MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

COVERSHEET

Minister	Hon Dr David Clark	**Portfolio**	Commerce and Consumer Affairs
Title of Cabinet paper	**Establishing a Consumer Data Right**	**Date to be published**	9 July 2021

List of documents that have been proactively released		
Date	**Title**	**Author**
June 2021	*Establishing a Consumer Data Right*	*Office of the Minister of Commerce and Consumer Affairs*
30 June 2021	*DEV-21-MIN-0145* *Establishing a Consumer Data Right*	*Cabinet Office*
June 2021	*Regulatory Impact Statement*	*MBIE*

Information redacted **YES**

Any information redacted in this document is redacted in accordance with MBIE's policy on Proactive Release and is labelled with the reason for redaction. This may include information that would be redacted if this information was requested under Official Information Act 1982. Where this is the case, the reasons for withholding information are listed below. Where information has been withheld, no public interest has been identified that would outweigh the reasons for withholding it.

Some information has been withheld for the reason of constitutional conventions.

MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

Regulatory Impact Statement: Establishing a consumer data right

Advising agencies	*Ministry of Business, Innovation and Employment*
Decision sought	*Analysis produced for the purpose of informing Cabinet decisions*
Proposing Ministers	*Commerce and Consumer Affairs*
Date	*23 June 2021*

Summary: Problem and Proposed Approach

Introduction

Key terms

A **consumer data right** describes the ability of a consumer to securely share information that is held about them by businesses or other entities with third parties.

Consumer data is information about a consumer. For the purposes of this RIS, a consumer can be an individual or an entity such as a business.

Examples of consumer data include the amount of energy an individual consumes over a month, or the transactions within a business' bank account.

Product data is data that relates to the products and services offered by businesses.

Examples of product data include information about the offering, terms and conditions, price and charges associated with certain products.

Data portability is the ability for an individual to request access to information that is held about them, and to direct an entity to share that same personal data with a third party.

Scope of this RIS

This Regulatory Impact Statement (RIS) is the first of two that will be prepared to assess proposals to establish a consumer data right. This RIS accompanies a Cabinet paper seeking approval to initial, high-level proposals for the design of a consumer data right. Proposals covered in this RIS include:

- types of data and functionality under a consumer data right
- options for the regulatory model

- options for the components of the regulatory framework.

The second RIS will accompany a further Cabinet paper seeking approval to detailed and second-order design questions. We expect Cabinet approval will be sought in Q4 of 2021. Proposals covered in the second RIS will include:

- institutional arrangements
- enforcement and offences regime
- funding

Should Cabinet agree to the proposals in this, and the future RIS, we anticipate that further decisions will be sought in 2022 regarding the implementation of the consumer data right. This will include the sectors that will be designated, and the timing of those designations.

Structure of this RIS

The structure of this RIS is as follows:

- Summary:
  - Problem definition
  - Proposed approach
  - Benefits and costs
  - Evidence certainty and quality assurance
- Section 1: General Information
- Section 2: Problem definition and objectives
- Section 3: Options identification
  - Types of data and functionality under a CDR
    Impact analysis
  - Options for regulatory approach
    Impact analysis
  - Options for components of a regulatory framework
    Impact analysis
- Section 4: Conclusions
- Section 5: Implementation and operation
- Section 6: Monitoring, evaluation and review

Problem definition

What problem or opportunity does this proposal seek to address? Why is Government intervention required?

Opportunity

Facilitating the sharing of individual and business consumer data with third parties provides an opportunity to maximise the value of that data to consumers. Higher and more widespread data flows promote innovation, which is likely to benefit individuals – through access to a greater range and choice of products and services available to consumers at lower cost, increased speed, convenience, personalisation, and security – and businesses, by enabling growth, improving productivity, and reducing risk.

Problem

Strong commercial disincentives, reduced competitive constraints, a lack of transparency, and fragmented regulatory systems, have created an environment in which data flows are constrained, causing New Zealand to miss out on the societal and economic benefits that would have been enabled by the flow of that data.

Progress implementing sector-specific initiatives has been slow, and these have had a modest impact to-date. For the most part, these regulatory and non-regulatory initiatives are not workable on a wide scale, therefore they are not expected to have a significant impact on data flows. It is unlikely that businesses will pursue initiatives that will deliver consumer-oriented and large scale benefits without a form of external pressure, compulsion, or the credible threat of regulation. We have therefore concluded that government intervention is required to remove barriers that individuals and businesses face in accessing data, to enable higher, more widespread flows of data through the economy.

Proposed approach

How will Government intervention work to bring about the desired change? How is this the best option?

We propose establishing a 'consumer data right' (**CDR**) legislative framework that allows New Zealand consumers and the economy to realise the long term benefits of data sharing, by enabling higher and more widespread flows of data through the economy. The CDR would improve choice and control by allowing individual and business consumers to more readily access their data, and direct that it be shared with and used by third parties, for consumers' benefit.

To overcome the existing barriers to data sharing, a sector designation model is proposed. This model is similar to the Australian Consumer Data Right (ACDR) and comprises an overarching primary legislative framework, which would establish the CDR and empower the Minister to designate particular sectors or markets as subject to the CDR. The potential benefits of consumer-driven transfer have widespread application, so this model would allow the CDR to be implemented in large parts of the economy over time. While implementation would occur at a sectoral level based on the defined requirements for each sector, the overarching framework would ensure consistency and interoperability across sectors.

