

The value of a standard consent taxonomy is strengthened when applied at the point of collection, in addition to when data sets are shared. Having different consent requirements for collecting data and for sharing data increases complexity and makes it more difficult to ensure a consistent level of data protection. This would be largely mitigated if consistent internal organisational policies and controls for consent were applied throughout the data life cycle.

In the absence of consistent consent frameworks for both the collection and sharing of data, effective data segregation is an essential measure to protect both CDR data and other personal information from use or disclosure beyond the purpose for which it was collected, and in keeping with the notice provided to consumers.

In addition, CDR participants must also account for the use, disclosure and retention of some CDR data as a result of other legislative requirements, such as lending assessments, Know Your Customer (KYC) or Anti-Money Laundering (AML). This makes it important that CDR participants have clarity and traceability of their CDR data, including the associated consents and lawful purposes that justify subsequent use, disclosure or retention of data.

Recommendation 9

The CDR framework should address the requirements for, and application of, a consistent consent model to support internal organisational governance, management and protection of CDR datasets. This may include embedding specific requirements within accreditation criteria.

Consent Fatigue

As the CDR is rolled out across the economy and expands to new sectors, consumers will need to navigate multiple data consent relationships in multi-lateral data sharing arrangements resulting from the interaction of multiple data holders and multiple data recipients (and potentially intermediaries).

Consumers potentially face an exponential increase in the number of messages and notifications they will receive as they consent to sharing their data, and an increasingly complex consent dashboard.[52] This is likely to lead to consent fatigue and message fatigue, which risk reinforcing a number of behavioural biases, including for example analysis paralysis and status quo bias. This could adversely impact the likelihood that consumers make an informed decision, or that they make a decision at all.

As noted, a standardised consent taxonomy has the potential to reduce consent fatigue, especially amongst consumers that have a lower level of data literacy.

An important criterion for assessing consent dashboards is whether they help consumers to provide informed consent.

It will be important that the current design for consumer dashboards is reviewed and adapted as CDR expands. This will be particularly important if the CDR is extended to include write access, or if the CDR dashboard also includes consents consumers provide under payment scheme arrangements.

Some submissions on the CDR Rules framework proposed that consideration could be given to sector specific consent dashboards to reduce the cognitive load on consumers. Other submissions noted that sector specific consent dashboards could create a consent framework which is more confusing and more difficult to manage, particularly for consumers who are less data literate. Sector specific consent frameworks would also be less effective for propositions seeking to integrate data across industry sectors.

While sector specific consent dashboards may provide an interim solution to reducing complexity as consumers become more familiar with the CDR, centralised dashboards are more likely to provide a simpler and consistent consumer consent experience.

Future reforms, including standardised visual consent aids may be necessary to simplify the delivery of notice and reduce the likelihood that consumers will be unable to provide informed consent.

Recommendation 10

The consent dashboard framework should be tested with consumers, particularly as the CDR expands and the number of consents that a consumer could provide increases, to determine the most effective way of enabling them to provide informed consent.

Further developments to consumer dashboards may be required, for example to provide a consolidated industry view of consents, per consumer.

[52] The challenge of message fatigue was also noted in the work done on the Consumer Data Standards. Refer Greater Tobias (2019), page 22.

Voluntary Data Sets

Any organisation currently has the opportunity to voluntarily provide additional data sets to customers. This could result in an industry cooperating so that a broad range of competitors elect to voluntarily provide additional data sets to customers.

While this has the potential to enhance consumer benefits by increasing the amount of information that is available, there are also some additional risks.

- If 'voluntary' data sets are provided by data holders for a fee, there would need to be a clear and understandable communication to customers that the 'voluntary' data sets provided for a fee were not CDR data.
- Consideration should be given to applying the CDR consent and data protection standards to 'voluntary' data sets received by an accredited data recipient so that 'voluntary' data sets received were not used for purposes which would otherwise be proscribed by the CDR regulations.
- The promotion of voluntary data sets should be supported by measures to protect individuals from the inherent privacy risks associated with the practice of sharing identifiable, de-identified or derived data sets for the purpose of creating industry-wide insights.

Specifically in relation to aggregated data, the potential for re-identification as a result of technically ineffective de-identification practices, or matching of new and existing data sets creates a significant privacy risk to individuals.

For example, analytics tools or matching techniques have the potential to link data sets to reveal someone's lifestyle, consumer habits, social networks and more – even if no single data set reveals this personal information.[53] This risk is amplified by technically ineffective de-identification, and circumstances in which data sets are transferred between industries with shared customers.

The Data61 De-Identification Decision Making Framework (DDF), which must be considered by accredited recipients prior to de-identification, provides a strong basis under which CDR participants are required to de-identify CDR data.[54]

Recommendation 11

Given the increased risk of re-identification as additional datasets are added, the framework should continue to be applied and regularly reviewed as more industries are included and the nature of the datasets change.

[53] Deloitte Canada, '*Have it all: Protecting Privacy in the Age of Analytics*', 2014, p3. See also https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/Analytics/ca-en-analytics-ipc-big-data.pdf

[54] Competition and Consumer (CDR) Rules 2020 (Cth), Division 1.4, 1.17 (CDR data de-identification process).

Tiered Accreditation

At present, the CDR Rules provide a single level of accreditation for CDR participants ('unrestricted'). This is a strict standard for participants that provides a high level of security and privacy protection for CDR data and should promote confidence in the CDR framework.

However, while single-tiered accreditation provides valuable protections for consumers, it is both a cost and time intensive exercise. In Deloitte's submission on the CDR Rules Framework we noted that 'a core principle of regulation is that broadly defined benefits should be weighed against broadly defined costs'.[55]

Submissions on the CDR Rules noted that tiered accreditation would potentially enable consumers to share data within the CDR system with organisations providing consumer services such as accountants and financial advisers and counsellors who would otherwise not seek to become an accredited data recipient.[56] Such parties may be included as intermediaries as a result of the ACCC's consultation on allowing third party service providers to collect CDR data.[57]

Further expansion of the CDR to a range of new sectors and participants could include a tiered accreditation approach. This would allow participants to receive CDR data commensurate with their level of maturity. In addition, tiered accreditation has the potential to reduce the barrier for many CDR participants that would otherwise be unable to implement capabilities to meet 'unrestricted' requirements, whilst also allowing for the use of intermediaries in the collection of CDR data on behalf of accredited persons.

A tiered accreditation approach is also consistent with the Review into Open Banking, which recommended the implementation of such a model, under which 'parties would be accredited to receive and hold data, based on the potential harm that the relevant data set and that party pose to customers, and to the Open Banking system.'[58]

Deloitte's submission to the ACCC on the CDR Rules Framework proposed a number of options to support a system of tiered accreditation[59]:

- Tiering based on the ***attributes*** of the CDR data being shared, e.g. basic customer information could be an example of a limited data set available to a lower tier accredited CDR participant. This could be supported by the definition of standard subsets of data attributes to be made available to lower tier participants. A subset of data may exclude higher risk data attributes, resulting in a lower risk profile for the provision of the limited data set.
- Tiering based on the ***sensitivity*** of the CDR data being shared. This would allow for higher accreditation requirements for data recipients receiving data sets that have data that are more sensitive or that include sensitive data attributes such as data from minors or, at a future point, health data.
- Tiering based on ***standardised*** and/or ***approved uses*** of CDR data e.g. lower tier participants may be eligible to receive CDR data for purposes such as proof of income / expenditure or to summarise monthly expenditure by merchant type. The tiered accreditation could be restricted to a set of use cases that might be considered lower risk for consumers, e.g. aggregation of data.

These options remain viable for a future expansion of the CDR.

[55] Deloitte, *Deloitte Submission on the Consumer Data Right Rules Framework*,12 October 2018, p10. See also: https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/accc-consultation-on-rules-framework

[56] For example, Consumer Policy Research Centre, *Submission by Consumer Policy Research Centre to ACCCC – Consumer Data Right Rules Framework*, 12 October 2018

[57] ACCC, *CDR Consultation paper – participation of third party service providers*, 23 December 2019.

