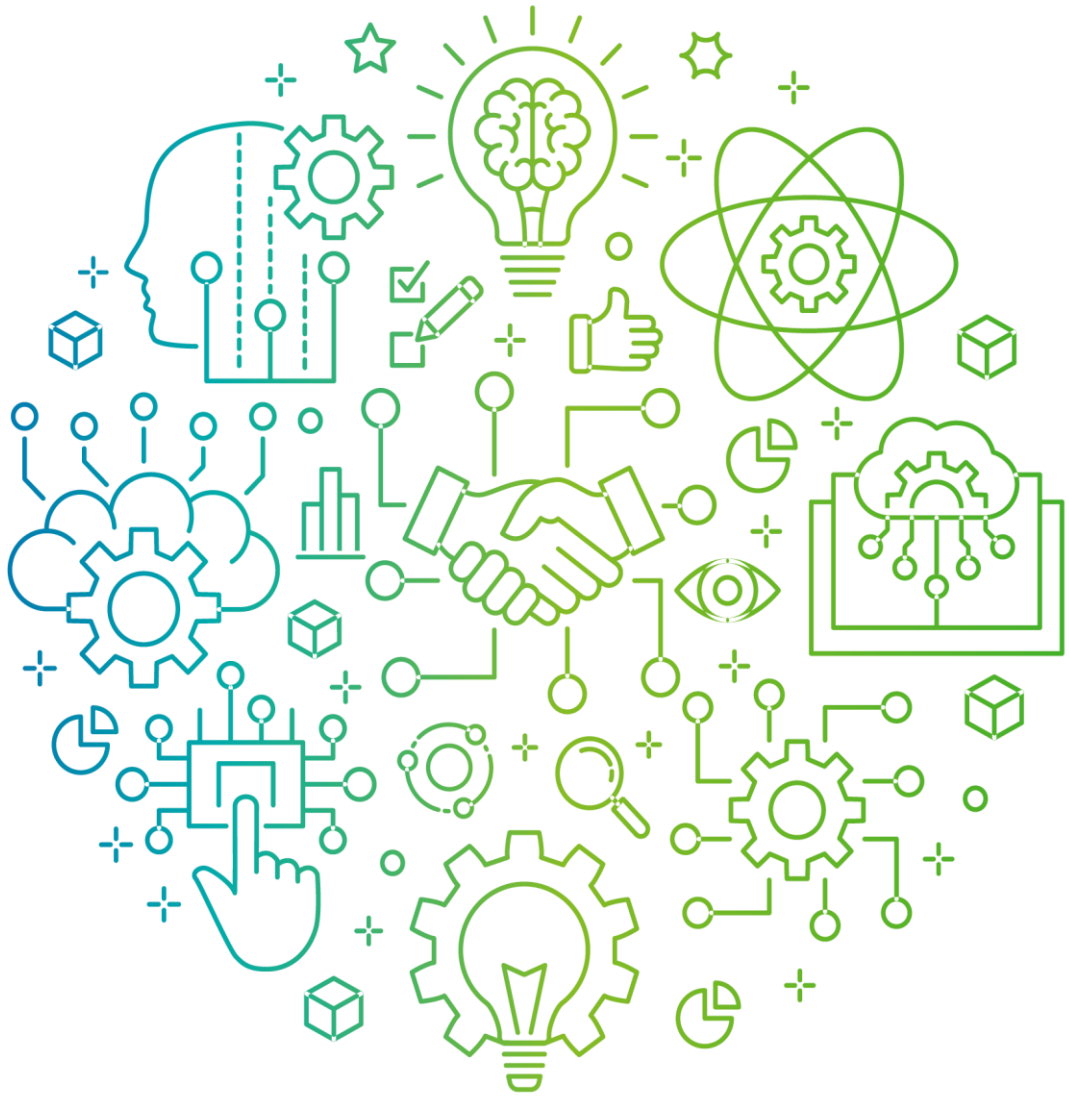
Deloitte.



Supporting New Zealand's Digital Economy

Submission to MBIE on options for establishing a Consumer Data Right

October 2020

Table of Contents

Section 1: Introduction

Introduction

On 5 August 2020 the Ministry of Business, Innovation and Employment (MBIE) released a discussion document titled *Options for Establishing a Consumer Data Right in New Zealand,* seeking input on whether to develop a consumer data right (CDR) in New Zealand to give individuals and businesses greater choice and control over their data.

Globally there are a range of approaches which have been adopted by countries and jurisdictions to data rights, privacy and data sharing, as well as specifically to open banking. Broadly speaking, some jurisdictions have allowed market-driven approaches, some have specific sector initiatives underway (e.g. Japan, Singapore and USA) while others have opted for regulatory intervention (e.g. the European Union (EU), Hong Kong and Australia).

Countries that have started with a focus on open banking, are now starting to explore the pathway to open finance and ultimately open data across the economy. Jurisdictions, such as the EU, which have started with a focus on privacy (through their General Data Protection Regulation (GDPR)) and payments (Payments System Directive (PSD2)) are now pursuing a broader data strategy as they seek to become leaders in a data-driven society.[1]

Australia, which started with a focus on data availability and use across the economy[2] and has established a consumer data sharing right, is now reviewing the path beyond banking, the first sector to which Australia's Consumer Data Right (ACDR) was applied, and beyond just data sharing (i.e. 'read-access'), to explore the potential that account opening and payment initiation (i.e. 'write access') have to enhance the ACDR.

Several countries, like New Zealand, are reviewing these global developments to determine the right framework and the right timeframe for data sharing in their environment.

Deloitte is pleased to provide in this submission its views on options for establishing a Consumer Data Right in New Zealand.

Summary comment

Overall, we believe that data sharing, and open data more broadly, have significant potential to enhance the New Zealand economy. With digitisation already at our doorstep, New Zealand is part of a global economy that is rapidly driving towards a successful digital economy.

The challenges and opportunities that New Zealand faces as it decides whether and how to develop a consumer data right are a subset of those it faces to ensure New Zealand is well-placed to transition to the digital economy.

Solving the right problem

In determining whether we need a regulated framework for data sharing, New Zealand needs to be clear on what market failures we are seeking to solve using regulations. While regulations generally result in change, they are only effective if:

- They make a positive difference in the desired areas of intervention
- They are able to target the problem they are trying to correct as closely as possible
- The benefit of this intervention outweighs the costs associated with complying and enforcing the regulation.

[1] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, 19 February 2020. Refer https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en#:~:text=The%20European%20data%20strategy%20aims,businesses%2C%20researchers%20and%20public%20administrations.

[2] Productivity Commission Data Availability and Use Inquiry Report No. 82, 31 March 2017. Refer https://www.pc.gov.au/inquiries/completed/data-access/report

When deciding whether we need a CDR and how it would be implemented we are trying to balance a range of, sometimes conflicting, considerations:

- Protecting privacy in the face of a rapid digitisation
- Protecting consumers, especially for groups who may be particularly at risk
- Enabling greater economic benefits for New Zealand within a global market through increased data sharing
- Enhancing competition by reducing barriers for competitors and new entrants
- Driving innovation in products and services
- Empowering consumers by simplifying access to consumer data
- Driving choice for New Zealanders to share their data across multiple data holders
- Driving convenience for New Zealanders when it comes to sharing their data
- Ensuring there are sufficient safeguards so that New Zealanders can share data with confidence.

While CDR legislation can promote the above agendas, its design can just as easily be counterproductive. For example, new regulation can both be seen to stimulate competition and the economy by expanding consumer choice and seen as another cost of compliance which keeps new entrants at bay. For regulation to be effective, it is also increasingly important that it keeps pace with developments in the digital economy.[3]

CDR model for New Zealand

The MBIE has stated that its preference is for a CDR regulatory framework that is similar to the Australian model (Option Two).

It has been clear through the consultation process on the Australian CDR (ACDR) legislation and Rules framework that there is a wide range of often conflicting views on the design and scope of the ACDR. This same challenge is likely to face New Zealand.

Even though customer transaction data sharing only commenced in July 2020, the Australian government is undertaking an Inquiry into Future Directions for the Consumer Data Right. The Issues Paper for this Inquiry invited submissions on issues which will be relevant to the MBIE's consultation. These included leveraging international developments, behavioural and regulatory barriers to switching, the potential for developing a consent taxonomy, tiered accreditation and the role of intermediaries, the risks and benefits of including 'write access' in the CDR, interoperability of the CDR with other data portability regimes and consumer protection.

The submissions to the Inquiry contained a diverse and often conflicting range of observations, comments and recommendations. These points of view will be relevant to the MBIE as it considers whether New Zealand should implement a CDR and how it should be designed.

The majority of submissions supported the implementation of a CDR – and its role in supporting innovation and consumer benefits. Only a minority argued for a market-led approach – principally to create a lower-cost approach.

Deloitte has prepared a summary of the submissions to that Inquiry in our paper "Where to now? The future for the Consumer Data Right".[4]

[3] Productivity Commission, Information Paper: Regulatory Technology, October 2020. Refer: https://www.pc.gov.au/research/completed/regulatory-technology/regulatory-technology.pdf

[4] Deloitte Australia, The future for the Consumer Data Right, September 2020. Refer https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-deloitte-open-banking-where-to-now-future-of-consumer-data-right-160920.pdf

Essential ingredients for success

The Report on Open Banking in Australia (the Farrell Review)[5] noted that the objective of a Consumer Data Right should fundamentally be about 'reducing information asymmetries — giving customers better access to the information they need to enable them to make better decisions and to seek out products that better suit their circumstances.'[6] This same principle holds true for New Zealand.

To achieve this objective, two conditions are necessary:

1. **Trust** – so consumers are willing to share data. Consumers need to trust the regulatory framework in which they are sharing data, trust that the consent and data sharing process is secure, trust that the data recipients will keep their data secure, and trust that the data recipients will only use data the consumer has shared for the purpose and time frame for which it has been shared. Trust is both structural – people have confidence in the data-sharing framework – and behavioural – people trust the process when the benefits are explained, and as they see and experience it. This is supported by clear consent frameworks, accreditation, and a regulatory framework in which consumers have confidence.

2. **Value** – so consumers have a reason to share data. Consumers are choosing to share their private data because of the value that they expect to realise in exchange for sharing that information. This value can take many forms including, for example, saving consumers time or money, keeping them on track with their goals and objectives, making processes more convenient, inspiring them, providing them with rewards for their transactions or information, and helping keep their money and information secure.

Finding the balance between trust and delivery of value means that any accreditation criteria for a CDR need to be stringent enough to create trust, but not so stringent that they drive out new entrants or innovation which delivers value to consumers.

This was highlighted in a survey of consumer behaviour published by Deloitte in October 2019 after the enactment of CDR but ahead of the launch of account and transaction data sharing.[7]

The design of a data-sharing regulatory framework for New Zealand must also consider the scale and nature of New Zealand's economy. New Zealand has a relatively small population compared to other countries, with small to medium-sized businesses (SMEs) generating almost 30% of New Zealand's Gross Domestic Product, employing almost 30% of all New Zealand employees and accounting for 97% of all New Zealand businesses.[8]

The growth of Artificial Intelligence (AI) and machine learning together with increased data sharing in our small population, increase the risk that anonymised data can be re-identified. From a privacy perspective, this would support having more stringent controls that also incorporate data ethics.