The legislative framework would include a suite of regulatory tools, including an accreditation regime for participants that access data, the introduction of additional privacy safeguards for individuals and businesses that share data, the ability to make rules for how the data is shared and technical data standards to ensure the consistent treatment of data.

This regulatory impact statement has been prepared to assist Cabinet's decision on whether there is a need for regulatory intervention, the regulatory framework, and the regulatory tools available. These proposals do not represent the complete package of measures proposed to address the problem. Policy decisions on additional regulatory tools, enforcement measures, institutional arrangements and funding will be sought in Q4 of 2021.

The financial impact of these proposals on businesses is difficult to quantify and subject to a range of factors. The costs on the different regulatory system participants are discussed in detail in the following section.

Summary: Benefits and costs

Who are the main expected beneficiaries and what is the nature of the expected benefit?

New Zealand consumers (individuals and businesses) are expected to be the main beneficiaries of these proposals.

Non-monetised benefits

Consumers

Data portability is expected to benefit consumers (i.e. any end user of a product, including individuals or entities) by improving consumer outcomes, empowering consumers with greater control over their data, and supporting inclusion:

- Consumer outcomes: as the range and quality of products and services available to consumers improves, and they are given more control over their information, consumers have more choice over the products and services they use and more convenience in readily switching to ones that better meet their needs. A simple example is the development of new, cheaper payment methods or the ability to bundle bill payments. More sophisticated tools that could emerge to make consumers' lives easier include personal financial management platforms that aggregate spending data across users' various banks, loyalty programs, and payment platforms in order to provide insightful investment and financial advice.
- Greater control: the ability of individuals to require transfer of their data from one service to another, rather than needing to re-enter that data manually, will improve their control and autonomy over data and better enable them to engage the services of their preference.
- Inclusion: Intervention also has the potential to support greater inclusion through innovations that provide consumers with more choice of products and services at lower prices.

Businesses

Data portability is expected to benefit business by enabling growth, improving productivity, and reducing risk:

- Growth: A CDR would enable businesses to pursue new opportunities to extend their core business or develop completely new products or lines of business through partnerships with third parties. Using aggregated and categorised data, businesses may derive insights about customer behaviour and activity to personalise the products and services that are offered to customers.
- Productivity: A CDR would also remove the need for businesses to have bilateral agreements with individual data holders, and would allow smaller businesses to partner with third parties to utilise usage data to provide new service offerings or improve existing offerings. Businesses would also be able to provide more efficient products to help reduce administrative costs, streamline processes for making payments, managing invoices and suppliers, or leveraging economies of scale. Some could choose to become back-end infrastructure providers to industries. An example of this is in the cloud accounting sphere, where the services offered by Xero have provided significant benefits to businesses.

- Risk reduction: Businesses can pool data to identify fraudulent transactions and accounts, or to reduce their compliance burdens (for example, carrying out affordability assessments relating to consumer credit contracts).

Beyond these benefits, higher data flows offer a range of significant economic development opportunities. They can act as a spur for competition by expanding the range of providers via new entrants, reducing inefficiencies in the operations of existing services providers, improving the allocation of a sector's resources, facilitating comparison shopping and switching of products and enabling the creation of secondary markets. As data sharing becomes more widespread and sophisticated, new opportunities for growth and value may present themselves.

Outside of New Zealand, an increasing number of jurisdictions have regulated to accelerate the uptake of open banking models in particular. Several stakeholders provided anecdotal evidence of start-ups and small businesses that were moving offshore or bypassing the New Zealand market altogether, due to the barriers to data sharing and perceived uneven playing field. A benefit of intervention may be that these businesses remain in New Zealand onshore, and provide economic benefits to New Zealand consumers and the domestic economy.

Establishing a CDR offers an opportunity for New Zealand to harmonise with Australia, in turn enlarging the market of firms that use CDRs to provide innovative services that consumers and other firms value. Harmonising CDRs would advance the New Zealand-Australia Single Economic Market.[1]

Monetised benefits

It is difficult to estimate the overall monetary value of benefits to consumers (individuals and entities) of a CDR as this is contingent upon a number of factors, including the markets or sectors that are designated, the scope of any designations, the rate of innovations that rely on the transfer of data, and overall participation of consumers and businesses.

However, research in New Zealand and the United Kingdom suggests that individual consumers could save significant sums each year by moving to alternative bank accounts, and electricity or mobile plan providers that better suit their needs.[2, 3] A CDR would help consumers to realise these benefits, by making it easier for them to compare products and seamlessly switch between different providers, allowing them to choose a product that better meets their needs.

Where do the costs fall?

In the short term, businesses within a designated sector would be required to put in place systems and processes that enable data to be shared in a machine readable format if they wanted to participate in the CDR. The extent of these costs will vary depending on the size of the market, the types of data subject to the CDR, and whether businesses are already complying with other data

[1] Australian Government Productivity Commission and New Zealand Productivity Commission (2019). Growing the digital economy in Australia and New Zealand, Maximising opportunities for SMEs. https://www.productivity.govt.nz/assets/Research/b32acca009/Growing-the-digital-economy-in-Australia-and-New-Zealand_Final-Report.pdf

[2] Electricity Price Review (2019). Final Report. https://www.mbie.govt.nz/dmsdocument/6932-electricity-price-review-final-report.