[58] Review into Open Banking (2017), page 24-25

[59] Deloitte, *Deloitte Submission on the Consumer Data Right Rules Framework*, 12 October 2018, p9

Write Access

The Inquiry is interested in interested parties' views on these issues (potential uses and benefits of write access across sectors, barriers to enabling write access, compliance costs and risk involved, who should bear responsibility for payments made, and for changes made to data, and whether write access should extend to the ability to change details which identify a customer).

In the context of Open Banking, the Inquiry is particularly interested in interested parties' views on how the Consumer Data Right could best enable payment initiation.

Uses and benefits of write access

While there are various use cases for read access that deliver value for consumers, the ability to have both read access and write access enables providers to offer a broader range of innovative services, while empowering customers to take action rather than just being informed.

The Review into Open Banking noted 'while write access has significant benefits, it may take some time for customers to feel comfortable with third parties acting on their behalf … for these reasons it would be premature to consider implementing it at this stage.'[60] It is not clear that there have been any developments in Australia's payments landscape that would cause this view to change. Specifically, data sharing has not yet commenced in Australia's open banking regime, and the rollout of the New Payments Platform (NPP) has only just commenced.

But it is an important issue for the current review to consider.

In one of the articles in Deloitte's Open Banking series we noted that data sharing (read access) has the potential to provide insights and recommendations to customers but that without write access, 'consumers will not be able to automatically act on the data, or the insights that are generated. Consumers will not be able to instruct a third party to initiate a payment, transfer funds on their behalf to obtain a better rate, or change providers.' [61]

Submissions to the Review into Open Banking claimed that allowing third party write access would be 'the biggest reform to empower customers and improve bank competition'.[62]

One submission to the Review proposed that both read and write access should be implemented at the same time, after sharing data on customer validation to support the 'know-your-customer' requirements.[63]

A number of submissions on the CDR legislation and the Rules framework also noted the significant consumer benefits that are dependent on the inclusion of write access. In particular, write access has the potential to help address behavioural biases and 'act as an antidote to the inertia seen today in the retail banking market.'[64]

This has resulted in growing calls for the introduction of write access in Australia to be accelerated, notwithstanding the reservations noted in the Review into Open Banking.

In New Zealand, an industry pilot to inform API specifications for both read and write access identified significant value in write access. Payments NZ Chief Executive, Steve Wiggins, has noted that:

> *'…development partners found they had stronger use cases for the Payment Initiation standard within the constraints of the minimal viable product (MVP) environment. This led to a re-focusing of the group's efforts toward testing the Payment Initiation API standard.'*[65]

---

[60] Review into Open Banking (2017) page 109

[61] Deloitte, *Open Banking, Payment initiation – completing the vision*, December 2019.

[62] Review into Open Banking (2017), page 108, referring to FinTech Australia submission, page 5 and Cuscal submission page 4

[63] Review into Open Banking (2017), page 98, referring to FinTech Australia submission, page 17-18

[64] Australian Government, The Senate, *Senate Select Committee on Financial Technology and Regulatory Technology, Issues Paper*, October 2019, page 9

[65] Refer https://www.apicentre.paymentsnz.co.nz/about/news/making-payments-innovation-easier/ retrieved 11 September 2019.

There is a range of use cases, some live in the EU and UK now, which deliver value to customers based on propositions that integrate both read and write access: [66]

- A write access enabled intelligent assistant could move funds between accounts to ensure that funds are available in the correct accounts when payments fall due, and when earned interest is optimised.
- Write access could allow a third party to automate the payment of bills and invoices on the due dates and pay them from designated accounts.
- Write access could enhance the ability to provide wealth management services to consumers by allowing a third party to help consumers save and invest funds.
- Write access could make it easier to switch providers by enabling the transfer of accounts, banking authorities and transaction histories from one provider to another.
- Write access improves the feasibility of marketplace models, where a single aggregation platform provides access to multiple different providers for similar products, empowering the customer to more easily compare and choose different providers.
- Other use cases could include intelligent identification of optimal financial products across the market, and automatic migration of funds and transaction history to those products.

Write access is also likely to enhance the consumer benefits resulting from the extension of the CDR to other financial services sectors, such as superannuation and investment management.

While account aggregation is possible with read access, when combined with write access third parties can initiate transactions to move funds across accounts on behalf of a customer.

There are also a range of potential non-payment related functions that the implementation of write access capability could enable. These relate to many functions currently accessible through internet banking portals and service apps. Examples include initiating changes to existing products, changing membership tier levels, or pushing updates on personal details.

In addition, account opening (another functional element of write access along with payment initiation) will be an important element of the extension of CDR to non-financial services sectors.

Conversion to solar energy supported by bank financing is an oft used example of what the CDR could enable. Write access which allowed account opening, together with shared data, could potentially make this a seamless experience for a customer. It could enable a service provider to:

- Model the potential energy and financial savings from implementing a photo-voltaic system
- Apply for and drawdown a loan to acquire the PV system, the terms of which are dependent on the savings generated
- Change energy provider, e.g. to enable a customer to select an energy provider with better time-of-day pricing
- Make a payment to a PV system provider
- Repay the lender by transferring funds from a customer's account based on cost savings resulting from the energy generated by the PV system.

These examples focus on the benefits to consumers. But in fact, the opportunity for small and medium-sized business to benefit, may be even greater. Integrating read and write access can enable better cash flow management, reduce complexity and cost, and free up time for managers to focus on their customers, rather than administering their business. This is an important segment for the Australian economy, and one where technological integration and automation is critical in extending complex transaction banking capabilities to smaller customers. [67]

[66] Deloitte (December 2019), page 3
[67] Deloitte (December 2019), page 4

Write access offers potentially greater benefits to corporate business customers. Write capability enables a range of use cases for business customers, including accounts payable management, treasury and payroll. Integration of corporate systems to banks' technology environments in Australia is currently limited, partly due to the lack of standard APIs across the industry. Open banking provides those standards and could potentially result in a surge in end-to-end digitisation of corporate to bank relationships.

As noted in our comments on Switching, allowing third parties, with a consumer's consent, to open an account on their behalf could address some of the behavioural biases which prevent people taking action to change providers.

Risks

The Inquiry will consider … compliance costs and risk involved. This includes issues such as who should bear responsibility for payments made, and for changes made to data, and whether write access should extend to the ability to change details which identify a customer.

The Review into Open Banking noted that for the CDR regime to be successful in the long-term, 'customers need a high level of confidence that their data is secure and that it is only being used for the purpose that consent is given'.[68]

Notwithstanding the significant potential benefits to consumers, write access – including both payment initiation and account opening – also increases privacy and information security risks both for CDR participants and individual consumers. For example, write access may lead to greater risk of malicious cyber or fraud related activities that are aimed at taking control of a consumer's accounts.

The CDR rules and regulations go to great lengths to mitigate and manage the risks associated with sharing customer data with third parties. This includes specification of customer consent requirements and customer experience standards; accreditation of data recipients; requirements on technical security standards; and clear governance around customer privacy. All of these are backed by penalties for breaches that are meaningful, even for large institutions.

Given that the commencement of CDR has been delayed, and the rollout of NPP is closer, consideration should be given to ensuring that rules for write access, including both payment initiation and account opening, are developed and aligned with the functionality being rolled-out through the NPP and existing payment initiation mechanisms.

As the CDR is extended to include payment initiation and account opening it will be important that the regulatory, enforcement and penalty arrangements are aligned to provide a consistent integrated framework for operation and compliance.

Existing payment initiation mechanisms are comprehensively governed by responsible entities such as card schemes (Visa, Mastercard, Amex, eftpos) and NPP Australia. These bodies set governance standards in the form of scheme rules and a mandatory compliance framework. As CDR is extended to include payment initiation, these existing payment regulatory frameworks should be utilised where appropriate.

However, as with all new capability, there are potential vulnerabilities that may be exploited. These need to be identified and remediated quickly to ensure trust in the new capabilities is built and maintained. A recent example is the exposure of PayID customer data through inappropriate use of the address 'look-up' function. These were quickly addressed at both a technical and governance level.[69]

Privacy and information security standards: While banks have typically had strong privacy and information security standards as part of their ADI accreditation, as CDR is extended to other sectors many organisations will need to significantly improve privacy and information security maturity. Many CDR participants seeking to utilise write access will require significant investment to achieve the accreditation necessary to do so.