The scale of the SME sector also makes it important that the compliance costs associated with participating in a regulated data-sharing environment do not inadvertently create barriers to entry for this sector.

We have included comments on these issues in our submission.

New Zealand has an opportunity to learn from the Australian experience and from other jurisdictions which have implemented data sharing. Other key issues will include:

- Inclusion of write access to extend the value generated from open data
- Introducing intermediary and data aggregator roles and simplified/consistent tiered accreditation mechanisms based on quality standards to enhance security controls and minimise compliance costs for SMEs
- Considering the potential limitations of the sector designation approach and the concept of reciprocity to allow cross-sector innovation
- Exploring the benefits of consistency with Australia under the Trans-Tasman Mutual Recognition Arrangement.

---

[5] Australian Government, The Treasury, *Review into Open Banking: giving customers choice, convenience and confidence*, December 2017 (the Farrell Review). Refer: https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf

[6] Farrell Review (2017), page 41

[7] Deloitte, *Open Banking: Switch or Stick*, October 2019. Refer: https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-open-banking-survey-2019.pdf

[8] New Zealand Foreign Affairs & Trade. Refer: https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/cptpp/supporting-smes/

It is not just about CDR

When considering the issues associated with the design of a CDR for New Zealand, it is also important to remember that data-sharing is one element of the emerging digital economy. 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. 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.

New Zealand has an opportunity to design a CDR which is part of an enhanced regulatory framework supporting a digital economy.

Therefore, our paper includes comments on a range of related areas that would strengthen a CDR in New Zealand:

- Ensuring customer experience criteria are key elements in the design of a data-sharing framework to truly drive consistent user convenience.
- Reviewing the regulation of digital platforms which are becoming increasingly integral to value creation for businesses in a digital economy.[9]
- Reviewing the regulation of privacy as data rights are extended beyond the existing regulation, and seek consistency in consumer experience of data rights when data is collected and used as well as when it is shared.
- Creating a Digital ID framework to enable people to more easily engage in the digital economy and data sharing.
- Concurrently developing a regulatory framework for the use of AI, algorithms and machine learning, possibly leveraging the Algorithm charter for Aotearoa New Zealand[10] which is focused on how government agencies use algorithms.
- Enhancing consumer protection legislation so that they are appropriate for the emerging digital economy.
- Enhancing consumer literacy around data, privacy, the use of digital methods and the associated benefits. This may need to specifically address certain vulnerable cohorts within society.
- Supporting those parts of the community who may somehow be disadvantaged from are not able to or refuse to embrace a digital economy. The recent COVID-19 pandemic has shown that it is indeed possible to reduce this kind of gap considerably.

We believe ultimately this is where the goal should lie, and we need to get there quickly and safely. The CDR regulatory framework is important, but not the only element in building New Zealand's digital economy.

[9] Deloitte, *Platform Business Model explained…in under 100 words*. Refer: https://www2.deloitte.com/ch/en/pages/innovation/articles/platform-business-model-explained.html

[10] Data.govt.nz, *Algorithm charter for Aotearoa New Zealand*. Refer: https://data.govt.nz/use-data/data-ethics/government-algorithm-transparency-and-accountability/algorithm-charter

Section 2: Does New Zealand need a Consumer Data Right?

Regulatory Settings

Question 1: Are there any additional problems that are preventing greater data portability in New Zealand that have not been identified in this discussion document?

The discussion paper highlights the current role of the Privacy Act 1993 in regulating the collection, use and disclosure of personal information. It also sets out several potential concerns which have been raised about how regulatory factors are currently impacting consumer data portability.

In addition, to the issues noted in the discussion document, we believe privacy practices in New Zealand are likely to have similar challenges to those noted by the Australian Consumer and Competition Commission (ACCC) in its digital platforms inquiry[11] and its review of customer loyalty schemes[12], and in submissions on Australia's CDR legislation[13] and Rules Framework.[14] These reviews and submissions highlighted several 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 [15]
- There is a gap in privacy notice practices and data protection when compared with consumer expectations [16]
- The majority of consumers were not aware that the privacy policies and terms of use limited the extent of control they retain over their data [17]
- 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'[18]
- 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[19]
- 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 [20]
- Consumers are concerned about the sharing of their data with unknown third parties, with limited insight and control over how their data is shared [21]

[11] Australian Competition and Consumer Commission, Digital Platforms Inquiry, June 2019. See also: https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platforms-inquiry
[12] Australian Competition and Consumer Commission, Customer loyalty schemes, Final report, December 2019. See also: https://www.accc.gov.au/focus-areas/market-studies/customer-loyalty-schemes-review
[13] For example, Consumer Policy Research Centre, *Submission to Treasury Laws Amendment (Consumer Data Right) Bill 2018 – Exposure Draft*, 7 September 2018
[14] American Express, *Submission on the CDR Rules Framework*, October 2018, page 5. Refer: https://www.accc.gov.au/system/files/CDR%20-%20Rules%20-%20Submission%20to%20framework%20-%20American%20Express%20-%20PUBLIC%20VERSION.pdf
[15] ACCC (December 2019), page 34
[16] Nguyen, P. and Solomon, L., *Consumer Data and the Digital Economy*, 2018, as cited in Consumer Policy Research Centre (September 2018), page 2
[17] ACCC (June 2019), page 383
[18] ACCC (December 2019), pp vii and 34
[19] ACCC (June 2019), page 383
[20] ACCC (June 2019), page 384
[21] ACCC (December 2019), pp vii and 34

- 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[22]
- 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.[23]

The Australian 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.' [24]

It is notable that during Australia's 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 in Australia.

The 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.' [25]

There are a number of other considerations when designing the regulatory framework for a New Zealand CDR:

- One of the challenges in implementing a legislated consumer data right is to find the right balance between promoting competition and new entrants and at the same time avoiding privacy and cyber security risks. Potential data recipients will also need to build Application Programming Interfaces (APIs) to be able to share and receive data. However, it will be important that in establishing standards for privacy, cyber security and APIs, a legislated consumer data right in New Zealand does not inadvertently create new barriers to entry.

- It is clear that it will be important that organisations in New Zealand seeking to access customer data under a consumer data right will need to be able to comply with New Zealand's privacy legislation, meet minimum cyber security standards and be able to build the required APIs. However, technology capability is not evenly distributed and for some businesses, particularly smaller businesses and start-ups, meeting the minimum privacy and cyber security standards which would form part of New Zealand's consumer data right will be expensive.

- Australia has faced similar challenges. These have resulted in the ACCC publishing a discussion document on rules to permit the use of third-party service providers that collect or facilitate the collection of CDR permitted data from data holders on behalf of accredited persons ('intermediaries').[26] Given the small size of organisations participating in New Zealand's economy, it will be important that this issue is addressed when designing a CDR.

- Clear definitions will be required around where a consumer that is the subject of the CDR is (or is not) domiciled and any jurisdictional boundaries associated with data holders. Opening up the CDR to overseas entities and aligning with various overseas models of open data presents new risks and opportunities.

- Currently, the discussion paper does not include comments on reciprocity. Please refer to our response to question 16 for more details on this.

---

[22] American Express, *Submission on the CDR Rules Framework*, October 2018, page 5. Refer: https://www.accc.gov.au/system/files/CDR%20-%20Rules%20-%20Submission%20to%20framework%20-%20American%20Express%20-%20PUBLIC%20VERSION.pdf

[23] 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 (June 2019), page 391

[24] ACCC (June 2019), page 383

[25] ACCC (June 2019), page 3

[26] ACCC, *CDR Consultation paper – participation of third party services providers*, 23 December 2019. Refer: https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/accc-consultation-on-facilitating-participation-of-intermediaries-in-the-cdr-regime

The issues we have noted will be amplified as data sharing under a CDR is extended to more 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.' [27] These same issues will be heightened in a New Zealand CDR framework given our small population.

The discussion paper refers to businesses sharing data with consumers. There is also an opportunity for New Zealand to extend the CDR principles to data that citizens share with government agencies. This would support a number of principles covered in our opening summary, such as providing consistent customer experience across the economy and promoting innovation, including when consumers do business with government agencies.

One of the key limitations today is that New Zealand's regulatory framework does not present the requirements or conditions around sharing the data that agencies collect on individuals. This is left to the agency and the individual to work out. As a result, where it is shared, it is often not shared in a consistent format or there are fees associated with accessing the data. Further, there is no obligation to share, even with consent. These are likely because the data holder does not currently perceive it has any direct value to gain.

Benefits of a Consumer Data Right

Question 2: Do you agree with the potential benefits, costs or risks associated with a consumer data right as outlined in this discussion document? Why/why not?

Broadly, we agree with the benefits, costs and risks outlined which are also consistent with those noted in the Farrell Review in Australia.

Benefits	Costs/Risks
Enables innovation Data sharing is likely to hasten innovation by reducing barriers to new entrants. While the full range of new products and services, and their potential benefits cannot be foreseen, it is likely that some of these innovations will help address the behavioural biases and gaps in financial and data literacy that currently act as barriers to consumers searching for alternative providers and then deciding to switch. This is particularly important in supporting a digital economy.	**May delay innovation** Potential innovations may not be realised or may be delayed if the regulatory requirements for accreditation in a regulated data sharing environment are too high, if the data sharing mechanisms are too restrictive and if the roadmap to enabling economy-wide data sharing is unclear or too long.
Facilitates competition Competition is enhanced in a regulated data-sharing framework in which consumers have confidence, that has the potential to increase their willingness to engage with the innovative products and services offered by new entrants.	**May impose a barrier to entry** For consumers to realise the benefit of the innovation enabled by data sharing, it will be important that the accreditation process for data sharing regulation does not create a new barrier to entry which locks out new participants, but also maintains minimum standards for privacy and cyber security so that consumer trust and consumer protection are not compromised.
Strengthened privacy and data protection A successful CDR will result in more data being shared, with more data recipients across a broader range of industry sectors. This increases the risk that data can be intercepted or acquired by malicious actors. To maintain consumer confidence and trust, the regulatory framework should require that participants meet minimum	

[27] ACCC (June 2019), page 392

Benefits	Costs/Risks
standards for privacy and cyber security, and there are standards for data transfer.	
Increased productivity Data sharing has the potential to reduce the search and switching costs – financial, time, and behavioural – that consumers encounter when selecting products and services. It also has the potential to reduce the time and costs incurred by businesses during the application process that consumers go through when seeking a new product or service, such as credit assessment, and the costs associate with providing services to customers. A CDR encourages automation of processes that were previously manual, by virtue of using APIs that can be orchestrated by machine. The productivity benefits to New Zealand could be substantial.	**Implementation costs for government and industry** While there are potentially significant benefits, these need to be considered against the costs that will be incurred by the government in establishing and monitoring data sharing regulation, and the costs incurred by businesses in implementing and maintaining data sharing. .
Consumer welfare Consumer confidence and trust in the regulatory framework and participants are critical to the success of data sharing regulation. This is enhanced by a clear and consistent consent experience. Consumer welfare will also be enhanced with appropriate consideration of other factors such as regulation of AI and algorithms, and inclusion of the best interest duty for comparator websites. Consumer welfare is also supported when the data sharing regulatory framework includes a comprehensive liability framework with meaningful penalties.	

Question 3: Are there additional benefits, costs or risks that have not been explored in the above discussion on a consumer data right?