[3] United Kingdom Competition and Markets Authority (2016). Retail banking market investigation, Final Report. https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf;

portability regimes, such as the European Union's General Data Protection Regulation (**GDPR**). Those wishing to access data will incur costs associated with obtaining accreditation.

The costs of accreditation may be greater for smaller providers or new entrants, who are less likely than larger existing providers to have already made adequate investments in infrastructure to handle and protect data. [4] In 2018, Westpac Australia estimated the cost of open banking at between AU$150million and AU $200 million.[5] This was attributed to the complexity of the existing systems as well as the need for specialised skills in order to implement open banking. Others have estimated the cost to an organisation to build a data storage centre capable of hosting CDR data to the required security standard could be in the range of AUD $50,000 - $70,000.

The proposals will involve an initial, one-off cost to government to establish a new regulatory regime, and ongoing costs for the new regulatory functions. The extent of these costs will depend on a range of factors that will be considered in a second RIS later in 2021, including decisions relating to the sectors that might be designated under the CDR and the institutional arrangements. As an example of potential costs to the Crown, the Australian Government had forecast A$100 million of expenditure over five years. In their recent Budget 2021 announcements, the Government announced a further A$113.1 million in funding to accelerate the implementation of the CDR. We anticipate that a CDR could be implemented at a lower cost, by learning from the Australian experience, leveraging existing systems and building economies of scale.

These costs will be phased as it is proposed that the CDR be implemented on a sector-by-sector basis. Third party businesses that do not wish to access consumer data will not be obligated to incur these costs. Over time, as uptake increases, we expect to see intermediaries and other third parties help to reduce the costs for data holders and data recipients to ensure compatibility with different technological specifications, and the costs of creating data links for portability, standards, interoperability, and compatibility.

Work is underway to identify sectors of the economy which would be among the first to be designated. This pipeline of implementation will improve certainty for businesses and support them to prepare and plan for the associated expenditure.

What are the likely risks and unintended impacts, how significant are they and how will they be minimised or mitigated?

Impacts on regulatory systems

Data portability risks having unintended adverse effects on competition and consumer welfare. It could give large multi-national companies access to significant volumes of data which could entrench their market position at the expense of smaller firms and new-entrants. Therefore, concerns have been raised about the effectiveness of data portability in fostering market competition. Market participants who risk losing their user base due to lower switching costs may be dis-incentivised from investing and innovating in the collection of data in the first place, given

[4] OECD, Working Party on Data Governance and Privacy in the Digital Economy (2021). Data Portability: Analytical Report, Mapping data portability initiatives and their opportunities and challenges. DSTI/CDEP/DGP(2021)1.

[5] https://www.zdnet.com/article/westpac-predicts-open-banking-to-cost-au200m-to-implement/.

the lower expected returns on investment. Additionally, as data management costs tend to increase with data sharing which can reduce returns on investment, incentives to invest and innovate can be further reduced.

As the number and variety of actors that can access data increase, there is a corresponding increase in the risk of that data being subject to new forms of theft or online fraud, data breaches lack or breaches of privacy, digital security incidents, excessive data profiling leading to financial exclusion, , and the manipulation of consumers' behavioural biases when operating online. A fundamental tension exists between enabling the economic and social benefits of data sharing, while ensuring privacy and data protection. An additional layer of complexity is the potential commercial sensitivity of data. The biggest risk of these proposals is that the balance struck by the CDR is not well calibrated, and goes too far to protect privacy and information at the expense of competition and innovation, or vice versa and that innovation is enabled at the expense of privacy and trust. To mitigate this risk, we have examined international approaches and issues with the designs from those experiences, and have proposed measures that we consider will best support a pro-competitive and innovative system with adequate regulatory supervision. This includes the introduction of an accreditation regime that prescribes standards for information security and limits who is able to access consumer data. Information security risks could also be offset by the requirement for businesses to update their systems in order to participate in the regime.

Risks of a CDR not achieving its intended objectives

There is a risk that in the short term, accredited entities will pass the costs of accreditation onto their customers, which could offset any consumer benefits derived through access to lower priced products and services. This is likely to have a small impact on consumers (and prices), because it is expected businesses would seek to spread these costs across customers.

If the costs of compliance (including accreditation) are set at a level that creates higher barriers to entry than exist in the current environment, this may reduce participation in the CDR and prevent innovation from occurring. Many stakeholders with a trans-Tasman presence noted that this had occurred in the implementation of ACDR, which they perceived to have imposed disproportionately onerous requirements on smaller or lower risk participants. These stakeholders strongly encouraged officials to learn from the Australian experience when designing the accreditation framework for New Zealand. These risks would be mitigated by adoption of a risk-based (tiered) accreditation system, and close consultation with industry and Australian counterparts on the requirements for accreditation.

Traditional narratives espoused by governments and businesses have warned consumers of the risks of sharing their personal information with third parties, and discouraged consumers from doing so. This mentality is counter to the premise of a CDR. Consumer trust and confidence will be critical to the success of a CDR. Distrust in digital systems, like a CDR, will hamper individuals' and consumers' willingness to engage. Reduced participation in the CDR could inhibit the CDR from achieving its policy objectives. This risk will be minimised through a consumer awareness and education programme about the benefits and security of a CDR. This impact of the programme would be maximised if it were delivered in partnership by the public and private sector. Further, to ensure that data sharing doesn't come at the expense of confidentiality and give grounds to potential consumer fears, appropriate security measures to protect data and make remedies available will be enacted, which will focus on giving consumers control. It will be essential to educate and engage consumers about the value of their data, and how they can utilise it for their

own benefit through a CDR, including to gain access to more personalised services or better priced products from their existing providers or competitor providers.