[68] Review into Open Banking (2017), p108

[69] New Payments Platform Australia, *Uplifting cybersecurity controls*, Press Release, 20 August 2019 (retrieved 11 September 2019)

Payee lists: Concerns were raised in submissions on the CDR Rules framework that the sharing of payee lists under the CDR could negatively impact the payee's privacy as they would require sharing the payee's name, account name, BSB and account number.[70]

We do not believe that this represents a significant privacy risk if managed appropriately. Customers are already able to use and share this information. CDR has the potential to enable this to be done more easily as part of both read and write access. Write access will be more valuable to consumers where, with a consumer's consent, an accredited data recipient is able to utilise payee lists or direct debit lists to initiate payments or to facilitate switching. If shared within the framework for data protection provided more broadly for read access under CDR, this should not present incremental privacy concerns.

It is noted that as part of the NPP, both the PayID capability and the planned Mandated Payment Service create functionality that provides for simple addressing and a standardised way for managing payee lists and payments mandates (i.e. customer consent for "pull" payments). We encourage the CDR reform to leverage these capabilities, in part because doing so should mitigate privacy or security concerns.

Screen scraping: Write access can currently potentially occur where consumers share their user IDs and passwords with third parties, enabling them to initiate transactions. Screen-scraping raises significant privacy and security risks associated with the transferring of passwords, collection and processing of significant amounts of financially sensitive customer data. The development of an established write access mechanism has the potential to significantly reduce these higher risk activities, especially those undertaken by non-accredited organisations as an alternative to data sharing through the CDR.

Financial and data literacy: The introduction of third-party payment initiation capability will also amplify the challenges for consumers with limited financial and data literacy. People may confuse making an enquiry with making a payment; or may confuse authorising a recurring payment with making a one-off payment. It will be important that the consent frameworks for payment initiation are thoroughly tested, particularly for vulnerable customers. However, it is also important that, in the absence of fraud or inappropriate conduct, that consumers are accountable for the decisions they make, including decisions on payment initiation.

Tiered accreditation: Tiered accreditation would enable organisations to participate in CDR as an accredited data recipient with increasingly higher standards required for payment initiation and account opening based on the size and nature of the transactions.

Best Interests duty: The risks of inappropriate payment initiation are reduced or at least mitigated if there is a 'best interest' duty for sites which promote account opening, account switching and payment initiation (see comments on Comparator websites and 'best interests' duty).

Education: Consumer education will be very important if customers are to avoid being impacted by financial crime. Regulators, financial services providers, technology providers, industry bodies and consumer groups will all need to closely monitor developments and inform the broader public of risks and preventative strategies.[71]

Ability to change details which identify a customer: The Know Your Customer (KYC) requirements are a key element of managing financial crime in Australia. An organisation's ability to meet their KYC obligations is potentially compromised where a third-party is able to change customer details. It would be important to understand the use cases and proposed customer benefits associated with including this functionality as part of extending the CDR to include write access.

If there are significant benefits associated with allowing details which identify a customer to be changed by a third party, the risk of fraudulent activity as a result of changing details which identify a customer could be mitigated by: phasing in this element of write access restricting this element to organisations with higher tiered accreditation; increasing insurance requirements for organisations providing this function; and increasing penalties associated with breaches.

[70] For example, Australian Banking Association, *Consumer Data Right Rules Framework: ABA response to ACCC Position Paper*, 12 October 2018, page 6; Choice, *Consumer Data Right Rules Framework, Submission to the ACCC*, 12 October 2018, page 2; Westpac Banking Corporation, *Westpac Group Submission – Consumer Data Right Rules Framework*, 12 October 2018, page 15.

[71] Deloitte, *Open Banking: What does it mean for financial crime?*, June 2018.

Write access and the New Payments Platform

Payment initiation could be expediently delivered by enhancing capabilities already being developed for the NPP, specifically payments initiation messages and the Mandated Payment Service. This would ensure that CDR write access was tied to the future-oriented real-time payment platform and would enable participants to deliver a smooth customer experience. The key focus of the establishment of payment initiation should be the harmonization of the CDR and NPP consent mechanisms to ensure inter-operability to enable efficient implementation by ADIs and a single consistent customer experience (see comments on New Payments Platform).

Linkages and interoperability with existing frameworks and infrastructure

Digital ID

The Inquiry will consider, for example, how customer authentication requirements for the Consumer Data Right relate, or could link, to other digital identification and verification processes.

Digital identity is, or at least has the potential to become, a key element of a digital and open data economy. This is because *'in our digital society, trust is determined through digital identity—the corpus of data about an individual, an object, or an organization that helps identify them through unique qualities and use patterns.'*[72]

Digital identity is catered for in a rudimentary manner within the current version of the CDR legislative framework. The CDR standards specify a binding mechanism between the accredited data recipient and the data holder whereby the user presents an identifier that the data holder will recognise which it then uses to send a onetime password to the user through a known and trusted channel. At no point does the user provide their credentials to the data holder. No further guidance is provided on the use of digital identity within CDR standards.

As the CDR is extended to other sectors the proliferation of data holders and accredited data recipients will inevitably result in an administrative burden for users – consent fatigue and message fatigue – as they are asked to manage additional usernames and passwords, one for each accredited data recipient with which they sign up.

> *'One of the obstacles to third party access is the difficulty of verifying the customer's identity and their consent to the disclosure. ...arrangements for third party access are made more problematic by different market participants adopting different verification and consent requirements.'* [73]

Data holders have spent many years building sophisticated authentication systems that ensure that their users have secure and frictionless access to their data. Raise the assurance bar too high and the user is burdened with too many access challenges; drop the bar too low and security is at risk. Getting the right level of assurance for the resources or services being accessed is a difficult challenge and tends to be refined over time. However, these sophisticated systems are not currently available to accredited data recipients and so they must build their own digital identity systems into their offerings.

> *'In today's "zero trust" environment, companies continuously monitor and authenticate users—constantly determining their level of risk based on who they are, what they access, and when and where they do it.'* [74]

As the market for services from accredited data recipients is hoped to be vibrant and competitive, time to market will be important factor in the success of fledgling FinTechs aiming for a return on their investment. This market pressure has the potential to drive their focus towards financial functionality (competitive edge) and away from the less visible aspects of digital identity and security. As a result, there could be a range of assurance levels for authentication across accredited data recipients managing similar types of data. As the CDR is expanded to other sectors, the sensitivity of some data and the possibility of extending CDR to write access including payment initiation will require more sophisticated authentication systems.

Over time, users will want to see consistent levels of assurance being used across both their data holders and their accredited data recipients. Consistency will foster trust by demonstrating that an individual's data is being protected in a similar manner across systems.

---

[72] Deloitte Insights, *Rediscovering your identity: How a comprehensive approach to digital identity management can empower everyone*, 2019. See also: https://www2.deloitte.com/content/dam/insights/us/articles/6359_rediscovering-your-identity/DI_rediscovering_your-identity.pdf

[73] Australian Energy Council, *Open Banking and the implementation of the Consumer Data Right: Implications for energy sector*, 23 March 2018. See also: https://treasury.gov.au/consultation/c2018-t247313/ :

[74] Deloitte Insights (2019), page 4

Data holders have also built sophisticated mechanisms for access delegation. Delegation can take many forms: read only access for an accountant to conduct tax returns, full delegated access for elderly or disabled people to family members or other trusted parties. Family sharing of access is also becoming common across many service providers. Users expect these mechanisms to be available when considering service offerings.

The Australian Federal Government identified the proliferation of delegation mechanisms across agencies a few years ago and as a result built the Relationship Authorisation Management (RAM) system. While still in its early stages, the motivation to provide citizens a common and consistent means to manage their government authorisations is a good one.

Delegated access does not currently form part of the CDR legislative framework, but it is possible that users will want to have this capability in the future.

Recommendation 12

Many users will inevitably want to use an existing trusted identity provider of choice to access their data recipients. To support this aim consideration should be given to extending the CDR standards to support OpenID Connect (OIDC) for accredited data recipients so that users can choose to bring their own identity, for example Apple ID.