Potential additional benefits of establishing a CDR include:

Enabler of the digital economy: Data read and write access help to amplify and accelerate the digital transformation of business. This is particularly important in a post-COVID new normal as businesses globally are focused on digital delivery of services. Implemented well, a CDR has the potential to accelerate New Zealand towards lifting its digital trust framework so that even small businesses are required to adapt and therefore able to export digitally fit products and services.

Consumer confidence: A CDR implemented with the appropriate safeguards gives consumers greater confidence that their privacy rights are protected when exploring the use of new service providers and/or entirely new services, including those which may not be based in New Zealand. Further, data read and write access can help to address financial and data literacy issues that prevent people from searching for information or comparing providers.

Increasing technology capability for greater competition: A CDR forces a change in the technology capability of sectors upon its introduction. This has been seen, for example, in New Zealand's energy retail sector. Although the cost of this change is not insignificant, the improved technology capability sets the sector up to be more competitive, more resilient and better able to respond to market forces.

Simplifying compliance: A comprehensive CDR could make it easier for lenders to comply with responsible lending/ Credit Contracts and Consumer Finance Act (CCCFA) requirements through real-time access to customer credit information, ensuring customers are only taking on reasonable amounts of debt for their financial position.

Avoiding screen-scraping: There are a range of viewpoints on the merits of digital data capture (DDC) also referred to as screen scraping. Proponents have noted that it has been a necessary practice and an effective way of enabling new entrants to compete. In Australia the Australian Securities and Investment Commission (ASIC) has noted that they were not aware of any consumer loss from screen scraping[28], However, a number of organisations and consumer groups have noted that screen-scraping is an unsafe data sharing practice and raises significant privacy and security risks associated with the transferring of passwords, collection and processing of significant amounts of financially sensitive customer data. These organisations have called for screen-scraping to be banned or for reliance on it to be reduced.

A CDR could specifically call out and prohibit less secure methods of data sharing, including screen scraping, and therefore remove the security risks associated with this technique.

The following potential additional risks also exist which should be considered:

Unethical data processing: Data recipients may process consumer data unethically. This may pose a harm to individuals i.e. use of data for purposes other than the original purpose. There would also need to be clear rules in a CDR around accountabilities for data security and specifically the delineation points during the data transfer process. The design rules would also need to consider principles around data ethics to address these issues.

Marginalisation of the consumer: The development of new platforms that use algorithms / AI to profile a consumer and use it for their own benefits such as monetisation with no or little consumer benefit. Further, businesses may behave as if there is no obligation to provide a service without a customer disclosing a high level of personal data to a third party. This implies that certain business conduct considerations may be required in the overall CDR framework such as a 'best interests' duty to the consumer for businesses using CDR data. AI ethics would also need to be considered in the overall design rules.

Data accuracy: In a world of greater shared data and near-perfect information, there is an increased risk that a customer may in fact be disadvantaged if a data holder fails to correct erroneous information. The CDR could address this issue through enhancing the current privacy obligations around agencies maintaining accuracy of personal information (Principle 8 of the NZ Privacy Act 1993) and through incorporating the concept of write access within CDR to allow any shared agency to correct the source.

AI, algorithms and automated decision making: The adoption of a CDR will introduce heightened ethical responsibilities for use of shared data, including 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 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.

A CDR could also cause unexpected intelligence to be derived from aggregating data sets, given the relatively small population in New Zealand. Further, there is also a potential that de-identified data and derived data is still used by data holders even after a consumer revokes consent. These aspects need to be considered within the design rules for data sharing in New Zealand.

Pricing discrimination: The introduction of data sharing is likely to mean that organisations face competitive pressure to reduce prices, rates and fees across the products and services they provide to customers. In response, some organisations are likely to implement strategic pricing such as risk-based pricing at an individual customer level.

In financial services, for example, data sharing will potentially enhance the ability of financial institutions, particularly challenger banks and fintechs, to assess, price and manage the risk associated with each customer individually. This can occur at origination and throughout the life of a loan. By varying pricing to more accurately reflect a consumer's risk, rather than their bargaining power, risk-based pricing lowers the cost of credit for lower-risk customers, while higher-risk borrowers are provided credit, albeit at a higher price.

[28] Mr Sean Hughes, Commissioner, ASIC, *Committee Hansard*, 27 February 2020, page 9, as reported in the Commonwealth of Australia, the Senate, Select Committee on Financial Technology and Regulatory Technology. Refer: https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology/FinancialRegulatoryTech/Interim_report

However, a consequence could be that those with imperfect credit history are discriminated against if their data was not highly portable.

In designing New Zealand's data sharing regulatory framework it will be important that the framework adequately addresses potential conduct considerations of fairness, transparency, vulnerability and suitability.

Blurring industry boundaries: Increased use of open data can blur industry boundaries. There is a risk that an industry focussed approach to implementing a CDR distorts competition without the concurrent introduction of data-sharing reciprocity requirements. These risks are avoided if an economy-wide approach is adopted for data sharing, as is the case in the EU.

Inconsistent treatment of shared business data: The inclusion of businesses as parties that can share data introduces the issue of confidentiality which sits outside the scope of existing privacy legislation. We would want to avoid having potentially confusing and inconsistent privacy frameworks.

Complex and inconsistent consenting regimes: The CDR could create considerable noise around privacy notices and consenting methods such that consumers are put off or confused about how to actually use their rights. A common consent taxonomy along with a programme to address consumer literacy around data and privacy could be used to address this risk. This supports our opening comments around addressing consistent customer experience as part of a CDR regime.

Scope of the consumer data right

Question 4: What would the costs and benefits be of applying the consumer data right to businesses and other entities, in addition to individuals?

One of the key design considerations for a data-sharing regulatory framework is who should be able to direct that data be shared.

The discussion paper notes that 'a CDR should apply equally to any end-user of a product or service. This will mean that individual consumers, as well as businesses and other entities, will receive the benefits of a CDR.'

This issue was also addressed in the Australian Productivity Commission's Report on Data Availability and Use[29] (the PC Data Report) and the Farrell Review.

Small businesses

The PC Data Report had proposed that the broader CDR apply to small businesses. The Farrell Review noted that information asymmetries are particularly acute for small businesses.[30] The Interim Report of the Financial System Inquiry in Australia had stated that "Information asymmetries are the most significant structural factor contributing to the higher cost and lower availability of credit for small-to-medium-sized enterprises (SMEs) and can be a barrier to competition in SME lending.[31]

The Australian experience for small businesses is likely to be relevant in a New Zealand context and suggests that there are potential benefits for small businesses from being included in the scope of entities able to direct that data be shared.

The incremental costs to data holders are unlikely to be significant as the APIs developed for sharing retail customer and transaction data would be similar to those used to share small business customer and transaction data.

Large businesses

If small businesses are able to direct that their data be shared, the exclusion of larger businesses would require the ability to create a clear definition of these businesses. However, as the Farrell Review noted, "there are always difficulties created when policy carves in or carves out, certain groups. Many questions arise such as: which definition of small business should be used (based on employee numbers, or turnover)?; how will the data holder identify whether the business qualifies, especially if there are aggregation rules or 'grandfathering' eligibility through changes in status?"[32]

[29] Productivity Commission (2017)
[30] Farrell Review (2017), page 41
[31] FSI Interim Report, pages 2-62 as noted in Farrell Review (2017), page 41
[32] Farrell Review (2017), page 42

The primary challenges that have been noted in relation to accounts for entities other than individuals include establishing who is authorised to share information and identifying all of the entities and accounts for larger complex groups.

Challenges could also arise where data on a customer is held across multiple product systems. This could result in some customers being able to request data be shared, whereas other customers whose information is recorded on the same system would not be able to request data be shared.

As a result, the risk of attempting to exclude larger businesses would be greater regulatory complexity and additional costs. There is also the risk that this leads to unintended consequences. The ACDR seeks to address some of these challenges by the designation of specific data sets in the designation instrument for a sector. For example, in banking only certain product types are included in the accounts designated as those from which a customer can direct that data be shared.

The inclusion of businesses in the scope of New Zealand's CDR will also result in greater alignment with the ACDR.

Deloitte supports the inclusion of businesses as well as individual consumers in New Zealand's data-sharing regime. A consequence of this will be that considerations of confidentiality will need to be considered when designing the privacy framework supporting data sharing regulation.

Question 5: Do you have any comments on the types of data that we propose be included or excluded from a consumer data right (i.e. 'consumer data' and 'product data')?

Derived data

We support the exclusion of derived data from the definition of consumer data. This protects the IP and assets built by data holders to apply transformation and analytics to enhance value from data.

However, it will also be important that the definition of 'derived data' is not so narrow that it excludes meaningful information, for example, account balances derived from account transactions. The Australian experience suggests that this is best addressed through the designated data sets for a sector.

The discussion paper notes that 'derived data may still be considered 'personal information' for the purposes of the Privacy Act 1993 if it relates to a natural person, and that individuals could therefore request this information under that Act.

The creation of a consistent experience for consumers is an important element of building trust and confidence in data sharing. We believe that this is compromised where consumers can access similar information from an organisation through different regulatory frameworks and should be avoided.

Consideration should be given to including data sets which an individual is entitled to access through other regulatory frameworks in the scope of the data sets designated in a CDR designation instrument.

Reciprocity

An important issue to be considered when designing New Zealand's CDR is reciprocity. This is a topic which was the subject of many points of view during the consultation process for the ACDR legislative framework.

New Zealand, like Australia, is considering the implementation of a sectoral designation based CDR. 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.'[33]

Initially, the ACDR legislation has pragmatically limited 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 the ACDR 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

[33] 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

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 ACDR 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.'[34]

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 whether to share it.

If New Zealand adopts a sectoral designation approach to CDR, it should consider how equivalent data and the principle of reciprocity will be treated in a multi-sector environment.

Product data

The discussion document notes that a CDR should incorporate information about the products or services offered to consumers by a business. This could include information about fees, rates and prices for products and services.

Deloitte supports the inclusion of product data as a data set to be shared under the CDR.

Shared product and pricing information is often used by comparator websites (also referred to as product comparison websites, price comparison websites and PCWs). Based on the CDR product data, these sites can encourage customers to change providers.

In Deloitte's open banking consumer behaviour survey, comparator websites were one of the top three influencers of consumers' switching behaviour.[35] 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 ability for a third party to open an account on behalf of a customer addresses some of the behavioural biases to searching and switching by making comparisons of often complex products easier, and helping consumers in their decision-making process. The inclusion of write access in New Zealand's CDR framework would further enhance the opportunity for PCWs to create value for consumers by initiating and simplifying account opening and switching.

However, the use of CDR product data by PCWs also introduces new risks.

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.

People's willingness to purchase via comparator websites are held back by relationship trust gaps – they don't trust that PCWs have their best interests at heart. A report into PCWs in Australia by the ACCC highlighted a number of concerns about conduct in the industry[36]:

- 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

[34] Australian Retail Credit Association, *Submission on the Treasury Laws Amendment (Consumer Data Right) Bill 2018*, 7 September 2018
[35] Deloitte (October 2019), page 41
[36] A review of comparator websites in Australia by the ACCC highlighted 'a lack of consumer trust in the motivations of, and benefits offered by, comparator websites. Australian Competition and Consumer Commission, *The comparator website industry in Australia*, November 2014, pages 18-29. Refer: https://www.accc.gov.au/system/files/926_Comparator%20website%20industry%20in%20Australia%20report_FA.pdf

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

Some classes of entities which may participate in the CDR regime already have a duty to act in their customer's interest. These include, for example, accountants and financial advisers. However other classes of entities may continue to be remunerated on a commission basis.