Identify any significant incompatibility with the Government's 'Expectations for the design of regulatory systems'.
We have not identified any significant incompatibilities with the Government's 'Expectations for the design of regulatory systems'.

Summary: Evidence certainty and quality assurance

Agency rating of evidence certainty?
Overall we have a high level of confidence in the evidence base for the opportunity and problem definition. The Australian and UK reviews into open banking/retail banking markets, as well as the Commerce Commission's analyses of local electricity and telecommunications markets, have provided clear evidence of barriers to data sharing, and issues with existing data sharing practices. A range of consumers submitted on the barriers to data sharing that they experience and which exists across large parts of the economy, in particular, the banking and finance sector. Some of these submissions also canvassed the commercial structures (disincentives) that they perceive to have been an impediment to meaningful progression of data sharing initiatives. Several stakeholders provided anecdotal evidence of start-ups and small businesses that were moving offshore or bypassing the New Zealand market altogether, due to the barriers to data sharing and a perceived uneven playing field. The quantitative evidence available to assess the likely impact of the various options against the status quo is limited. In the United Kingdom, there has not been an audit of the impact of open banking, or attempts to quantify the impact on consumer and economic outcomes. The Organisation for Economic Co-operation and Development (OECD) acknowledged in a 2021 working paper that poor evidence base and scarcity of empirical literature has hampered efforts to compare the various approaches to data portability, including analysis of the economic and social opportunities and challenges.[6] In Australia, the government commissioned an Inquiry into the Future Direction of the Consumer Data Right following the initial implementation of the ACDR. The Inquiry was completed in October 2020 and made a number of recommendations, largely aimed at improving the efficiency and reducing compliance costs of the ACDR. Our analysis incorporates the lessons from this inquiry. We have not sought to quantify the value of data flows to the New Zealand economy. Such estimates are complex and not yet well understood globally. For example, this year the OECD commenced a two-year project "Data Governance for Growth and Wellbeing" to enhance the understanding of data, their properties, use, transfer, and flows.

[6] OECD, Working Party on Data Governance and Privacy in the Digital Economy (2021). Data Portability: Analytical Report, Mapping data portability initiatives and their opportunities and challenges. DSTI/CDEP/DGP(2021)1.

To be completed by quality assurers:

Quality Assurance Reviewing Agency:
The Treasury and the Ministry of Business, Innovation and Employment
Quality Assurance Assessment and Reviewer Comments:
A quality assurance panel with members from the Treasury's Regulatory Impact Analysis Team and the Ministry of Business, Innovation and Employment (MBIE) has reviewed the Regulatory Impact Statement (RIS) "Establishing a consumer data right" produced by MBIE. The review panel considers that it **meets** the Quality Assurance criteria. The RIS presents a clear problem definition and provides robust analysis on a range of options relating to high-level policy decisions in establishing a consumer data right in New Zealand. A wide range of stakeholders have been consulted, with stakeholder views accounted for in the identification and assessment of options. The Panel notes that the detailed costs and benefits of a consumer data right are difficult to assess at this point, however this will be considered further in a second RIS to be produced at a later stage on detailed and second-order design questions.

Impact Statement: Establishment of a consumer data right

Section 1: General information

Purpose
The Ministry of Business, Innovation and Employment is solely responsible for the analysis and advice set out in this Regulatory Impact Statement, except as otherwise explicitly indicated. This analysis and advice has been produced for the purpose of informing key (or in-principle) policy decisions to be taken by Cabinet.

Key Limitations or Constraints on Analysis

Scoping of the problem

The RIS covers opportunities to better realise the potential benefits from sharing and use of consumer data within the economy. It does not consider more general issues with New Zealand's privacy regime that fall within the Justice portfolio.

Evidence of problem and quality of data

This RIS relies on predominantly qualitative and anecdotal data to assess the impacts of the proposed options, including findings and reports commissioned by Australian and UK reviews of the CDR frameworks established in those jurisdictions (Furman report, Australian Productivity Commission's report, and the Open Banking review), and public submissions on a consultation document. For the most part, this evidence relates to the state of data portability in the banking and financial sector, though a limited amount of evidence was also submitted in relation to the telecommunications and energy sectors. Nonetheless, the evidence suggests that the same structural barriers are likely to encumber efforts to increase levels of data portability in other sectors in future, such as insurance or utilities.

The data sources relied on offered little in the way of quantitative evidence of the problems identified, or of the costs and benefits of the proposed options. This is because quantitative evidence on the overall impacts of data portability on competition is still very limited.[7] Esayas and Daly (2018) noted that there is very limited empirical research on data portability regimes and the extent to which consumers make use of these rights, or to which this facilitates competition.[8]

[7] OECD, Working Party on Data Governance and Privacy in the Digital Economy (2021). Data Portability: Analytical Report, Mapping data portability initiatives and their opportunities and challenges. DSTI/CDEP/DGP(2021)1.

[8] Daly, A., Esayas, S.Y., 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3236020. European Competition and Regulatory Law Review 3, 1-15.

Where possible, the RIS draws on multiple evidence sources to increase the robustness of the conclusions reached and our confidence in the underlying assessments.