Data holders could be encouraged to either provide their existing digital identity systems as identity providers to the data holder market, and/or participate in the Government's Trusted Digital Identity Framework (TDIF) as an Identity Provider.

Consideration should also be given to extending the CDR standards to accommodate TDIF identity providers such as Australia Post's Digital iD.

Recommendation 13

As data holders mature, users will expect to see delegated administration capability. To support this aim consideration should be given to extending the CDR standards to define delegation for digital identity. In addition an authorisation management broker should be defined and opened to the market for implementation. This could be based on the federal government's RAM system.

Recommendation 14

As write access or transaction initiation becomes part of the CDR standards, it will be important to have a clear and consistent level of assurance framework.

To support this, a level of assurance framework should be developed along the lines of the TDIF. As data types and transactions are defined in CDR the appropriate level of assurance should be mapped to this data in the standards.

New Payments Platform

In the context of Open Banking, the Inquiry will consider how the Consumer Data Right, were it expanded to enable write access, could relate to or interact with existing and future payments systems and infrastructure, such as the New Payments Platform (NPP), Bulk Electronic Clearing System, and EFTPOS.

While the CDR currently neither requires nor supports write access, the ability to initiate a payment from a transaction account by a third party already exists in various forms in the payments system in Australia.

However, as we noted in one of the articles in Deloitte's Open Banking series, 'The introduction of the New Payments Platform (NPP) and, to a lesser degree, innovations by the card schemes, will make elements of payment initiation possible in 2020 with the full roll-out scheduled by 2022.'[75]

The NPP was launched in February 2018 and is Australia's first real-time payments infrastructure. NPP enables households, businesses and government agencies to make fast, any time, data-rich, and simply addressed payments.

The payments can be made with near real-time funds availability to the recipient, on a 24/7 basis between any supported account types across all participating institutions. This is possible because of the Fast Settlement Service (FSS) infrastructure developed by the Reserve Bank, which settles each payment in real time.[76, 77]

The NPP also introduces the concept of PayID, which is a customer-friendly alternative to identifying a bank account using a phone number, email address or Australian Business Number. Rather than requiring users to remember BSB and account numbers, NPP payments can be made using more easily remembered PayIDs.[78]

The implementation of write capability using the NPP is contingent on the implementation of third-party payments initiation messages and the NPP Mandated Payments Service (MPS) now laid out in the NPP roadmap.[79] MPS will enable customers to authorise third parties to initiate payments from their bank accounts using the NPP. It could also provide customers with the ability to manage the consents they have provided to authorising third parties to access funds and initiate payments from specified accounts.

NPP, FSS and MPS are significant changes to the Australian payments system. Using the NPP infrastructure and the platform's native capabilities, parties can develop innovative payment offerings to customers, provide additional remittance information with a payment, as well as be authorised to initiate payments.[80]

It was because these developments were anticipated, that the Review into Open Banking recommended that customer experience and take up of real-time person-to-person payments using the NPP infrastructure should be taken into account when considering extending the CDR to include write access.[81]

These capabilities could provide a similar if not greater functionality for customers than the payment initiation capability implemented under both the UK and EU open banking regimes (with the exception of international payments).

---

[75] Deloitte (December 2019)

[76] As of April 2020 there are more than 67 million Australian financial institution accounts NPP-enabled which is estimated at about 90% of all accounts that will eventually be reachable. Refer NPP Australia, *Update on the New Payments Platform Roadmap*, 30 April 2020. See also https://nppa.com.au/wp-content/uploads/2020/04/NPP-Roadmap-April-2020_final.pdf

[77] The Reserve Bank Fast Settlement Service (FSS) infrastructure provides for settlement of NPP transactions between financial institutions on a 24/7 basis across their Exchange Settlement Accounts (ESAs) at the Reserve Bank. Reserve Bank of Australia Bulletin, *The New Payments Platform and Fast Settlement Service*, 20 September 2018

[78] As of April 2020, there were approximately 4.7 million registered PayIDs. Refer NPP Australia (2020) page 3

[79] NPP Australia (2020), page 6

[80] Reserve Bank of Australia, The New Payments Platform. See also: https://www.rba.gov.au/payments-and-infrastructure/new-payments-platform/

[81] Review into Open Banking (2017), page 10

Comparing open banking payment initiation: NPP vs UK

Attribute	New Payments Platform	UK open banking payment initiation
Payment initiation APIs exist	API framework defined	Yes
Third party payments initiation mechanisms exist	Under development (Mandated Payments Service)	Yes
Customer consent framework	Under development (Mandated Payments Service)	Yes
Scheduled payments and standing payment order support	Under development (Mandated Payments Service)	Yes
Accessible to non-banks	Indirectly via a NPP participant as an 'Identified Institution' or potentially directly as a 'Connected Institution'[82]	Yes, as a Payment Initiation Service Provider
Connectivity required	Via one connection point[61]	Yes, via multiple connection points to each bank or via a shared API point
International Payments supported	No	Yes
Real time payment rails	NPP infrastructure	UK Faster Payments
Customer friendly account addressing	PayID (email, mobile number, ABN): relatively broad penetration PayM (mobile number): limited penetration	PayM (mobile number): limited penetration

How a customer provides their consent or authorisation for payments to be initiated by a TPP on their account is critical to the proposed MPS. The customer consent model and framework has been extensively developed as part of open banking read access, right down to detailed customer experience guidelines. Where it makes sense, given the differences in use cases, it would be useful for the payments consent process adopted by MPS to align to the open banking consent model. This would provide customers with a consistent consent experience.

eftpos Payments Australia Ltd is also developing an e-commerce capability that is likely to support third party payment authorisation in a similar manner to the other card schemes, and already supports digital wallets. eftpos is also proposing to develop a real-time payment capability in competition with the NPP, which it claims could lower cost.[83]

In implementing write access it will be important to develop a consistent customer experience. This would require harmonisation of the consent mechanisms across the CDR, NPP, eftpos Australia and other payment schemes, recognising that some differences exist in the technical, legal and compliance requirements for payments authorisation versus data sharing consent.

This would also allow inter-operability of alternative payment schemes improving the customer experience and reducing the implementation costs incurred by ADIs and other payments participants.

[82] Once payment initiation capability is available as per the NPP roadmap
[83] Eyers, James, *Eftpos outlines plan to take on payment behemoths*, Australian Financial Review, 24 October 2019.

Given NPP is building out the payment capability to provide third party payment initiation independent of CDR, a consistent payment initiation consent framework would also contribute to enhancing customer understanding and data literacy.

Recommendation 15

Where appropriate, the consent mechanisms used for payments undertaken through NPP, eftpos Australia and other payment schemes should be harmonised with the CDR read access consent framework, and any extension of this to include write access.

International Payments platforms

Globally international payments are based on standards such as ISO 20022 or SWIFT gpi for payments messages.

The incorporation of these standards when CDR is extended to include payment initiation will enhance the interoperability of Australia's open banking payment initiation functionality with payment systems used globally.

This could:

- contribute to a consistent customer experience
- enhance the ability of new entrants from other jurisdictions to operate in Australia, increasing competition
- reduce the implementation costs incurred by ADIs and other payments participants
- enhance the ability to transfer customer data across international borders to countries with comparable privacy and confidentiality regimes.

Recommendation 16

The standards used globally for international payments should be used as the basis for the standards developed to support payment initiation in the CDR regulatory framework.

Leveraging Consumer Data Right infrastructure

Information Security Standards

The Consumer Data Right has established solutions to problems that may also exist elsewhere in the digital economy – in particular, in relation to data portability and custodianship of data. For example ...:

- ***it establishes information security standards with the aim of ensuring that customer data is held safely from internal and external threats.***
- ***it provides systems of assurance and verification relating to compliance with these security standards (e.g. accreditation and the associated register).***

There are a range of existing regulatory frameworks that seek to address similar problems – often in potentially inconsistent or industry-specific ways which are not compatible or interoperable with each other. ...