In designing New Zealand's CDR, consideration should be given to whether PCWs seeking to use CDR product data should have a duty to act in their customer's best interests.

We do not believe that CDR should also include sharing anonymised market-level data, particularly in its initial implementation. If this information is required, consideration should be given to obtaining this information using New Zealand's official data agency, Stats NZ.

Question 6: What would the costs and benefits be of including both read access and write access in a consumer data right?

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.

Write access however comes with several risks, namely customers abdicating control over their choices to a third party. It is therefore important to define rules for establishing liability when errors occur, or fraud is committed.

There are 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. For example:

- 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 new sectors. For example, 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 is 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. Please refer to the Deloitte publications, *Payment initiation – competing the vision*[37] and *Shaping the Future Consumer Data Right - Deloitte*[38] that further discuss benefits, costs and risks related to read and write access.

[37] Deloitte, *Payment initiation – competing the vision*, December 2019. Refer https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fsi-open-banking-december-2019.pdf

[38] Deloitte (September 2020)

Section 3: What form could a consumer data right take in New Zealand?

What outcomes are being sought

Question 7: Do you have any comments on the outcomes that we are seeking to achieve? Are there any additional outcomes that we should seek to achieve?

The future role and outcomes of a CDR bring significant opportunities for the creation of value for consumers, citizens and society. It 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.

A CDR should have positive consumer welfare and economic development outcomes however these can only be achieved by enhancing or enabling a number of capabilities. 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.

Consumer Welfare

The discussion paper notes a range of consumer welfare outcomes that are expected to result from a data-sharing framework: strengthened privacy rights, innovation, reduced search and switching costs, and facilitating competition.

A core consumer welfare objective of data sharing is to encourage competition and the development of more competitive markets. To achieve this outcome, it is important to understand the role that data sharing can play in addressing how market structure and sources of market failure adversely impact competition.

A focus on the market structure can help determine the priority for sector designation in a sector-based data sharing regulatory framework. In Australia, it is unsurprising that the three sectors initially identified to which the ACDR will be applied – banking, energy and telecommunications – have oligopolistic market structures.

The absence of access to customer transaction data has been seen as creating a barrier to other competitors and new entrants. A data-sharing framework can help to contribute to reducing this barrier, provided the process to become an accredited data recipient does not create a new barrier to entry.

The absence of clear product information increases search costs and makes a comparison of alternative products and services more difficult.

The absence of easily shared product and consumer transaction information makes it difficult for a consumer or a third party on behalf of a consumer, to assess the potential benefits of alternative products and services to that consumer.

A consumer welfare objective to encourage competition and the development of more competitive markets enables a broader focus than just 'increasing access to more affordable products and services.'

Another potential consumer welfare outcome from data sharing is its role in mitigating consumer behavioural biases.

Deloitte's open banking consumer survey highlighted that people's behavioural biases influence whether and how people search for information and make a decision to change provider.[39] Research by Deloitte[40] together with a study on product innovation[41]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 consumer confidence in a decision they have made and can prevent them 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.

The impact of emotion on behaviour: "I worry about failure, and I hate feeling dumb." Consumers are often overcome by the 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 for having chosen poorly.

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. They 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.

All of these factors must be considered to realise the perceived outcomes of innovation and providing access to affordable products and services through increased competition, and reduced search and switching costs.

Consumer welfare outcomes do not explicitly include the creation of a safe framework for data sharing. This is a critical element in creating consumer confidence. Strengthening existing privacy rights is an important element of this. Other elements include the consent process, cyber security requirements, the data transfer mechanism, the accreditation of data recipients and the liability and dispute resolution framework.

Economic Development

The discussion paper correctly identifies that data sharing can contribute to the growth of the digital economy by enabling the development of new and innovative sectors of the economy. It also notes that strengthening existing privacy rights is important.

As we have noted earlier, there are other elements which will be important in building a successful digital economy:

- In addition to strengthening privacy legislation, it will be important that there is an appropriate framework in place for digital platforms and the use of AI, algorithms and machine learning. It will also be important to ensure that existing consumer protection legislation is appropriate for the emerging digital economy.
- Ensuring customer experience criteria are key elements in the design of a data-sharing framework to truly drive consistent user convenience.
- Creating a Digital ID framework to enable people to more easily engage in the digital economy and data sharing.
- Enhancing consumer literacy around data, privacy, the use of digital methods and the associated benefits. This may need to specifically address certain vulnerable cohorts within society.
- Supporting those parts of the community who may somehow be disadvantaged from not being able to or refusing to embrace a digital economy. The recent COVID pandemic has shown that it is indeed possible to reduce this kind of gap considerably.

[39] Deloitte (October 2019), pages 50 and 72
[40] Deloitte University Press, *Frozen: Using behavioural design to overcome decision-making paralysis*, 2016. Refer: https://www2.deloitte.com/us/en/insights/focus/behavioral-economics/overcoming-decision-making-paralysis.html
[41] Gourville, John T., *Eager Sellers Stony Buyers: Understanding the Psychology of New-Product Adoption*, Harvard Business Review, June 2006 pp 98-106. Refer https://hbr.org/2006/06/eager-sellers-and-stony-buyers-understanding-the-psychology-of-new-product-adoption

- New Zealand has an opportunity to design a CDR which is part of an enhanced regulatory framework supporting a digital economy.

Question 8: Do you have any comments on our proposed criteria for assessing options? Are there any additional factors that should be considered?

The criteria for assessing the options must be able to effectively provide a construct to evaluate the options for a CDR which is able to address current issues, realise the perceived benefits and is not cost-prohibitive. The discussion paper outlines five criteria for assessing options for data sharing: Trust, Reach, Speed, Cost and Flexibility.

We broadly agree but we provide some commentary on these criteria below.

Trust is necessary for data sharing to be successful. 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. We believe trust is one of the most important assessment criteria.

The Issues Paper for the Australian Treasury's Inquiry into Future Direction for the Consumer Data Right[42] highlights that by establishing systems which support trust between participants, together with a framework that introduces standardisation, clear liability and providing access to the data necessary to create innovative products and services, the ACDR has the potential to create the conditions for an Australian digitised ecosystem to grow. The UK Competition and Markets Authority (CMA) has also highlighted that the benefits for consumers from providing their data will only be realised if consumers can trust the firms that collect and use it.

Trust also supports the speed with which data sharing becomes widespread through the economy.

One of the key outcomes of a CDR is economic development, and its success in achieving this will be dependent on the **reach** across the economy including sectors and markets. The broader the reach of the data-sharing framework, the more it is able to support the emergence of a digital and open data-enabled economy.

Speed of implementation and adoption is important if consumers are to realise the benefits of data sharing. However, speed is potentially an outcome of other factors. Some of these relate to the consumer experience, for example, the level of consumer's trust in the data-sharing framework; the consistency of the consumer experience with data sharing across sectors; the level of consumer education about the data-sharing framework and the potential benefits available the investment in consumer financial and data literacy.

Others relate to the regulatory framework for data sharing, for example, the customer experience and API standards adopted; the accreditation process for data recipients; the sector assessment and designation process; the capability and funding of the regulator(s) responsible for data sharing.

As a result, it is not clear that speed should be a criterion that is used to assess the options for establishing a CDR.

We support the objective of the discussion paper that the **cost** of a regulatory framework for data sharing should not outweigh the benefits. However, it is not clear that cost alone or cost minimisation should be criteria that are used to assess the options for establishing a 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 the 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?

[42] Australian Government, The Treasury, *Inquiry into Future Directions for the Consumer Data Right: Issues Paper*, March 2020. Refer: https://treasury.gov.au/sites/default/files/2020-03/200305_issues_paper.pdf

Flexibility will be important as a one size fits all approach will not be possible. Different sectors have different market structures, conditions and regulatory frameworks. In addition, flexibility allows extensibility, the capacity of a system to be adapted for different purposes.[43] Extensibility provides the option of a staged approach to implementation. For example, sectors to be designated for data sharing at different times, different levels of accreditation to be introduced, and phased implementation of functionality, such as write access.

However, flexibility has the potential to reduce consistency in the consumer's data sharing experience and as a result, the understanding and confidence in data sharing. If a sectoral-designation approach to data sharing is adopted with requirements tailored to a specific sector to enhance flexibility, it will be important that any assessment of costs and benefits for a sector includes the adverse impact on consumer trust and understanding of having wide variations in how data sharing is applied to each sector.

In the spirit of consumer focus, differences in the Rules and Standards applied to different sectors should be minimised to enhance consumer understanding, and ultimately usage, of data sharing.

Other factors that could be considered when assessing data sharing options are outlined below:

Ability to advance the digital economy – How well the option supports the emerging digital economy and the creation of a data ecosystem. This could include, for example, the ease with which data can be shared with participants operating in different sectors, through consistent rules and standards, minimisation of sector-specific rules and standards, and the ability to support other elements of the digital economy, such as digital ID.

Consumer focused – How the option contributes to benefits for consumers. This includes its comprehensibility by consumers, its ease of use by consumers, the inclusion of standards focused on consumer experience, its ability to generate consumer trust. This also includes the consistency of the data sharing mechanisms within the data sharing frameworks and with other data sharing mechanisms operating in the economy.

Consumer reach – How the option provides an opportunity to best reach and benefit the entire population. A digital economy needs to have the widest possible consumer reach to be most effective and not leave out or disadvantage certain cohorts within society.

Regulatory capability – What skill sets will be required to ensure that the regulator of the data-sharing framework can effectively, where relevant, assess the benefits to sectors, accredit third parties as data recipients, monitor ongoing compliance with the regulatory framework and take enforcement action for breaches.

Interoperability – How easily New Zealand's data sharing regulatory framework allows New Zealand companies to compete overseas, and entities operating in jurisdictions with similar data-sharing regulatory frameworks to operate in New Zealand.

Value – The option should be assessed for its ability to create and generate the most value from a consumer and economic benefit perspective. Consumers should be able to extract the value from their data through the increased sharing of it and the use of new products and services. The digital economy should be enabled such that it can generate value and grow markets.

Innovation – How the option provides the best opportunity for innovation including identifying global market opportunities through innovation. There may be further opportunities for certain sectors to offer new products and services to global consumers in jurisdictions where similar CDR regimes already exist or are imminent. Regulations in NZ may drive the development of readiness capability across such sectors.

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 New Zealand's data literacy similar to the challenge Australia faced is likely to be as important, if not more important than improving financial literacy for New Zealanders to realise the outcomes 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. However, in New Zealand similar to Australia, 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.

[43] Farrell Review (2017), page 83

In creating the future open data economy there are areas that could be enhanced in New Zealand as was required in Australia. These include:

- Consistency of user experience of the collection, use and storage of data by organisations to complement the consistent experience of data sharing that CDR enables.
- 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 other organisations.
- Developing consumers' financial literacy so that people are able to understand the potential benefits of participating in an open data economy.
- 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.

Options to establish a consumer data right

Question 9: Do you have any comments on the discussion of Option One: Status quo?

Option One stipulates that data portability remains unregulated in New Zealand. Unless there is a compelling benefit to the data holder it may tend to prioritise other issues and the consumer benefits of data sharing may not be realised at the same pace.