Range of options considered

We have sought to give priority to the options that are more likely to deliver the greatest scale of benefit to consumers. All options have been assessed against the status quo. There are compelling commercial disincentives that make it extremely unlikely that under the status quo data sharing will become widespread across the economy, or occur at significantly increased levels, without regulatory intervention.

Assumptions underpinning impact analysis

A majority of the evidence relied on in making this assessment is the findings from Australian and UK reviews into the state of open banking. We have assumed that these findings can be extrapolated to other sectors, except for where we have canvassed the specific developments in the telecommunications and electricity sectors. Evidence of reduced competitive constraints strengthening incumbency advantage and posing barriers to entry and expansion apply equally.

Responsible Manager

Authorised by:

Daniel O'Grady
Competition & Consumer Policy
Ministry of Business, Innovation and Employment

23 June 2021

Section 2: Problem definition and objectives

2.1 Current state within which the action is proposed (status quo)

Data sharing can have many benefits

Businesses across New Zealand and the global economy are collecting and using increasingly larger volumes of personal data, acquired through the provision of goods and services to consumers. This has been partly enabled by improvements in the ability of businesses to collect, store, process, aggregate, link, analyse, and transfer vast quantities of data. It has also been accelerated by the shift in consumer preferences to trade online. Globally, data intensity is among the highest in the financial services sector.[9]

Once a consumer's data has been stored by a business, there are a range of potential benefits that come from its further use by the consumer. The value and utility of a consumer's personal data is a function of their ability to access and use that data for their own benefit. New technologies and uses of data can also increase the societal and economic benefits of personal data.

Data sharing can promote competition, by expanding the range of product and service providers via new entrants to a market, contribute to increasing the efficiency / productivity of service providers' operations, and facilitate comparison of and switching between products. Data sharing can also stimulate innovation (the development of new products, processes, and business models) by expanding access to information. Innovations which rely on the transfer of consumer data can provide consumers access to a wider range of products. These products can more affordable, convenient, security and personalised. This increased access can support inclusion in different sectors, for example, data sharing in the banking and financial sector has the potential to improve financial inclusion of groups that are vulnerable and/or currently excluded.

From a data protection perspective, data sharing can empower individuals with more control over their data, by allowing them to move their data easily and provide it for use by other businesses.

Examples of data sharing initiatives that have brought economic and social benefits to New Zealand include banks sharing data with cloud-based accounting platforms, or with credit reporting bureaus to assist in the loan application process, energy tariff data to better compare retail energy plans, or the sharing of location data with a wide range of apps.

Nascent data portability arrangements are present in a number of sectors of the New Zealand economy, and are available to New Zealand consumers through a range of online services. Below we discuss the arrangements in electricity, telecommunications and banking.

The New Zealand Productivity Commission recently completed an inquiry into maximising the economic contribution of New Zealand's frontier firms. Frontier firms are the most productive firms in the domestic economy within their industry, and as such, they play an important role in influencing our total productivity. They do this by diffusing new technologies and business practices into the New Zealand economy. The Productivity Commission identified the introduction

[9] OECD (2020). Financial Consumer Protection Policy Approaches in the Digital Age: Protecting consumers' assets, data, and privacy. www.oecd.org/finance/Financial-Consumer-Protection-Policy -Approaches-in-the-Digital-Age.pdf.

of a CDR as one intervention that could maximise the performance and contribution of New Zealand's frontier firms to the economy.[10]

Electricity

In the electricity sector, the Electricity Authority has directed a form of electricity data portability through the Electricity Participation Code 2010. The Commerce Commission considers that the sector is leading data sharing in New Zealand, with consumers and comparison websites making good use of the ability to compare usage and pricing.[11]

Consumers are able to request their consumption data, and retailers must comply with these requests within five working days. Retailers are also required to make tariff data available, and there is also an Application Programming Interfaces (API) for third parties to access information about the type of meter held by the consumers in order to inform what tariffs are available to them. In 2020, the Electricity Authority extended these rules to enable authorised third parties to access consumption data on behalf of consumers. Third parties wanting to use the standardised formats and file exchange software must sign up to certain terms and conditions of use.

Telecommunications

A form of data portability also exists in the telecommunications sector. The sector complies with specific legislation relating to the use of personal information, such as the Telecommunications Information Privacy Code. In 2007, the sector introduced mobile number portability, which allows a subscriber to keep their unique telephone number when they change telecommunications providers. Twin aims of the initiative were to increase competition amongst operators and enable the exercise of consumer choice, by removing the disincentive of losing one's phone number when switching providers.

In 2020, the Commerce Commission published an open letter to the telecommunications industry requesting they commence work to allow New Zealanders to share usage and product data between telecommunications providers and comparison services, to improve consumer choice.[12] The letter followed a report that examined mobile billing data, which found that many consumers were significantly overspending on their mobile plans due to transparency and inertia related issues, which were leading to non-competitive outcomes. As discussed in the benefits section earlier, that inquiry found that a majority of the 80,000 persons sampled had not switched mobile plans during the year, despite there being savings of over $100 a year available in doing so for over a half of those surveyed.

In response, the three mobile telecommunications providers agreed to undertake work to address transparency and inertia issues to improve consumer outcomes, including implementing three key measures:[13]

---

[10] New Zealand Productivity Commission (2021). New Zealand firms: reaching for the frontier Firms. https://www.productivity.govt.nz/assets/Documents/Final-report-Frontier-firms.pdf.