In order for a data recipient to be able to request and receive data from a data holder under the Consumer Data Right, the data recipient must first be accredited by the Australian Competition and Consumer Commission. The Inquiry will consider whether there is potential to leverage this accreditation regime (or elements of the regime – such as the information security standards) in other contexts in developing a safe and efficient digital economy.

The Inquiry welcomes views on the above as well as any broader role that other aspects of the Consumer Data Right regime could play in supporting productivity and data security in the digital economy.

A range of industry standards exist to support organisations in assessing and mitigating their cyber security risks. Global cyber security standards such as ISO27001 Information Security Management and the NIST Cybersecurity Framework offer related control objectives and requirements, but differ in terms of scope and granularity. These standards are reviewed and updated on a periodic basis to remain consistent with industry trends and the global cyber threat environment.

These standards exist to provide a global better practice perspective on cyber security organisations and control objectives, with some tailored to specific industries. These include the:

- Australian Government's Information Security Manual
- AICPA Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy
- APRA CPS234 Information Security (for financial services institutions)
- Payment Card Industry Data Security Standards (PCI-DSS) (for credit card data)
- NERC Cyber Security Standards (for electrical utilities).

The CDR information security controls guidance retains a mapping against ISO27001, PCI-DSS and the AICPA Trust Services Criteria.

We agree that this can create a complex interrelationship between cyber security requirements in the protection of data depending on the network of control standards selected.

While acknowledging that the current CDR information security controls guidance are subjected to an assurance and accreditation mechanisms to measure organisational ability to protect data, they are a subset of the broader cyber security controls base that would be found in more holistic international and cross-industry standards.

The CDR information security controls, while generally consistent with control objectives and requirements raised in global and industry-specific standards, would require greater breadth to take into consideration additional areas including cyber security policy, operating models, governance, reporting, assurance and a broader cyber controls base.

There is merit in maintaining a consistent set of cyber security requirements for organisations that transcends industry-specific requirements for data security, where practical. This may be via expansion of the CDR information security control guidance, or consideration and adherence to other globally recognised standards.

If CDR information security guidance were to become a de facto equivalent standard, there would need to be a degree of oversight and governance to ensure they remain up to date and fit for purpose.

As additional sectors are designated under CDR, consideration should be given to whether the cyber security framework which would apply under CDR could replace any existing cyber security framework which applies to entities in that sector. This would contribute to standardised and simplified cyber security requirements for a specific sector.

This should support and be integrated with the architecture of any tiered accreditation. A base level of control must be applied across all instances; however additional tiers of control could be implemented depending on the attributes stored, volume and sensitivity of the data held and/or received by the CDR participant.

Consumer protection

The Inquiry invites submissions from interested parties on how to ensure that, as the Consumer Data Right develops, it does so in a manner that is ethical and fair, as well as inclusive of the needs and choices of all consumers. This includes ways to encourage socially beneficial uses for the Consumer Data Right.

It will be important that Australia's consumer protection legislative framework anticipates changes that could result from the emerging open data economy.

In Deloitte's submission on the Consumer Data Right legislation we noted certain design principles that should influence the CDR framework. These included:

- ensuring that there are appropriate and effective enforcement mechanisms consistent with an emphasis on outcome-based regulation;
- ensuring that a culture consistent with an emphasis on outcome-based regulation is maintained within each of the regulators.

Conduct

In one of the articles in Deloitte's open banking series, we noted that the introduction of open banking (as well as Comprehensive Credit Reporting (CCR)) is likely to mean that financial institutions will face competitive pressure to reduce interest rates and fees across all of the credit facilities they provide to customers. In response financial institutions will need to consider implementing strategic pricing, such as risk-based pricing, at an individual customer level.[84] Similar considerations could result in greater price discrimination in other sectors to which the CDR is extended.

This in turn results in potential conduct considerations of fairness, transparency, vulnerability and suitability.[85]

Fairness: The implementation of strategic pricing, including risk-based pricing, potentially raises fairness questions if certain customer segments experience significant increases in the price of borrowing, or are unable to access credit altogether.

If organisations adopt strategic pricing in response to CDR, open banking and CCR they will need to adjust for socially sensitive data such as gender, ethnic background, and family status.

An example of unintended consequences is redlining[86] – denying services to certain ethnic groups through selective price discrimination.[87] In the United States banks and insurers have been accused of defining zones in which minorities are unable to access financial services at reasonable rates (or at all) through an over-reliance on a risk-based view of the world.[88]

Vulnerability: Where organisations use the additional information from CDR (and CCR) to price discriminate between customers with differing credit risks, some vulnerable customers may be in a better position to demonstrate credit worthiness. However other vulnerable customers may be disadvantaged

---

[84] Deloitte, *Open banking: Potential pricing implications*, March 2018. See also: https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-open-banking-potential-pricing-implications-140618.pdf

[85] Deloitte, *Open Banking, Conduct: it's everyone's responsibility*, March 2018. See also: https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-open-banking-conduct-250319.pdf

[86] Badger, Emily, *Redlining: Still a thing*, Washington Post, 28 May 2015. The word has particular roots in the 1930s when the government-sponsored Home Owner's Loan Corporation first drafted maps of American communities to sort through which ones were worthy of mortgage lending. Neighborhoods were ranked and color-coded, and the D-rated ones — shunned for their "inharmonious" racial groups — were typically outlined in red. See also: https://www.washingtonpost.com/news/wonk/wp/2015/05/28/evidence-that-banks-still-deny-black-borrowers-just-as-they-did-50-years-ago/?utm_term=.20347640bf58

[87] Human Relations Commission, *Unlawful Discriminatory Predatory and Reverse Redlining Guidelines in Housing and Commercial Property*", Pennsylvania, 27 September 2017. See also: http://www.phrc.pa.gov/Resources/Law-and-Legal/Documents/Policies%20and%20Guidelines/Predatory%20Lending%20Guidelines.pdf

[88] Glantz, Aaron and Marintez, Emmanuel, *For people of color, banks are shutting the door to homeownership*, Reveal News, 15 February 2018. See also: https://www.revealnews.org/article/for-people-of-color-banks-are-shutting-the-door-to-homeownership/

if they experience a significantly higher price for credit or are excluded from access to finance or services altogether.

If credit or services are provided based only on a customer's current credit scores organisations risk ignoring an individual's propensity to improve their credit risk profile over their lifetime.

Transparency: Transparency means that better informed customers can be more conscious of their credit rating and behavioural factors that can affect perceptions of their credit risk. The Review into Open Banking noted that 'standard economic theory, and a range of corroborating empirical evidence, suggests that markets work most efficiently when: customers are informed; there is transparency in pricing and in the quality of available products and services; there is a level playing field between competitors; and where the costs of switching between providers and barriers to entry for new providers are low.'[89]

In addition to transparency of pricing and product features, financial institutions should be transparent with a customer about how their credit and pricing decisions are made.

The US Federal Trade Commission's (FTC) Risk-Based Pricing Rule requires lenders to notify consumers if they are getting worse terms of credit than those available to other consumers because of information in their credit report. In the US transparency regarding risk-based pricing requires customers to be able to:

1. Access information about how their risk-based price is determined
2. Understand in plain language the information used by the financial institution in determining the price of credit for that customer
3. Compare how risk-based pricing is implemented across different organisations to improve market competitiveness and prevent barriers to customer mobility and choice.

US financial institutions must also suggest ways in which customers can improve their perceived risk, such as paying down debt, or obtaining co-signing guarantors.

Under UK open banking regulations, banks are required to publish accurate and unbiased information that lets consumers evaluate their service quality. Transparency on service quality is intended to encourage banks to deliver a better customer experience.[90]

Suitability: Suitability is a question of whether an organisation should reasonably know whether there is a better option for the customer based on the information it has on hand.

While under the CDR organisations may receive more customer transaction information, their ability to make recommendations based on an assessment of a product's suitability for a customer may be impacted by their obligations under the consumer protection framework (i.e. general v personal advice obligations).

There are also claims that new entrants and new untested products can, and have in the past, led to significant predatory behaviour. Concern has also been expressed that additional choice can lead to additional complexity 'particularly for vulnerable and disadvantaged consumers.'[91]

These concerns may be amplified as the CDR is extended to other sectors of the economy and the use of platform-based business models increases.