Jurisdictions are adopting their own approaches to open banking, reflecting their markets and policy objectives. The variations across 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.[44]

A number of countries, including India, Japan, Singapore, and South Korea, do not currently have formal or compulsory Open Banking regimes, but their policy makers are introducing a range of measures to promote and accelerate the take-up of data sharing frameworks in banking. 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 FinTech organisations. In Japan, the FSA has established an authorisation process for Third Party Providers (TPPs), introduced an obligation for banks to publish their Open APIs policies, and encouraged banks to contract with at least one TPP by 2020. The majority of Japanese banks are taking this regulatory encouragement very seriously and are on track to fulfil the deadline.

The US has also opted for a market-led approach, but without any material government initiatives to support the development of Open Banking products and services. A recent US Treasury report 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. The major US banks are well aware of the strategic importance of Open Banking and 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. This is costly and inefficient for TPPs, but also difficult for banks which remain solely responsible and liable towards their customers, including when TPPs use screen scraping without the bank's knowledge by accessing the account with the customer's bank credentials. We note that screen scraping typically gives a TPP access to much more customer data than is often required to deliver the service the customer wants, increasing the risk for both the customer and the bank.

With regards to the role of data protection regulations, some jurisdictions, including the US, have been largely silent on whether they are planning to review their data protection regimes in light of the expected increase in data sharing due to Open Banking. This is particularly worrying as the use of screen scraping, which as we mentioned remains wide spread, does not give customers any real control over which data they are sharing, nor does it establish a clear liability framework in case of

[44] Deloitte, *Open Banking around the World*, 2018. Refer: https://www2.deloitte.com/global/en/pages/financial-services/articles/openbanking-around-the-world.html

data breaches or fraud. In the EU for example, while PSD2 technically does allow screen scraping[45] the conflict with GDPR requirements is clearly steering banks towards the development of API communication solutions.

We acknowledge that there may be ways other than the introduction of a new data-sharing regulatory framework to achieve some of the desired outcomes of a CDR. For example, sector-specific data sharing arrangements; reducing interchange rates for card payment schemes through regulation (as has been implemented in Australia); increasing privacy requirements for data holders; and other options to reduce switching costs and enhance product comparisons.

The primary benefit of a status quo approach is that New Zealand businesses do not need to incur a new cost to implement a regulated data-sharing framework. This consideration may be relevant as businesses seek to respond to the impact of COVID-19 on the economy.

However, overall, we concur that Option One is likely the slowest way to realise the full consumer benefits of a CDR and least likely to enhance New Zealand's readiness to participate in a digital economy.

Question 10: Do you have any comments on the discussion of Option Two: A sectoral-designation process?

Outside the EU, two major jurisdictions have opted for a regulatory-driven approach as envisaged in Option Two – Hong Kong and Australia – although a number of countries are now considering this approach.

The Hong Kong Monetary Authority (HKMA) 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, and ending with sharing of transactional information and payments initiation services. 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.

But it is Australia that stands out for its innovative approach and scale of ambition. It is, arguably, currently unique in its design as an economy-wide data sharing policy initiative.

Like other Open Banking initiatives, the ACDR will allow consumers to share their data with whichever accredited third parties they choose. The key difference, however, is that the ACDR is a data policy initiative and not a financial services one. While it will apply to banks first, the CDR will subsequently apply to the energy and telecommunication sectors as well, and eventually, it could be applied to any sector.

The ACDR is also the first data sharing legislation to introduce the concept of 'reciprocity'. Currently, the ACDR 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 ACDR from one sector (such as banking) to any other sector from which a non-traditional competitor emerged.

However, under Option Two, 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.

As a result, it will be important for a CDR based on Option Two to consider the treatment of equivalent data and the principle of reciprocity.

It is notable that the review of the 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.[46] Option Two is a logical approach to CDR implementation and would allow for sector working-groups to create the necessary structures and standards to make a CDR successful for that sector. Another benefit of this approach is that the overall cost of implementing a CDR is spread over time, giving follow on sectors time to learn and adapt. In addition, different sectors are likely to have higher or lower requirements of security, which could be accommodated by Option Two.

However, under Option Two, too much variation in the detailed rules designed and applied to each sector will reduce consistency which has the potential to have an adverse impact on consumer confidence, understanding and use of data

[45] Deloitte (2018)

[46] Open Data Institute, *The Open Banking Standard*, July 2019. Refer: http://theodi.org/wp-content/uploads/2020/03/298569302-The-Open-Banking-Standard-1.pdf

sharing. As the emerging digital economy contributes to the blurring of industry boundaries, particularly with the emergence of platform-based business models, Option Two could result in inconsistent data sharing frameworks for competing organisations, which has the risk of introducing new barriers to entry.

Further, if the CDR focused only on the regulation of data sharing, it can result in inconsistent consumer consents for data which is shared compared to the those required for the initial collection and use of data.

Another risk of Option Two is that the benefits of a CDR are realised over a longer period of time unless there is a rapid process for assessing and designating sectors.

Question 11: Do you have any comments on the discussion of Option Three: An economy-wide consumer data right?

As the discussion paper notes, the EU's GDPR establishes economy-wide data rights and sets our rules for the protection and processing of personal data. With its strong focus on privacy, the EU's GDPR has been seen, across the world, to set a new gold standard for data protection. In contrast, while the ACDR is an economy-wide reform, it will only apply to sectors which have been designated.

GDPR was implemented at the same time as the EU's PSD2 which introduced elements of write access to the EU. In hindsight, it is clear that while the two policies share similar objectives in terms of data security and portability, the details were developed in silos and have been difficult to reconcile in practice[47].

By implementing an economy-wide data right that applies to all sectors Option Three would provide a broader and more consistent customer experience of data-sharing. It establishes rights for consumers when data is initially collected as well as when it is shared.

Adopting this approach for New Zealand would also avoid needing to establish a new regulatory framework, and potentially a new regulator.

However, with its focus on privacy, the GDPR does not have a clear objective on enhancing competition and encouraging innovation. Implementing an economy-wide approach is likely to be difficult to manage and would be disruptive to multiple sectors. There is also a risk that the complexity, cost and time commitment to realise the benefits of an economy-wide CDR would outweigh the benefits sought. Considerable analysis and changes will be required to align current regulations, including those within each sector. For example, NZ's current Privacy laws do not sufficiently address data portability rules to allow consumers better tools to move their data.

An economy-wide data right would also require enhancement of NZ's cyber security standards and accreditation framework so that there are fit for purpose and consistent ways for all data holders to demonstrate compliance with a minimum set of expectations.

Question 12: Do you have any comments on the discussion of Option Four: Sector-specific approach?

Option Four could be described as a hybrid of a market-based approach and the sector-specific approach of Option Two.

A sector-specific approach of Option Four would more likely result in deeper sector-specific rules and standards without an overarching framework. This is likely to have an adverse impact on consumer understanding of and confidence in data sharing. For example, a range of different consent experiences could compromise the extent to which a consumer understands and is able to manage the consents they have provided.

It would also be less likely to be able to support cross-industry data sharing, which could limit potential innovations and the potential for new competitors from outside a sector.

Like Option Two, if a sector-specific CDR focused only on regulations for data sharing, consumers may continue to have a different consent experience, or none at all, when they initially provide data to organisations.

[47] Deloitte, *PSD2 and GDPR - friends or foes?*, August 2017. Refer: https://blogs.deloitte.co.uk/financialservices/2017/08/psd2-and-gdpr-friends-or-foes.html

In Option Four the lack of consistency that may arise from a sector-specific approach could result in loopholes whereby new innovative services that overlap multiple sectors may circumvent the key benefits sought by a CDR regime. To address this New Zealand would need to establish principles based overarching criteria to avoid unexpected interpretations of the regulations. This may be a lighter version of the overarching legislative framework in Option Two.

Further, New Zealand would need to strengthen certain areas of legislation which are cornerstones for protecting consumer rights, such as privacy legislation to consider 'Data Portability'.

Question 13: This discussion document outlines four possible options to establish a consumer data right in New Zealand. Are there any other viable options?

In New Zealand, the government has already started initiatives to enable New Zealand to become a thriving digital nation where its people, businesses and government are all using technology to drive innovation, improve productivity, and enhance the quality of life. As part of this, the government has conducted research on the digital economy and digital inclusion to assist them with the decision-making.

In Australia, although ACDR has only just commenced, recent reviews have highlighted the need to enhance a range of legislation so that the regulatory framework better supports the digital economy and data sharing under the ACDR.

Changes to the Australian Privacy Act were recommended by the ACCC 'in order to ensure consumers are adequately informed, empowered and protected, as to how their data is being used and collected.'[48] 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.

Changes to the Australian Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) and AML/CTF Rules (2007) (AML/CTF Rules) have been made to allow the sharing of information about the outcomes of identity verification.

The extension of data rights to include data on individuals held by government agencies was noted in the PC Data Report[49] and the extension of the ACDR to include this data was explicitly recommended in submissions on the draft CDR legislation.[50]

Based on Australia's experience, New Zealand could consider supplementing Option Two by incorporating elements of Option Three including strengthening New Zealand's Privacy legislation, to ensure consumers are adequately informed, empowered and protected, as to how their data is being used and collected in addition to when it is shared under CDR. This has the additional advantage of increasing international harmonisation of legislation on data rights including data sharing.

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.[51]

Question 14: Do you have any comments on our initial analysis of the four options against our assessment criteria?

The initial analysis of the four options is, by its nature, only a high-level assessment.

One of the key challenges is understanding the costs and benefits of each option. The analysis set out in the discussion paper doesn't capture the different burdens of implementation costs on private and public sectors and where the greatest benefits consumers lie. For example, under Option Two, costs are borne largely by private institutions but benefit the economy in aggregate. As a result, it is not clear that the indicative analysis set out in the table for 'Cost' is accurate.

We have noted in our response to Question 8 a range of other criteria against which the options could be assessed. These include the ability of an option to advance the digital economy, the extent to which the option is consumer-focused and

[48] ACCC (June 2019), page 3
[49] Productivity Commission (2017), Finding 3.1, page 33
[50] Business Council of Australia, *Submission: Response to the Treasury Laws Amendment (Consumer Data Right) Bill 2018, September 2018*, page 3. Refer: https://d3n8a8pro7vhmx.cloudfront.net/bca/pages/4360/attachments/original/1538111090/Response-to-draft-legislation-for-the-Consumer-Data-Right.pdf?1538111090
[51] Deloitte (2018)

inclusive, the impacting of enforcing the regulatory framework chosen, its international interoperability, the ability of the option to generate value for society and consumers, and the extent to which the option promotes innovation.

Further analysis at a sector level, including informed research involving consumers and the competitive landscape, is required to understand where the greatest benefit lies for consumers. This type of analysis would be necessary to understand where government intervention is best applied.

Question 15: Do you agree or disagree with our assessment that Option Two is most likely to achieve the best outcome using the assessment criteria?

Option Two enables those entities subjected to the implementation costs to be the most likely beneficiary from the enhanced efficiencies of a CDR regime. It provides enhanced privacy safeguards and an overarching legislative framework that would be flexible enough to introduce other sectors at a later stage if the benefits for businesses and consumers can be proven.

It further could minimise the likelihood of data breaches and therefore the need for enforcement by initially applying the CDR regime to sectors that are already heavily regulated, such as financial services, and which already have a good understanding of their privacy obligations to protect personal information.