[11] Commerce Commission (2020). Mobile operators should improve consumer choice through easier comparisons. https://comcom.govt.nz/news-and-media/media-releases/2020/mobile-operators-should-improve-consumer-choice-through-easier-comparisons.

[12] Commerce Commission (2020). Mobile Operators should improve consumer choice through easier comparisons. https://comcom.govt.nz/news-and-media/media-releases/2020/mobile-operators-should-improve-consumer-choice-through-easier-comparisons

[13] Commerce Commission Open Letter "Addressing transparency and inertia issues in the residential mobile market", 9 March 2021, https://comcom.govt.nz/__data/assets/pdf_file/0022/242923/Open-letter-from-the-Commerce-Commission-addressing-transparency-and-inertia-issues-in-the-residential-mobile-market-9-March-2021.pdf.

- providing at least 12 months' usage and spend information to customers
- providing customers with an annual summary of their usage and spend along with a prompt to consider alternative options
- promoting the development of tools to enable more effective comparison and choice for telecommunications consumers through the TCF.

The Commission has publicly noted that they expect these measures to lead to significantly improved outcomes for mobile consumers, particularly insofar as:

- the provision of better information will enable consumers to make more meaningful comparisons and choices; and
- facilitating the introduction of comparison tools that fairly and accurately compare mobile plans for consumers will enhance competition and choice in the market.

Banking and finance

A modest level of data sharing is occurring in the banking and finance sector (**financial sector**). Banks currently share data with partner companies, mostly by entering into negotiated bilateral agreements:

- A common example of a data sharing agreement is that concluded between a bank and a credit bureau for the purposes of assessing the creditworthiness of current or prospective customers. When a customer applies for credit, a bank will seek consent from the customer to allow data sharing to occur in accordance with the requirements of the Credit Reporting Privacy Code 2020. This involves the bank providing information to the credit bureau about credit inquiries, defaults or (in the case of 'comprehensive credit reporting') active credit facilities, balances, and credit payment history. Credit bureaus in turn analyse this data, to provide information about the creditworthiness of the consumer to the bank. Notably, this initiative is intended to benefit the bank, and many consumers are unaware of the process through which this assessment is produced.
- Banks also have data sharing agreements with accounting software providers to help their business customers manage their accounting needs. In this situation, the banks are compensated for the provision of information to the accounting software platform.

Some data is transferred via 'screen scraping', which is discussed in section 2.3.

The Payments NZ API Centre has led the development of shared technical standards that could enable data sharing between banks and third parties (**open banking**). These standards prescribe how data is to be shared between banks and third parties, both in terms of the process and the form of data. However, as discussed in the next section, there has been little progress made to implement the standards. We consider that this progress has been slow as banks and other incumbents lack commercial incentives to invest in the development of APIs that would enable third parties to access data. This slow progress has reduced the overall effectiveness of open banking in New Zealand.

In line with the findings of the open banking reviews conducted in Australia and the UK, we expect there are low levels of search and switching among New Zealand banking consumers.

International context

Internationally there is increasing recognition of the growing importance of the value associated with data, including its role as an input to service provision. Some jurisdictions have attempted to intervene by engaging in legislative reform to promote consumer data portability or strengthen existing privacy rights, including the European Union (EU) through its General Data Protection Regulation (GDPR). After the introduction of regulation in Europe, a number of other countries followed suit, including Australia through the ACDR. The trend in some jurisdictions has been to extend what was initially conceived of as an 'open banking' framework across multiple sectors, in effect establishing a CDR for insurance, utilities, and pension data.[14]

Australia

In 2017, the Australian Treasurer commissioned the Review into Open Banking in Australia to recommend the most appropriate model for open banking in Australia. The Australian Government agreed to the key findings in the review for the framework of an overarching CDR, and for an iterative implementation of the right to open banking. Subsequently, in 2019, Australia has legislated the ACDR to give Australians greater control over their data, empowering customers to choose to share their data with trusted recipients only for the purposes that they have authorised. The legislation is principles-based, to enable it to adapt as the technological and legal environments evolve.

Under this model, the Australian Government determines which sectors the ACDR applies to by issuing a designation. Rules are prescribed for how the ACDR applies to the sector. The Rules allow a consumer to direct a company to share data held about them with third parties. The right has been implemented in the banking, energy and telecommunications sectors to date, and is expected to be rolled out to the entire economy on a sector-by-sector basis. Data on credit and debit card, deposit and transaction accounts at the main banks were required to be available from mid-2019, data on mortgages became available in February 2020, and data relating to products including business loans, overdraft facilities, and foreign currency accounts, became available from 1 February 2021. The ACDR in the banking sector does not contain a right to authorise other parties to initiate transactions on consumers' bank accounts ('write access' or 'action initiation'). Without this functionality it is unlikely the Australian banking sector will achieve the full potential of open banking.

The intention of the regime is that consumers will have the improved ability to compare and switch between products, which will encourage competition between service providers. The aim is that the ACDR will result in lower prices for consumers and encourage the development of innovative products and services in participating sectors.