Recommendation 17

As the CDR is implemented and extended to other sectors, consideration should be given to the interaction of the CDR with existing consumer protection frameworks and whether the regulatory framework in Australia addresses consumer protection issues that may emerge as a result of actions taken in response to CDR.

[89] Review into Open Banking (2017), p3

[90] Deloitte, *Open Banking, How to flourish in an uncertain future*, June 2017. See also: https://www2.deloitte.com/uk/en/pages/financial-services/articles/future-banking-open-banking-psd2-flourish-in-uncertainty.html.

[91] Consumer Action Law Centre, Financial Rights Legal Centre and Financial Counselling Australia, *Supplementary submission to the Open Banking Review - Issues Paper*, 25 October 2017. See also https://policy.consumeraction.org.au/tag/open-banking/

Responsible Lending

Credit licensees must comply with responsible lending conduct obligations[92] These obligations do not just apply to new credit contracts, but also, inter alia, when considering whether to increase a credit limit, assisting a consumer apply for an increased credit limit, and assisting a consumer by suggesting they remain in an existing credit contract.[93]

Under RG209, credit licensees – credit assistance providers and credit providers – must not enter into a credit contract with a consumer, suggest a credit contract to a consumer or assist a consumer to apply for a credit contract if the credit contract is unsuitable for the consumer. Credit providers are required to make a final assessment about whether the credit contract is ***'not unsuitable'*** for the consumer.[94]

Credit licensees are also required to have appropriate systems and processes to identify whether a proposed credit contract or consumer lease is likely to cause ***substantial hardship*** to a consumer.[95]

These requirements also apply to energy providers that provide loans for new energy products.

The sharing of customer transaction data between entities under the CDR has the potential to result in a significant increase in the amount of data acquired or held in relation to a particular customer.

As a result of the information about a customer that has been shared by a third party, a credit licensee may:

- where a credit facility was originally assessed as 'not unsuitable' for a customer, form a view based on the additional information received, and subsequent to the initial assessment, that a credit facility is no longer 'not unsuitable' for a customer (i.e. that it is in fact unsuitable)
- where a customer was not assessed as being in 'substantial hardship', form a view based on the additional information received, and subsequent to the initial assessment, that a person with a credit facility is subject to 'substantial hardship'.

Recommendation 18

Consideration could be given to clarifying how the National Credit Act should operate in relation to information shared as a result of the CDR legislation.

Analytics and AI

In another article in Deloitte's open banking series[96], we noted that a survey in 2018 highlighted that three quarters of executives involved in cognitive technologies believe that AI will substantially transform their companies within three years.[97] This can only be amplified in an environment in which more customer data is being shared.

AI is already giving rise to new ethical dilemmas, particularly in relation to considerations of fairness.[98] The heightened ethical responsibilities for use of data include how data is interpreted via algorithms. This requires an understanding of any unintended consequences and potential biases in algorithms. The use of socially sensitive data such as gender, ethnic background, and family status may have unintended

[92] These are set out in Regulatory Guide 209 Credit Licensing: Responsible Lending Conduct (RG209), Chapter 3 of the *National Consumer Credit Protection Act 2009* (the National Credit Act) and the consumer protection provisions in the *Australian Securities and Investments Commission Act 2001* (Part 2, Division 2)
[93] RG209.5 and RG209.6
[94] RG209.2
[95] RG209.102
[96] Deloitte, *Open banking: What does it mean for analytics and AI*, September 2018. See also:: https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-open-banking-analytics-ai-250319.pdf
[97] Davenport, Thomas H and Rajeeve Ronanki, *Artificial Intelligence for the Real World*, Harvard Business Review, Jan-Feb 2018. See also https://www2.deloitte.com/us/en/ pages/deloitte-analytics/articles/hbr-report-artificial-intelligence-for-the-real-world.html
[98] World Economic Forum, *The New Physics of Financial Services – How artificial intelligence is transforming the financial ecosystem*, August 2018. See also: https://www.weforum.org/reports/the-new-physics-of-financial-services-how-artificial-intelligence-is-transforming-the-financial-ecosystem

consequences when utilised to develop strategic pricing models. For example, analytics and algorithmic pricing could inadvertently change the pricing or access to credit for very specific customer segments. This could discriminate against a protected class of people.[99]

Bias can also be introduced where loan approvals are based solely on historical data such as repayment history. Axiomatically, it is not possible for an algorithm to determine the potential repayment history for loans which were not approved. This could introduce bias into a credit assessment or credit pricing algorithm for certain groups of people.[100]

> *'Even as many decisions enabled by algorithms have an increasingly profound impact, growing complexity can turn those algorithms into inscrutable black boxes. Although often enshrouded in an aura of objectivity and infallibility, algorithms can be vulnerable to a wide variety of risks, including accidental or intentional biases, errors, and fraud*.' [101]

To account for these factors organisations applying AI to CDR data would have to:

- Determine which type of biases to remove
- Assess direct and indirect fairness considerations
- Determine when fairness considerations will apply to groups and when to individuals
- Understand the difference between disparate treatment (intentional discrimination) and disparate impact (unintentional discrimination)
- Include both unfairness prevention and unfairness discovery in their model validation.[102]

These obligations would apply to both incumbents and new entrants. They may be more onerous to implement for non-traditional players with a limited track record in AI and algorithmic pricing.

Recommendation 19

As the CDR is implemented and extended to other sectors, consideration should be given to whether the regulatory framework in Australia addresses consumer protection issues that may emerge as a result of the use of AI and algorithms applied to data shared under CDR.

Comparator websites and 'best interests' duty

Comparator websites (also referred to as product comparison websites, price comparison websites and PCWs) use product and pricing information to help reduce some of the behavioural barriers to searching and switching by making comparisons of often complex products easier, and helping consumers in their decision making process. [103]

In Deloitte's open banking survey, comparator websites were one of the top three influencers of consumers' switching behaviour. [104] Comparator websites are almost twice as influential for people who changed their credit cards, personal loans and term deposits when compared to mortgages, transaction accounts and savings accounts.

The inclusion of write access in Australia's CDR framework would further enhance the opportunity for PCWs to create value for consumers by initiating and simplifying account opening and switching.

---

[99] Petrasic, Kevin with Benjamin Saul, James Greig, Matthew Bornfreund, *Algorithms and bias: what lenders need to know*, White & Case, 20 January 2017. See also: https:// www.whitecase.com/publications/insight/algorithms-and-bias-what-lenders-need-know

[100] This is known as sample selection bias

[101] Deloitte, *How CDO's can manage algorithmic risk*, June 2018. See also: https://www2.deloitte.com/insights/us/en/industry/public-sector/chief-data-officer-governmentplaybook/how-cdos-can-manage-algorithmic-risks-and-data-ethics.html

[102] Kamishima, Toshihiro, *Fairness aware data mining: Sources of Unfairness in Machine Learning*, 2018. See also: http://www.kamishima.net/fadm/

[103] These were noted in the ACCC's report in 2014 on the comparator website industry. Australian Competition and Consumer Commission, *The comparator website industry in Australia*, November 2014. See also: https://www.accc.gov.au/system/files/926_Comparator%20website%20industry%20in%20Australia%20report_FA.pdf

[104] Deloitte, Open Banking: Switch or Stick, October 2019, page 41

However, while comparator websites are influential when helping people understand product information, most people do not yet trust them enough to provide them with their customer account and banking transaction information. Most people use comparator websites for research rather than purchasing, with people's willingness to purchase via comparator websites held back by relationship trust gaps, what the ACCC has referred to as 'a lack of consumer trust in the motivations of, and benefits offered by, comparator websites'.[105]

The ACCC's report highlighted a number of concerns about conduct in the industry[106]:

- the extent to which information provided by PCWs was unbiased, impartial or independent
- the ability to manipulate algorithms used to match providers with an individual consumer's stated preferences
- the preferential treatment of some products based on commercial relationships rather than an individual consumer's stated preferences
- the creation of artificial churn – particularly where driven by the remuneration structure under which the PCW is compensated.