As such, based on the criteria presented it comes across as the most attractive option amongst the four outlined in the discussion document.

As noted in our response to Question 13 New Zealand could consider supplementing Option Two by incorporating elements of Option Three including strengthening New Zealand's Privacy legislation, to ensure consumers are adequately informed, empowered and protected, as to how their data is being used and collected in addition to when it is shared under CDR. This has the additional advantage of increasing international harmonisation of legislation on data rights including data sharing.

Section 4: How could a consumer data right be designed?

Question 16: Do you agree with the key elements of a data portability regime as outlined in this section? Are there any elements that should be changed, added or removed?

The discussion paper outlines six potential design considerations for a sectoral designation approach to a CDR: the designation process, the scope of a designation, the rules and data standards which would form part of the broader legislative framework for a CDR, the accreditation regime, privacy safeguards, and the liability, enforcement and redress process.

The design considerations do not include the regulator model. Comments on this are included in our response to Question 25.

Question 17: Do you have any feedback on our discussion of any of these key elements?

- Designation process: Determining the regulatory impact of designating a sector is important as one of the challenges of building a framework for a digital economy is that the regulatory responsibility is spread across several different regulatory agencies and government departments. This was acknowledged in the Australian Government's Explanatory Memorandum to the ACDR 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.'[52] 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.[53]
- Scope of a designation: We appreciate that making additional data shareable carries both additional opportunity and additional risk. Therefore, in working out what data could be within scope for a specific sector, the focus should be maintained on what benefits it could deliver to consumers if it was in scope, and what risks would arise that then need to be managed.
- Rules and data standards: As a design principle, New Zealand should seek to align New Zealand's regulations with international standards unless there is a strong rationale to do otherwise. As write access or transaction initiation becomes part of the CDR standards, it will be important that the Digital Identity Trust Framework is fully developed and ready to be implemented. To support this, an identity assurance framework should be developed along the lines of the Digital Identity Trust Framework (DITF) which is being progressed by the New Zealand Government. As data types and transactions are defined in CDR, the appropriate level of assurance should be mapped to this data in the standards.
- Accreditation regime: Finding the balance between trust and delivery of value means that any accreditation criteria for a CDR needs to be stringent enough to create trust, but not so stringent that they drive out new entrants or innovation which deliver value to consumers. As new sectors become designated under the CDR, regulators and standards bodies will need to have sufficient capability and capacity to meet the demand in a timely manner. A tiered accreditation approach could be adopted which would allow participants to receive CDR data commensurate with their level of maturity or the risks of the data set being shared. 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.

[52] Australian Government, The Treasury, *Exposure Draft Explanatory Materials*, 2018, paragraph 1.34, page 10, as noted in https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/au-fsi-deloitte-open-banking-customer-data-170620.pdf
[53] Deloitte Access Economics, Shaping the Future: Deloitte submission to the Interim Report of the Financial System Inquiry, 26 August 2014

The design of New Zealand's CDR will also need to consider the operating model for accreditation and which entity should be responsible for accreditation. Australia initially included this (the Registration Accreditation Process (RAP)) as one of the responsibilities of the ACCC. However, this is subject to review given the recommendations of the Interim Report of the Senate Select Committee on Financial Technology and Regulatory Technology, and the current Inquiry into Future Directions for the Consumer Data Right. We have included further comments on the regulatory model in our response to Question 25.

- Privacy safeguards: In the process of designating sectors 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 that offer products and services requiring the collection of sensitive personal information, for example, health information. In addition, the inclusion in CDR data of information about the location and time of a transaction creates a higher risk profile from a data privacy perspective. The inclusion of this information would need to be permitted or constrained by the consumer at the time they provide consent.
- Liability, enforcement and redress: The CDR rules and regulations should 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 should be backed by penalties for breaches that are meaningful, even for large institutions.

We note the following additional elements for consideration:

- Foreign consumers: Application of CDR to businesses and consumers outside NZ who operate in jurisdictions with similar frameworks for data and privacy could prove to be advantageous to the New Zealand economy. The regulatory change programme to accommodate the CDR should consider this aspect, including the protection of consumer rights when data is processed in foreign locations.
- Reciprocity: 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.'[54]

  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.
- Customer experience: When designing the CDR rules and regulation, the government should consider the risks associated with sharing customer data with third parties. This could include specification of customer experience requirements in addition to just customer consent standards.

  Case Study – The UK's Open Banking Customer Experience Guidelines states the following:

  Customers will only use Open Banking services if they feel informed, secure and in control. These guidelines address the processes a customer follows within an Open Banking enabled app or web service. They balance regulatory requirements and customer insights to optimise consumer satisfaction. Customers will only use Open Banking products and services if their experience matches or betters their expectations, and information is presented in an intuitive manner that allows them to make informed decisions. It is therefore important that the interplay between the data recipients and the data controllers is as seamless as is possible while providing customer control in a secure environment. In particular, it is essential that customers are clearly informed about the consent they are providing and the service they are receiving.

  The Customer Experience Guidelines form part of the UK Open Banking Standard Implementation Requirements. The European Banking Authority's (EBA) Draft Guidelines on the contingency mechanism exemption conditions state in Guideline 6 "where an Account Servicing Payment Service Provider (ASPSP) is implementing a market initiative standard, it should provide to its competent authority information as to which standard it is implementing and whether, and if so how, it has deviated from any standard implementation requirements of the initiative".

[54] IIF (July 2018), pp 2-3

The UK Open Banking Implementation Entity (OBIE) is therefore developing a range of Standard Implementation Requirements. The Customer Experience Guidelines and Checklist form part of the Standard Implementation Requirements and set out the customer experience required to deliver a successful Open Banking ecosystem, alongside technical, performance, non-functional requirements and dispute resolution practices.[55]

Question 18: Are there any areas where you think that more detail should be included in primary legislation?

The following matters could include additional detail either in the primary legislation or supporting rules and standards:

Rules and data standards that should be elucidated:

- Rules should differ where required for each designated sector, for determining the rights and obligations of participants under the CDR. This is mainly because each sector will have different data set inclusions and different impacts on the consumers. However, this should be minimised to assist consumer understanding and to enhance the consumer experience.
- The Office of the Privacy Commissioner (OPC) should consider the interaction of CDR with existing industry codes and the development of new Codes of Practice specific to the additional sectors. For example, the existing Superannuation Schemes Unique Identifier Code 1995, Telecommunications Information Privacy Code 2003 and Health Information Privacy Code 1994.

Accreditation regime detail:

Deloitte has done some research on other similar accreditation regimes across the globe and has views on the design of the accreditation process in New Zealand.

- NZ could consider the EU accreditation model: eIDAS Qualified certificates (EU Regulation 910/2014),[56] which is a set of EU regulatory standards that define requirements for digital certificates, validation of their holders' identities, and the operation of the Qualified Trust Service Providers (QTSPs) that issue them. Certificates issued by QTSPs in accordance with eIDAS standards are known as "Qualified Certificates," and provide special status in certain legal and regulatory contexts across the EU.
- The concept of a public national register could also be considered. Under the EU's PSD2, a national register needs to be managed and maintained by each National Competent Authority (NCA) and made publicly available (accessible online). Whilst this is already the case in the EU today, the registers will almost certainly have to be further enhanced. This could mean a body such as the Financial Markets Authority (FMA) maintains this register and anyone including users, data providers and other recipients could verify the legitimacy of an accredited data recipient.
- Data recipients could be issued digital certificates based on their risk score level when assessed by New Zealand's equivalent of QTSPs. For example, Data Recipient A would be issued a digital certificate that allows them to receive product data and consumer data, or have both read and write access due to their compliance with security and privacy standards. However, an accredited Data Recipient B might be eligible for a digital certificate that only gives them access to product data, or only read access.
- Accreditation should be time-bound. This would mean that the data recipients would potentially renew their certificate annually.
- Lower level accreditation (intermediaries) could be considered, where one accredited intermediary collects and holds all consumer data that can be accessed by TPPs, but none of the TPPs will be able to store it.

[55] Open Banking Limited. *Open Banking Customer Experience Guidelines*, version 1.0, 12 September 2018. Refer https://www.openbanking.org.uk/wp-content/uploads/Customer-Experience-Guidelines.pdf

[56] DigiCert + QuoVadis. *What you need to know about PSD2 certificate compliance*, 2019. Refer https://www.digicert.com/wp-content/uploads/2019/06/DigiCert_PSD2_FAQ_6_11_19.pdf

Privacy Safeguards

- If New Zealand adopts a multi regulator model, the OPC should have a principal role in advising on and enforcing privacy protections in the CDR framework.
- While banks have typically had strong privacy and information security standards, as CDR is applied to other organisations and sectors, support regimes (in addition to a fit for purpose accreditation framework) may need to be established to assist in improving their privacy and information security maturity.
- The government should consider taking a Privacy by Design (PbD) approach to the CDR, performing Privacy Impact Assessments (PIAs) for CDR on all stages of its development, as has been undertaken in Australia.[57] This should include a detailed analysis of threats involved with the implementation of the CDR and mitigation strategies to support better management of those threats. This should be overseen by the OPC.

Liability, enforcement and redress

- The key principle to establish the CDR involves governance of consumer 'data', therefore, it is highly likely that most issues with its implementation and use will relate to data portability or data breaches. Hence, in line with the upcoming Privacy Act 2020, the OPC could be the primary point of contact for consumers, businesses and TPPs if CDR complaints relate to a data breach or data portability issues. Considering various elements of the primary legislation or supporting rules and standards, and designated sector-specific rules, it is likely that several issues may occur when establishing the CDR in addition to data breaches. It is recommended that complaint handling processes should be put in place and guidance should be given to the data holders, data recipients and consumers. This will enable the handling of various types of issues related to the course of activities regulated by other agencies (for example, consumer credit providers or financial services), other sector-specific regulators may be best placed to respond to a given concern. The only caveat is that this is only relevant if a multi-regulator model is adopted.
- Remedies available via regulators when data holders or recipients have breached the CDR rules should include infringement notices, civil penalties, compensation orders, enforceable undertakings and the de-accreditation of data recipients (or suspensions or imposition of conditions), depending on the circumstances. Injunctions (court orders compelling an entity to do or refrain from doing specified activities) should also be available, including orders for the deletion of data.
- An example of principles-based legislation is the Standards of Conduct (SLC 25C) for the UK energy sector. These standards outline the high-level behaviours that energy companies must have. It is agnostic of the process i.e. billing, complaints etc. The provider must ensure that each customer is treated fairly with the following guidance:

  - Behaviour towards consumers

  - Providing customers with information

  - Customer service processes

  - Considering vulnerable domestic consumers[58]

[57] The Australian Government, The Treasury, *Privacy Impact Assessment- Consumer Data Right*, March 2019. Refer https://treasury.gov.au/sites/default/files/2019-03/p2019-t361555-pia-final.pdf

[58] Ofgem, *Licence guide: Standards of Conduct*, 21 February 2019. Refer https://www.ofgem.gov.uk/system/files/docs/2019/02/licence_guide_standards_of_conduct_0.pdf

Question 19: How could a consumer data right be designed to protect the interests of vulnerable consumers?