In January 2020, the Australian Treasurer announced a review into the future directions of the ACDR. This was prompted by feedback that the existing settings were limiting the realisation of innovation and competition benefits, and not delivering the full range of expected benefits to consumers. The review made more than 100 recommendations to enhance the ACDR, including:

- to expand the functionality of the ACDR to deliver more convenience to consumers, including through action initiation, and provide certainty to consumers through ACDR dictionaries and improved consent management

[14] KPMG (2019). Open banking opens opportunities for greater customer value. https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/05/open-banking-opening-opportunities-for-customer-value.pdf

- to encourage broader participation in the ACDR to create more choices for consumers, by fostering innovative data sets and interoperability, and encouraging flexibility in sector assessments and reciprocity in data sharing
- to enhance specialisation and cooperation within the ACDR, and interaction with the digital economy, to create a data ecosystem that gives confidence to consumers, including by allowing trusted advisors to participate and enabling graduated accreditation, and leveraging its infrastructure and standards for wider applications
- to connect with similar overseas frameworks to provide broader choices for Australian consumers and opportunities for start-ups and digital businesses.

In regard to the final recommendation, we consider that aligning our respective frameworks to achieve inter-operability could result in significant economic benefit to each country. Officials from MBIE will continue dialogue with the Australian Treasury to ensure opportunities for synergies are considered through the policy development process.

European Union

In 2015, the European Union passed the second Payment Services Directive (PSD2), which gave effect to a sector-specific (financial) personal data sharing right. It aimed to increase competition and participation in the European payments industry from banks and non-banks, and to provide a level playing field by harmonising consumer protection and the rights and obligations for payment providers and users.

Specifically, the PSD2 gives customers the ability to grant third parties read and write access to their banking data via APIs. This means third parties can see and use customer banking data and also make payments on behalf of the customer. PSD2 promotes the use of APIs to retrieve account information from various sources on an ongoing timely basis, with full transaction details. Third parties must securely access this data, which they can then use to develop personalised/customised experiences to consumers. The expectation being that this would reduce the high barriers to entry for newcomers to the market, giving them a means of competing against existing providers to gain a competitive advantage.

The PSD2 does not include a principle of reciprocity or equivalency, as banks must share their customers' data with retailers but are not able to request access to the retailer's customer data. This risks creating an imbalance of information and having a chilling effect on innovation. Many have expressed concerns that large digital technology firms will leverage this data access to enter markets with negative effects in the long term.[15]

In 2018, the European Union introduced the General Data Protection Regulation (GDPR), which imposes a privacy-based obligation on organisations anywhere in the world which target or collect data related to people in the EU. The GDPR replaced a data protection directive from 1995, which was perceived as outdated and insufficient to respond to the risks and opportunities presented by the variety of ways in which data is stored, collected, and transferred today. The aim of the GDPR is to provide stronger data security and privacy protection rights via a single set of rules, to enhance how people can access information about them and place limits on what organisations can do with personal data. Additionally, it broadens the scope of existing EU law by introducing

[15] OECD, Working Party on Data Governance and Privacy in the Digital Economy (2021). Data Portability: Analytical Report, Mapping data portability initiatives and their opportunities and challenges. DSTI/CDEP/DGP(2021)1.

new data rights, including the right to deletion, the right to direct that data be shared, and the right to object to profiling. It also governs consent, privacy and liability.

In contrast to the PSD2, which is aimed at improving the seamlessness of sharing data in payment services, the GDPR regulates the protection of personal data across economies. The interaction between the two regulatory levers has raised compliance concerns among stakeholders. A lack of coordinating in the drafting, and guidance on the overlapping compliance, underlie these concerns.

All member states were obligated to incorporate the GDPR provisions into their national laws from early 2018, meaning companies have one personal data protection standard to meet within the EU. The GDPR is an economy-wide right data protection right, meaning the standard is uniformly applied to data used in cloud computing, banking, healthcare, social media markets etc. The standard of protection is relatively high, and is understood to have required most companies to make a sizeable upfront investment to develop and administer the necessary data protection infrastructure. Notwithstanding, under the GDPR, certain categories of sensitive personal data are given greater protection, for example, information about racial or ethnic origin, political opinions, religious beliefs, genetic and biometric data.

The GDPR has some limitations, including that it does not address the requirements of either safe and secure data sharing, or value generation from data portability that will be needed to realise the huge potential value of personal data.[16] Further, the right does not specify the obligation to respond in real-time to data portability requests, or any technical communication standards to transfer the data between organisations.

The 2019 Free-Flow of Data Regulation (FFDR) (the EU's newest data portability regulation) promotes data portability of non-personal data in business to business relationships. The FFDR instructs the European Commission to contribute to the development of EU Codes of conduct to facilitate the porting of non-personal data, such as anonymised aggregated data, or technical business data, in a commonly used and machine readable format, including open standard format. It also aims to integrate the EU data economy as part of the EU's wider strategic goal of a single data market.

United Kingdom

The United Kingdom was an early implementer of open banking. This was borne out of the release of a report in 2016, commissioned by Her Majesty's Treasury, which investigated the competitive and consumer outcomes of banks sharing transaction data with third parties using APIs. The recommendations of the report laid the foundation for open banking in the UK. These included an industry-led agreement on an open API standard to facilitate data access for third parties and an industry-wide approach for authorising third parties.