As well as the potential benefits it can provide, write access has the potential to amplify these concerns and the potential harm to consumers.

The ACCC is currently seeking feedback on the role of third-party service providers who collect or facilitate the collection of CDR data on behalf of accredited data recipients (intermediaries) and the disclosure of CDR data to non-accredited third parties.

Some classes of entities which may be classified as intermediaries, or seek tiered accreditation already have a duty to act in their customer's interests. These include for example, accountants and financial advisers. Following the Hayne Royal Commission, the 'best interests' duty has been extended to mortgage brokers. Some comparator websites operate under a mortgage broker's Australian Credit Licence (ACL) and therefore this 'best interest' duty will apply to them. However other classes of entities may continue to be remunerated on a commission basis.

Recommendation 20

As the consumer data right is extended to other sectors and if intermediaries are included as CDR participants it will be important that consumer protection legislation keeps up with Australia's nascent open data economy.

In particular this should include a review of the legislative framework under which PCWs operate, particularly if PCWs have the ability to open accounts on behalf of a customer or initiate payments once write access forms part of the CDR framework.

[105] ACCC (November 2014).
[106] ACCC (November 2014), pages 18-29

Privacy

The Inquiry will also consider potential privacy impacts of expanding the functionality of the Consumer Data Right in the ways described in this Issues Paper, and how any privacy risks may be mitigated.

Consent: Consent is a central component of information privacy, providing individuals with meaningful control over the way in which their personal information is collected and used.

An expansion of the CDR to include a wider range of industries, providers and functions will increase the number of opportunities and requests received by individuals from accredited recipients seeking to collect and use their CDR information. The capacity of certain individuals to provide free and informed consent may be significantly impaired where those individuals are vulnerable, disadvantaged or under duress (see comments on Conduct).

Under an expanded CDR, individuals with impaired capacity will be at an increased risk of providing consent to a broader range of CDR enabled services with potentially significant financial implications.

Greater safeguards may therefore be necessary to ensure, for example, that individuals at risk of domestic violence or financial hardship, minors or those with a disability are able to make a voluntary and informed decision about the collection and use of their CDR data. This is especially relevant in relation to joint-account holders.

The CDR rules could include the addition of 'capacity' as a requisite element of express consent, in effect requiring a CDR participant to take into account a customer's circumstances prior to collection of their CDR information.

Protection of Minors: The CDR Rules currently preclude individuals under the age of 18 from becoming 'eligible' CDR customers for the purposes of the banking sector. Further expansion of the CDR to include a broader range of industries and providers may create an opportunity to lower the age of eligibility to include children and minors.

Any future expansion of the CDR which grants CDR eligibility to minors should be accompanied by specific protections, such as those enshrined within the GDPR, to account for the imbalance in negotiating power between CDR participants and minors.

Other Matters

We invite interested parties to make submissions on any or all issues raised by this Issues Paper or the Terms of Reference. This includes views on potential developments and expansions in Consumer Data Right functionality, including their benefit and priority.

Designation of a Sector (Section56AD)

The CDR legislation includes a specific requirement for the Minister to consider consumer impact, market efficiency, privacy, competition, innovation, regulatory impact and other relevant matters before designating a sector (Section 56AD).

We have previously noted that 'regulation, and the compliance burden that accompanies it, comes at a cost. An unduly onerous regulatory or supervisory system risks adding unnecessary costs and restricting innovation throughout the economy. Good regulation must carefully consider this balance. Specifically, it should be demonstrably welfare enhancing. Overall, **a regulation should only be enacted if its benefits outweigh its costs**.' [107] This same principle applies to the designation of an industry sector for application of the CDR.

As a matter of principle, broadly defined benefits should be weighed against broadly defined costs, not just the regulatory burden component of costs. Thus, a Regulatory Impact Assessment (RIA) should seek to provide answers to questions such as:

- how much is consumer switching between providers likely to increase if consumers are provided with access to their data, but their ability and willingness to make decisions based on this information is not improved?
- how much will competition with large incumbents (as distinct from between large incumbents) increase if the large incumbents invest in superior capability to analyse the data and, hence innovate, while still benefiting from scale economies (including funding costs)?
- will the regulator and standards body have sufficient capability and capacity to meet demand in a timely manner, e.g. for accreditation?
- will the additional regulatory burden applied to accredited data recipients outweigh the benefits of receiving data?

The Chairman of the ACCC has recently reinforced that the CDR is a profound, economy wide reform which will be rolled out to all sectors of the economy.[108]

Determining the regulatory impact of designating a sector is important. This was acknowledged in the Explanatory Memorandum to the CDR which noted: 'While the CDR is intended to enhance competition, that should not occur at the expense of significant regulatory burden or disruption unless the **broadly defined benefits** of designation outweigh the **regulatory** impact.'[109] [Emphasis added]

The government has identified banking, energy (electricity) and telecommunications as sectors to which the CDR will be applied. Government ministers have, at various times, speculated about the extension of the CDR to superannuation, insurance and private health insurance. Others have speculated about the extension of CDR to investment management, platform businesses and loyalty schemes (which would cover a number of industries).

The growth of the Internet of Things will see consumers generating more data that is recorded by organisations. For consumers, this data will come from a range of sources: smart homes, remote appliances, connected cars and 'interoperable in-vehicle telematics platforms', personal health, activity and fitness data, and more. For example, some companies are offering energy devices that read

[107] Deloitte Access Economics, *Shaping the Future: Deloitte submission to the Interim Report of the Financial System Inquiry*, 26 August 2014
[108] Comments by Rod Sims, Chair of the ACCC at the AFR/Deloitte Banking & Wealth Summit, 30 March 2020.
[109] Australian Government, The Treasury, *Exposure Draft Explanatory Materials*, 2018, paragraph 1.34, page 10

household power levels a million times a second (compared to eight to twelve second intervals for 'smart meters'), providing data in real time on which appliances are operating. They can also identify specific appliances through their operating power 'signature'.[110]

This broadening of data further expands the potential sectors to which the CDR could be applied and broadens the value that could be created from cross-sector data sharing.

Given the potential impact that data sharing has on competition in a sector, and the resultant impact on organisational strategy, as well as the costs associated with preparing for CDR as a data holder or a potential data recipient, it would be helpful in the ACCC invited submissions on which sectors should be considered for designation, and then set out a medium term roadmap outlining the timeline in which the cost-benefit analysis for these sectors will be completed.

This would also result in greater accountability for the ACCC to ensure that the CDR is expanded to other sectors and enable them to commence the Regulatory Impact Assessment (RIA) process.

Recommendation 21

The ACCC should invite submissions on which sectors should be considered for designation, and then set out a medium-term roadmap outlining the timeline in which the cost-benefit analysis for these sectors will be completed.

Reciprocity

As the CDR is expanded to other sectors, the ACCC may also need to revisit the concept of reciprocity, a topic which was the subject of many points of view during the legislative framework consultation process.

In its paper on reciprocity, the Institute of International Finance noted: 'Data gathered from the provision of one service has value in other markets, and increasingly so with more advanced data analytics based on artificial intelligence.' It noted that making customers' data portable 'needs to occur equally across sectors so as to not accidentally distort competition.' [111]

Currently the CDR legislation pragmatically limits the concept of reciprocity and equivalent data to the data sets outlined in the designation instrument for a sector. To do otherwise would have resulted initially in the de facto extension of CDR from one sector (such as banking) to any other sector from which a non-traditional competitor emerged.

However, as the CDR matures and expands to other sectors, and as industry boundaries blur, it is possible that competitors could emerge from one sector providing specific services to a designated sector. Their competitive advantage could arise from aggregating data from a non-designated sector (which is not shareable) with data that is required to be shared by an entity operating in a designated sector.

For example, airlines, supermarkets and digital platform businesses currently provide some financial services. It is possible that companies in any of these sectors could seek to expand their financial services offerings. Their ability to compete could, at least in part, be determined by data they hold in relation to a customer's shopping patterns and products, their travel history, or their search history and social interactions.