Consumer protection is an important element in building consumer confidence in data sharing. Several submissions to the current Australian inquiry into their CDR argued for consumer protection to be at the centre of the CDR regime.[59]

It is important to ensure that consumer protection obligations, particularly with respect to vulnerable customers, apply to all CDR participants in a designated sector, and not just to the regulated entities in a sector.

Consumer protection is particularly important for vulnerable customers. In addition to the more traditional definition of vulnerable customers, which includes children, asylum seekers, the elderly, and people with physical and mental disabilities, a CDR should make provision for situations where there is a risk of imbalance in the relationship between the data subject and the service provider/controller, similar to the provisions of the GDPR.[60]

Identity validation: Data-sharing can be of significant benefit to many vulnerable people by providing easy access to more cost-effective options and facilitating switching. However, for some, the accidental or malicious exposure of their information as a result of data sharing could place them and their whānau at serious risk, which would deter participation. For many, the perceived or real risk could be exacerbated due to the sharing of computers, mobile phones, and email accounts, which amongst others are driven by affordability challenges, lack of digital literacy and technology aversion in some communities.

Enabling the CDR design for digital identity services and requiring easy to use identity assertions (e.g. grid cards), that do not require devices such as smartphones, will help to mitigate against associated risks, and support an inclusive strategy to promote uptake and participation by vulnerable people and communities.

Consumer education: Data sharing will inspire consumers' confidence if they have an understanding of:

- Their rights and responsibilities
- The value of their data; and
- The risks in the system and the safeguards to minimise those risks.[61]

Consumer education has an important role in building consumers' confidence and awareness, particularly for vulnerable consumers. This will be particularly important in helping consumers understand the consent process so that they provide explicit, fully informed consent and are able to easily revoke that consent.

Consent design: In designing a CDR it will be of great importance to make customers' data rights and permissions very clear and easy to understand. For this legislation to achieve its objectives, it has to be clear and easy for a customer to understand what data is, and is not, transferred and collected by companies. The use of plain English language and easily understood consent notices will be essential.

Consistent consent taxonomy: The adoption of an economy-wide model for consent, and a consistent consent taxonomy could also serve to empower vulnerable consumers by building consistent safeguards and facilitate participation through a 'learn-by-doing' approach. This said, the responsibility for ensuring that consumers are informed and capable, and that consent is explicit should be with the organisation that is seeking consent and the legislative consent framework in which those organisations operate.

Other steps to protect the interests of vulnerable consumers could include:

- Adopting a risk-based impact assessment similar to that included in the GDPR, to inform and support the regulation of CDR processing for vulnerable people and groups, with consideration of the risk of potential harm to such consumers.
- Developing standards and guidelines to define the minimum requirements to support vulnerable customers in a consistent manner, e.g. define additional steps to identify whether the consumer is adequately capable, informed and understands what they are agreeing to and the associated implications and risks.

---

[59] Business Council of Australia, *Submission: Response to the Treasury Laws Amendment (Consumer Data Right) Bill 2018*, September 2018, page 3. Refer: https://d3n8a8pro7vhmx.cloudfront.net/bca/pages/4360/attachments/original/1538111090/Response-to-draft-legislation-for-the-Consumer-Data-Right.pdf?1538111090.pdf

[60] Information Commissioner's Office (UK), *Data Protection Impact Assessments (DPIAs)*, version 1.0.77, 22 March 2018, page 4. Refer: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when11

[61] Farrell Review (2017), page 100

- Implement an economy-wide data ethics framework that provides for the challenges related to vulnerable people and communities, leveraging other data ethics work.[62] [63]

The introduction of a CDR in New Zealand provides an opportunity to undertake an economy-wide reform and modernise the consumer protection frameworks to ensure they consider the impact that a CDR can have on whether and how customers are identified as vulnerable.

[62] Data.Govt.NZ, *Government algorithm transparency and accountability*. Refer: https://data.govt.nz/use-data/data-ethics/government-algorithm-transparency-and-accountability/ accessed October 2020

[63] Data.Govt.NZ., *Discussion paper: International data ethics frameworks*, 7 June 2020. Refer: https://www.data.govt.nz/about/government-chief-data-steward-gcds/data-ethics-advisory-group/reports-commissioned-by-the-group/discussion-paper-2/

Further design considerations

Question 20: Do you have any suggestions for considering how Te Tiriti o Waitangi should shape the introduction of a consumer data right in New Zealand?

The discussion paper notes that the interaction of a CDR with Māori data sovereignty is an important consideration when implementing CDR in New Zealand and needs to be treated in line with the spirit and obligations of Te Tiriti o Waitangi.[64]

Māori Data (data generated by Māori or by others about Māori, including data about Māori resources) is collectively owned by whānau, hapū, iwi and Māori organisations. No one individual can own Māori data, and no non-Māori individual or group can own Māori data.[65]

There are many issues that will require careful consideration and consultation with Māori to shape the CDR that delivers in a meaningful way on Te Tiriti. For example, due to the aforementioned, a Māori consumer may not be in a position to decide on their own whether their information may be shared. Also, many iwis are now corporate entities that could decide to participate in the CDR but may not be able to share information due to the inherent complexities of Māori Data. Furthermore, the requirements in terms of Māori Data Sovereignty will have to be appropriately addressed if the CDR results in a requirement to share Māori Data outside of New Zealand.

The introduction of a CDR in New Zealand will be against an unfortunate backdrop of some data-led initiatives that are seen to have failed Māori and, in some instances, discriminated against Māori.[66] It is therefore realistic to expect that the introduction of a consumer data right will be met with a degree of scepticism and distrust by Māori communities. As such, getting the CDR right in respect to Te Tiriti, and observing its principles of partnership, participation and protection will be fundamental for a truly successful consumer data right in New Zealand.

Appropriate Māori inclusion and representation: The CDR design team and regulating body should include appropriate representation and authoritative subject matter experts on all relevant aspects of Māori Data governance. Consideration of Māori Data-by-design can avoid oversight, costly rework and help to facilitate implementation and consumer participation e.g. an accreditation and regulation regime that is appropriate for Māori Data requirements. Māori inclusion and representation in the design and implementation of the CDR can facilitate economic participation and benefit to Māori.

Data ethics framework: AI, algorithms and data analytics holds significant potential to augment CDR-enabled offerings and to optimise consumer campaigns. However, these methods are giving rise to new ethical dilemmas, particularly in relation to considerations of privacy, fairness and algorithmic bias.[67] While the Government Chief Data Steward (GCDS) made some progress in this regard via the Data Ethics Advisory Group (DEAG), a single and inclusive framework for AI, algorithms and analytics is not yet available. However, a more prescriptive approach holds benefits for the CDR e.g. de-risking the CDR for consumers and help to future proof the CDR, in line with the direction of geographies such as the EU and Australia. An opportunity, therefore, exists for the CDR to lead the way through close collaboration with the DEAG to include a data ethics compliance framework as part of the CDR accreditation regime.

Accreditation regime to provide for Māori Data: The accreditation regime for all entities/agencies wishing to participate in the CDR should require independent validation of sufficient measures to ensure governance over, and sovereignty of Māori Data, by default. This will serve strategic objectives for the CDR to be an inclusive regime for the benefit of all New Zealanders and benefit the broader digital economy through equivalent participation by Māori.

[64] Taiuru, Karaitiana N, *Why Data is a Taonga: A customary Māori perspective*, November 2018. Refer: https://www.taiuru.maori.nz/wp-content/uploads/Data-is-a-taonga.pdf
[65] Taiuru, Karaitiana N, *Māori Data Sovereignty and Digital Colonisation*, September 2020. Refer: https://www.taiuru.maori.nz/maori-data-sovereignty-and-digital-colonisation/
[66] Taiuru (2020)
[67] Deloitte Insights, *The rise of data and AI ethics*, 24 June 2019. Refer: https://www2.deloitte.com/us/en/insights/industry/public-sector/government-trends/2020/government-data-ai-ethics.html

Question 21: How could a consumer data right be designed to ensure that the needs of disabled people or those with accessibility issues are met?

People with a disability can be challenged to change their providers of goods and services due to a variety of factors including physical, mental, technology and logistical issues. The CDR, therefore, holds significant potential to enfranchise many such people by enabling access to new market offerings and facilitate switching.

Mandate accessibility in the CDR: The core building blocks to help realise the benefits of the CDR for people with disabilities are already in place, e.g. CGA, FTA and CCCFA, Health and Disability Commissioner Act[68], the DIA's Web Accessibility Standard[69] and international standards and good practice guidance on mobile accessibility.[70] During the design and standard-setting process, the CDR should focus on leverage existing instruments to mandate compliance with accessibility regulation and standards for participating entities.

Develop guidance for participating agencies: The CDR could leverage the intuitive principles of the Web Content Accessibility Guidelines (WCAG)[71], i.e. Perceivable, Operable, Understandable and Robust, to develop specific guidance for participating agencies, which will be especially useful during initial implementation.

De-risk the CDR for consumers with disabilities: The CDR can draw from the risk-based assessment approach adopted by international regulation such as the ACDR and the EU GDPR, with a focus to de-risk data sharing for more vulnerable consumers and those with disabilities.

Make CDR processes accessible: Specific focus should be given to accessibility during design and standard-setting stages to ensure that the CDR processes, particularly for granting and revoking consent, include consideration of how it is experienced by different groups of people with a disability. For example, CDR-enabled offerings should provide for situations where an authorised person/agent/carer is required to consent or execute on behalf of a person.

Accessibility of help and advice on CDR-related issues: The operating model of the regulator should establish a channel that provides ready access to help, support with complaints handling, and CDR-related resources designed for the communication and accessibility requirements of consumers with disabilities.

Question 22: To what extent should we be considering compatibility with overseas jurisdictions at this stage in the development of a consumer data right in New Zealand?

As a design principle, New Zealand should aim to align its CDR regulations with international standards unless there is a strong rationale to do otherwise. This will enable greater participation of international organisations and maximum economic impact as well as help future proof the CDR. The starting point for greater harmonisation of cross-border data sharing frameworks is greater harmonisation of legislation on data rights, including data sharing.

One of the issues for New Zealand to consider is whether its CDR will only introduce rights for data sharing or whether, either through the CDR or through changes to privacy legislation, New Zealand will also give consumers data rights over their data (not just personal information) when it is originally collected.

There are international regulations on data protection which could be used to guide the development of broader data protection rights, most noticeably the EU's GDPR framework.

The introduction of a CDR in New Zealand which creates data protection rights that extend to both the collection and sharing of a new subset of 'data', together with new data-sharing infrastructure, will create the conditions for, and form the basis of, a much richer range of services and products across the economy, and better position New Zealand for the emerging digital economy.

---

[68] Health and Disability Commissioner, *Health and Disability Commissioner (Code of Health and Disability Services Consumers' Rights) Regulations 1996*. Refer: https://www.hdc.org.nz/your-rights/about-the-code/code-of-health-and-disability-services-consumers-rights accessed October 2020

[69] Digital.govt.nz, *Web Accessibility Standard 1.1*, 1 July 2019. Refer: https://www.digital.govt.nz/standards-and-guidance/nz-government-web-standards/web-accessibility-standard-1-1/ accessed October 2020

[70] W3C, Web Accessibility Initiative. Refer: HYPERLINK "https://www.w3.org/WAI/standards-guidelines/mobile/" https://www.w3.org/WAI/standards-guidelines/mobile/ accessed October 2020

[71] Digital.govt.nz, *Accessibility*. Refer: https://www.digital.govt.nz/standards-and-guidance/design-and-ux/accessibility/ accessed October 2020

For entities operating in jurisdictions with a regulatory led approach with similar data rights and data sharing rights – specifically Australia, the EU and the UK – the consistency of these regulatory frameworks with New Zealand's CDR framework could be leveraged to allow faster regulatory approvals for them to operate in New Zealand. Aligning New Zealand legislation with those jurisdictions would also enable customers in those jurisdictions to take advantage of goods and services offered in New Zealand by the local businesses, and vice versa.