One submission on the CDR legislation noted that 'If it is identified that social networks were regularly obtaining transaction data from the banking sector, that sector should be subject to designation as a priority.' [112]

[110] Talbot, David, *Find out Which Appliance is Sucking all your Power*, MIT Technology Review, 13 July 2016. See also https://www.technologyreview.com/s/601881/find-out-which-appliance-is-sucking-all-your-power/

[111] Institute of International Finance, *Reciprocity in Customer Data Sharing Frameworks*, July 2018, page 2-3. See also: https://www.iif.com/Publications/ID/1684/Reciprocity-in-Customer-Data-Sharing-Frameworks

[112] Australian Retail Credit Association, *Submission on the Treasury Laws Amendment (Consumer Data Right) Bill 2018*, 7 September 2018.

Where this non-financial data, when combined with traditional financial transaction data, provides a competitive advantage, it is not clear why a consumer should not be allowed to access this data and choose to share it.

As a result, as the roadmap for inclusion of other sectors is established, the treatment of equivalent data and the principle of reciprocity may need to be reviewed and amended.

Consumer Data Rules (Section 56BA)

The ACCC will be responsible for defining rules across sectors, data classes, and CDR participants (customers, data holders, accredited data recipients, and potentially intermediaries). These rules may deal with, inter alia, disclosure of CDR data.

To support consumer awareness and understanding of the operation of open data in the Australian economy, the Commission should minimise the extent to which different rules are applied in different sectors and limit differences to those necessary to give effect to the application of CDR data sharing in that sector.

Interaction of CDR with Financial Crime legislation

Identity & Verification

One of the matters that is not included in the CDR legislation is the sharing of information about the outcomes of identity verification.

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) and AML/CTF Rules (2007) (AML/CTF Rules) allow reporting entities required to adopt an AML/CTF program to apply a risk-based approach to identifying, mitigating and managing financial crime risk. In essence, this allows a tiered approach to the identification and verification of all customers.

The Review into Open Banking highlighted the possibility of amendments to the AML/CTF Act to facilitate the sharing of standard Know-Your-Customer (KYC) information, principally the minimum identification and verification standards of specified entity types in Part 4 of the AML/CTF Rules.

There are two ways that the CDR could be used to support identity verification. One is through sharing the provision of customer data such as name, address and date of birth if directed by a customer to do so. The second is through sharing the outcome of an identity verification assessment performed on a customer if directed by a customer to do so.

For the first method, while the CDR data that an individual customer can choose to share includes their name and residential address, it does not include date of birth. Date of birth is a core requirement for the identification and verification of individual customers.

Reporting entities under the AML/CTF Act that were seeking to meet their KYC obligations through CDR data would need to identify a customer's date of birth from an alternate source.

The Review recommended the second approach, whereby:

> *'If directed by the customer to do so, data holders should be obliged to share the outcome of an identity verification assessment performed on the customer, provided the anti-money laundering laws are amended to allow data recipients to rely on that outcome.'* [113]

The Review noted that 'granting customers the right to instruct their bank to share the result of an identity verification assessment performed on them could improve efficiencies in the system'. [114] However, it cautioned that 'obtaining access to the supporting documents provided by an individual as part of an identity verification is one of the most common methods of identity theft.' [115]

[113] Review into Open Banking (2017), Recommendation 3.4, page 39
[114] Review into Open Banking (2017), page 38
[115] Review into Open Banking (2017), page 38

The amendments to the AML/CTF laws to allow third party reliance on an organisation's KYC protocols purposes are contained in the Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2019.[116] This bill has gone through review by a Parliamentary Select Committee and is currently awaiting passage into law through Parliament.

The Bill would allow a reporting entity under the AML/CTF Act to place reliance on the Customer Identification Procedure of another reporting entity but only if:

1. Initial due diligence is undertaken on the Customer Identification Program of the reporting entity on whom you seek to place reliance; and
2. Ongoing due diligence is also undertaken on the Customer Identification Program of the reporting entity on whom you have placed reliance.

To support the development of a digital economy it will be important that existing KYC processes undertaken by reporting entities are robust. It will be important for AUSTRAC to provide clear specification of KYC due diligence standards and appropriate regulatory oversight and enforcement to provide an environment which supports the CDR and maintains the accuracy and integrity of Customer Identification Data.

The effect of the additional initial and ongoing due diligence requirements outlined in the Bill is that a reporting entity which undertakes its own KYC due diligence could be approached by multiple reporting entities (e.g. challenger banks) seeking to undertake initial and ongoing due diligence on their Customer Identification Program. It is possible this could result in significant costs being incurred by both reporting entities and could create an impediment to a data recipient being able to rely on the outcomes of the identity verification assessment performed by a data holder.

In addition, it remains to be seen in practice whether reporting entities will be willing to release the outcome of risk-based identification and verification assessments performed on a customer to entities that are not AML/CTF reporting entities and who request the outcome of an identity verification assessment.

Recommendation 22

AUSTRAC should provide early guidance on the different data identification standards to assist a smooth regulatory transition to open banking and the CDR.

Recommendation 23

The government should review how the changes set out in the AML/CTF Amendment Bill impact the transfer of the outcome of a KYC assessment by a data holder to an accredited data recipient. In addition, it should review the impact on organisations who are not reporting entities for AUSTRAC.

[116] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6431

Suspicious Matter Reporting

Currently reporting entities under the AML/CTF Act are required to submit a Suspicious Matter Report (SMR) to AUSTRAC if, at any time while dealing with a customer, the entity forms a suspicion on a matter that may be related to an offence, tax evasion or proceeds of crime.

The sharing of customer transaction data between entities under open banking has the potential to result in a significant increase in the amount of data acquired or held in relation to a particular customer, both by individual entities that take advantage of open banking data sharing, and across the platform. In these circumstances a matter may only become suspicious, and therefore reportable, when considering the combined data about a customer, particularly the additional shared data.

Reporting entities may need to develop new risk-based monitoring, administration and reporting techniques where data obtained through CDR highlights unusual or suspicious identification profiles.

Recommendation 24

AUSTRAC should provide guidance on reporting entities' obligations to use data shared under CDR when meeting their suspicious matter reporting obligations under the AML/CTF Act.

Contact us

Paul Wiebusch
Partner, Open Data I Open Banking
+61 3 9671 7080
pwiebusch@deloitte.com.au

Robin Scarborough
Partner, Customer Strategy & Design
roscarborough@deloitte.com.au
+61 2 9322 3833

Kristina Craig,
Director, Customer Strategy & Design
+61 282606101
kristinacraig@deloitte.com.au

Dan Nilsson
Partner, Platform Engineering
+61 3 9671 8925
dnilsson@deloitte.com.au

Melissa Ferrer
Partner, Data
+61 2 9322 7844
meferrer@deloitte.com.au

John Jones
Partner, Digital ID
+61 2 8260 6636
johjones@deloitte.com.au

Daniella Kafouris
Partner, Privacy
+61 3 9671 7658
dkafouris@deloitte.com.au

David Batch
Partner, Privacy
+61 2 8260 4122
dbatch@deloitte.com.au

Piya Shedden
Director, Privacy
+61 3 9671 6077
pishedden@deloitte.com.au

Richard Miller
Partner, Payments
+61 3 9671 7903
rmiller@deloitte.com.au

David Giddy
Principal, Open Data Accreditation
+61 3 9671 5122
dgiddy@deloitte.com.au

Rosalyn Teskey
Partner, Conduct Advisory
+61 3 9671 6473
rteskey@deloitte.com.au

Chris Cass
Principle, Financial Crime
+61 2 9322 7070
ccass@deloitte.com.au

Paul Rehder
National Leader, Banking
+61 3 9671 8058
prehder@deloitte.com.au

Michael Rath
National Leader, Energy & Resources
+61 3 9671 6465
mrath@deloitte.com.au

Tanya Schneider
Partner, Open Data, Energy
+61 404 644 072
taschneider@deloitte.com.au

John O'Mahony
Partner, Deloitte Access Economics
+61 2 9322 7877
joomahony@deloitte.com.au

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/au/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte’s approximately 244,000 professionals are committed to becoming the standard of excellence.

About Deloitte Australia

In Australia, the member firm is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia’s leading professional services firms. Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 7,000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at www.deloitte.com.au.