Legislative design

Question 23: Do you have any comments on where a consumer data right would best sit in legislation?

The question of where a consumer right would best sit in legislation is dependent, in part, on the primary policy objective that a CDR is seeking to address, as outlined in our opening comments. The discussion paper outlines a number of potential benefits from establishing a CDR, but it does not explicitly state the primary policy objective that a CDR is seeking to address.

We have noted that New Zealand, along with other countries, is transitioning to a digital economy. Enhancing data rights and data sharing rights are an important element of this transition.

Deloitte agree that the legislative framework of a CDR intersects competition, consumer and privacy law and, as a result, consideration should be given to whether the CDR may sit better in a stand-alone Act.

The rationale for the creation of a stand-alone Act is strengthened if CDR legislation is accompanied by changes to, or the introduction of, legislation on a range of enablers for a digital economy including data rights for the original collection of data, enhanced privacy legislation, legislation on digital platforms, legislation on AI and algorithms, payments legislation, and digital ID.

A stand-alone Act and a new regulator could potentially help to ensure that developments in each of these components are consistent and contribute to an efficient, innovative, competitive and fair digital economy. In the absence of this, New Zealand would benefit from other measures to coordinate and align the initiatives which will contribute to the emerging digital economy.

The creation of a new stand-alone Act in Australia was a recommendation of the Senate Select Committee (Recommendation 19) and was recommended in the Australian PC Data Report.

If the primary policy objective for a CDR is to strengthen consumer's rights to access and share their data as the amount of data generated accelerates, then the CDR would best form part of New Zealand's privacy legislation. At its heart, the CDR is a consumer right to move their data from one provider to another. Inherent in the CDR is the implication that consumers know and understand what information is being transferred, why it is being transferred, to whom it is being transferred and what the personal information will be used for. To the extent that the data being transferred via a CDR is personal information, such transfers will be subject to the Privacy Act and it is fundamental to the success of the CDR that businesses do comply with the Act. Consideration of the NZ Privacy Act and other global privacy regulations when developing the CDR would reinforce to businesses and consumers that:

- The CDR is a consumer right that consumers can choose to either opt into or out of
- Fundamentally it is intended to benefit consumers
- The CDR needs to be utilised in a way which is consistent with the Privacy Act
- When enforcing breaches of the CDR, the regulator(s) should emphasise their focus on the protection of an individual's right to privacy

However, there is a risk in this approach that too strong a focus on privacy overshadows the promotion of competition and innovation. In addition, the Privacy Act applies to personal information so to the extent that the CDR incorporates business data, supplementary legislation would be required.

If the primary policy objective for a CDR is to promote competition, then the CDR would best form part of New Zealand's competition legislation. In this circumstance it would be appropriate for the Commerce Commission to oversee the CDR. This approach would be enhanced if there were concurrent enhancements to strengthen the privacy legislation and broaden it to include legislation on the original collection of data.

Institutional arrangements

Question 24: Do you have any comments on the arrangements for establishing any new bodies to oversee parts of a consumer data right?

One of the challenges of building a framework for a digital economy is that the regulatory responsibility is spread across several different regulatory agencies and government departments. This is amplified in a sector-based data-sharing framework as the CDR is extended to other sectors.

In Australia, the Farrell Review noted that:

> '*standards need to be written with the close involvement of experts and industry to ensure that they are fit for purpose and able to evolve to the changing technological environment. As proposed in a number of submissions,*[72] *a special body given the responsibility of setting Standards would ensure that all participants and potential future participants have an opportunity to contribute. Given the need to coordinate disparate views, ensure a fair hearing for all potential participants and protect against barriers to entry, this Data Standards Body would be appointed by the Government. It would include potential accredited parties, customer representatives, and data transfer experts*.'[73]

Further to this recommendation, various bodies were set up to regulate ACDR.

In addition to the Australian Treasury and the three regulators responsible for the ACDR – the ACCC, the Data Standards Body (DSB) and the Office of the Australian Information Commission (OAIC) – a broad range of other regulators have responsibility for various aspects of the digital economy including ASIC, APRA, AUSTRAC, the Australian Taxation Office (ATO), the Australian Energy Market Operator (AEMO), the Digital Transformation Agency (DTA), the New Payments Platform (NPP), Home Affairs and more.

In a multi-regulator model similar to Australia, New Zealand's Commerce Commission could potentially oversee the CDR to promote competition and protect consumers in New Zealand. In this approach the OPC would be well-placed to oversee the legislative aspects of CDR as it pertains to personal information and it might be possible to enhance its existing tools and enforcement options to manage breaches. Both regulators have well-established enforcement functions, and these would need to be funded appropriately to deal with any increase in workloads as a result of CDR and staffed with personnel with the necessary skills and experience.

A new data standards body could be set up in New Zealand as would a technical agency to oversee standards. It could potentially also manage accreditations for third-party providers. Such a DSB could include representation from potential accredited parties, customer representatives, and data transfer experts.

Currently, Payments New Zealand (PNZ) API Centre develops, maintains and publishes payment-related API standards for New Zealand. In Australia, CSIRO's Data61has been appointed as the DSB for the CDR regime. These standards have been prepared by the DSB. The work of standards development is conducted in close consultation with the as the lead regulator of the ACDR, supported by the OAIC.[74]

Irrespective of which approach is adopted, this will be important to adopt measures to coordinate and align the initiatives undertaken by these regulators where they contribute to the emerging digital economy.

Many jurisdictions which have adopted data-sharing initiatives have underestimated the scale and complexity of implementing them.[75] In Australia, the start of customer data sharing was 12 months behind the original release date of 1 July 2019 after having been delayed twice. Delays in designing and implementing the process for accrediting data recipients have meant that currently there are only three accredited data recipients able to receive shared data.

It is important that the regulatory entity or entities with responsibility for implementing a CDR for New Zealand can manage the complexity of building the regulatory and technological infrastructure and standards which support it. To achieve this, it will be important that the regulators have both the funding and appropriate expertise to enable this to be delivered.

---

[72] Australian Finance Industry Association submission, page 3 and the RBA submission, page 2 as referred to in Farrell Review (2017), page 21n. Refer: https://treasury.gov.au/sites/default/files/2020-07/afia.pdf and https://treasury.gov.au/sites/default/files/2020-07/rba.pdf

[73] Farrell Review (2017), page 21

[74] Consumer Data Standards. Refer: https://consumerdatastandards.gov.au/ accessed October 2020

[75] Deloitte (September 2020), page 2

Question 25: What are the pros or cons of having multiple regulators, or a single regulator, involved in a consumer data right?

Having multiple regulators responsible for oversight of the legislation and enforcement, accreditation of TPPs, privacy and confidentiality, and the development and implementation of technical standards could enable these activities to be undertaken by existing regulators who are currently undertaking similar functions. For example, the FMA may provide a supervisory role for accreditations within the financial services sector.

There are also potential benefits in having multiple regulators working together. In the case of the CDR, there are strong privacy and also competition law components to the right. We are fortunate that we have two regulators that have strong capabilities in these areas, and it would be useful to capitalise on this expertise to the extent possible.

One potential negative for having multiple regulators is the potential for consumer (or business) confusion about which to approach in what situation. This problem could be mitigated through public awareness programmes and also good communication between the regulators to ensure that complaints are dealt with by the correct entity.

There is also the potential for inconsistency across the regulators, delays where regulators need to work together, differing priorities and a diminishment in the powers or authority of the regulators compared to if the powers were centralised in a single regulator. In all cases, the regulators will need to be properly funded so they can build capability where necessary and can implement the legislation in a meaningful way to give consumers confidence in a CDR.

The Farrell Review recommended that Australia adopt a multi-regulator model with the ACCC (rules, accreditation, competition and consumer issues), the OAIC (privacy protections) and the DSB (technical standards) each having a regulatory role.[76] They would be supported by the RBA, ASIC and APRA which would provide advice as required.

The Review noted that one of the benefits was that this model would 'minimally disrupt current arrangements' and 'be the best vehicle to both protect customers and provide them with access to new opportunities and choices.'[77]

However, although it has only just commenced, this multiple regulator approach has been questioned by the Senate Select Committee on Financial Technology and Regulatory Technology, which recommended that Australia 'establish a new national body to consolidate regulatory responsibility in relation to the implementation of the Consumer Data Right' (Recommendation 19).[78]

This approach has also been raised in submissions to the Inquiry into Future Directions for the Consumer Data Right. Some submissions called for a single entity to be accountable for implementation given CDR is 'a significant economy-wide IT infrastructure project'[79] and noted the role of Singapore's Infocomm Media Development Authority (IMDA) as the body responsible for the data economy.[80] However other submissions questioned whether a single regulator would be able to fulfil the regulatory functions needed to support either industry-specific requirements or the broader data economy needs.[81]

New Zealand should consider the matters raised in the review being undertaken by Australia of the operating model for data sharing regulation and implementation when deciding what regulatory model is most suitable for New Zealand.

Monitoring and evaluation

Question 26: If government decides to establish a consumer data right, do you have any suggestions of how its effectiveness could be measured?

Measuring the effectiveness of a CDR must link back to the problems we are seeking to solve through its establishment.

In terms of privacy, before and after surveys could be used to gauge consumer sentiments and confidence levels in terms of data literacy and level of control.

[76] Farrell Review (2017), Recommendation 2.2, pp 16-17
[77] Farrell Review (2017), page 16
[78] Senate Select Committee (2020), page *ix*
[79] For example, submission by the Australian Banking Association to the Inquiry into Future Directions for the Consumer Data Right, 21 May 2020
[80] For example, submission by Data Republic to the Inquiry int Future Directions for the Consumer Data Right, April 2020
[81] For example, submission by the Australian Payments Network to the Inquiry into Future Directions for the Consumer Data Right, 21 May 2020

Other measures could assess the impact on the competitive landscape. Potential measures include the number of entities which have been accredited as data recipients. Businesses could be surveyed to report the extent to which new products have leveraged data shared under the CDR.

As for the rate of adoption of data sharing, measures could include the number of API calls made. In the UK for example, charts are published showing the use of API calls.

In terms of the impact on consumer experience, measures could be developed from consumer and industry surveys around the key benefits obtained and the actual experience when switching service provide.

Contact Us

Faris Azimullah
Partner, Risk Advisory Services
Deloitte
fazimullah@deloitte.co.nz
+64 9 303 0842

Damian Harvey
Partner, Systems Engineering|Consulting
Deloitte
dharvey@deloitte.co.nz
+64 9 306 4464

Paul Wiebusch
Partner, Open Data|Open Banking
Deloitte
PWiebusch@deloitte.com.au
+61 3 9671 7080

Rajesh Pradhan
Director, Risk Advisory Services
Deloitte
rpradhan@deloitte.co.nz
+64 9 303 0938

Deloitte.