The Open Banking initiative is a sector-specific framework, in step with the PSD2. The work programme under the initiative has focused heavily on payment system providers, such as payments initiation and data aggregation. There has been a slow and gradual uptake of initiatives by banks and the wider FinTech community. Recent developments indicate that the use of open

[16] United Kingdom Department for Digital, Culture, Media & Sport (2018). Data Mobility: The personal data opportunity for the UK economy. https://www.ctrl-shift.co.uk/reports/DCMS_Ctrl-Shift_Data_mobility_report_full.pdf

banking is starting to proliferate in the UK. Open banking now has around 3 million users, and a wide range of UK SMEs are using tools employing open banking functionality.[17]

We expect that many of the findings of the UK's report into open banking hold true in the retail banking sector in New Zealand, for example:

- customers tended not to be with a savings account provider that would offer them cost savings
- the magnitude of potential savings from switching providers suggested that many customers were not sufficiently aware of available alternative products
- a multiplicity of barriers existed to assessing and accessing information on product cost and service quality, for example, to identify the best savings account for their needs, customers were required to combine information on different account charges and conditions
- customers reported low confidence in their ability to switch without risk or error
- customers who switched accounts had higher incomes, higher account balances, and higher education levels than those who did not.

While quantitative evidence on the overall impact of the Open Banking initiative is unknown, the UK Financial Conduct Authority estimated that a 2013 initiative, which facilitated switching between current accounts resulted in a 22 per cent increase in the number of current account switches when compared with the predecessor system.[18] After the commencement of the enabling legislation and regulations in 2017, it was reported that more than 170 third parties had registered for the scheme.[19] In its first year of implementation, open banking in the UK was supported by USD $3.3 billion of equity investments in FinTech companies in 2018.[20]

In December 2019, the UK Financial Conduct Authority sought feedback on a proposal to expand open banking to 'open finance', recognising that the shift to a broader model could offer significant benefits to consumers, including increased competition, improved advice, and greater access to a wider and more innovative range of financial products and services. The Authority also noted that the expansion of data sharing would create and increase risks, and raise new questions around data ethics and identity. Feedback from industry, while supportive of the proposal, highlighted the difficulties in seeking to remodel a purpose-built banking framework to other sectors. We see this as a key learning New Zealand can take on board when electing the design of a CDR framework.

In January 2020, the Competition and Markets Authority launched a review into the future of the governance and oversight of open banking remedies in the UK. They recently published a blueprint

[17] United Kingdom Competition and Markets Authority (2021). The future oversight of the CMA's open banking remedies. https://www.ukfinance.org.uk/system/files/Open-Banking-Phase-II-report-FINAL.pdf.

[18] United Kingdom Financial Conduct Authority. (2015). *Making current account switching easier.* https://www.fca.org.uk/publication/research/making-current-account-switching-easier.pdf.

[19] Open Banking Limited. (n.d.). Meet the regulated providers. https://www.openbanking.org.uk/customers/regulated-providers/

[20] Innovate Finance (2019). UK FinTech investment reaches record levels. https://www.innovatefinance.com/news/uk-fintech-investment-reaches-record-levels/

and transition plan for the future of open banking. We will continue to follow this review and take account of any findings in the proposals for a CDR for New Zealand. [21]

United States

The open banking market in the United States is unregulated. High levels of data portability have been achieved in the banking and financial sector without an overarching enabling framework. This is evidenced by the steady rate of development of innovative products and services that rely on the transfer of consumer data.

Open banking has been industry-led, mostly via bilateral data sharing agreements. Although no specific regulatory or legislative framework has been implemented to support open banking, the Consumer Financial Protection Bureau has published non-binding principles aimed at the 'consumer-authorised data-sharing market'. These principles advocate giving consumers access to their own data in a useable format and allowing consumers to authorise (and revoke) read-only third party access. They also promote informed consumer consent, data security, and dispute resolution, and suggest protocols on data use, retention, and liability.

Singapore

The Singapore Government has taken regulatory action to facilitate data sharing in the financial sector. In November 2020, Singapore amended its Personal Data Protection Act (PDPA). This introduced a data portability obligation, alongside a host of other measures that seek to strengthen the accountability of organisations, recalibrate the balance between individual consent and organisational ability to harness data for legitimate purposes (such as research and business improvement), and strengthen enforcement efforts by the regulatory authority. Twin aims of the amendment were to provide individuals with greater autonomy and control over their personal data to prevent consumer lock-in, and facilitate the innovative and more intensive use of specified personal data held by organisations.

The PDPA, which functions in a similar way to the UK's GDPR, contains data privacy provisions that came into effect in 2014. It established an overarching data protection framework that sets out baseline rules for the way companies can collect, store, use, and disclose data. The key principles include: consent, deemed consent, withdrawal of consent, reasonableness, accuracy, and transfer.

This reform follows the joint development and publication of non-binding API guidelines in 2016 between the Monetary Authority of Singapore and Association of Banks in Singapore, which encouraged banks to adopt APIs. These guidelines also offer information on security standards and governance models. The MAS operates the Financial Industry API Register, which contains over 500 APIs. One initiative that emerged out of this is the Financial Planning Digital Service (FDPS) which aimed to facilitate data portability with a secure API framework underneath giving consumers greater access to, and control over, their financial data.

Summary

These jurisdictions have sought to improve data portability through different means. In short, some jurisdictions have sought to implement broad and shallow data portability regimes that apply across the entire economy and are often supported by sector-specific regulation. Other jurisdictions have sought to achieve data portability within individual sectors before introducing an economy-wide right. The Australian model combines these approaches, by establishing a

[21] United Kingdom Competition and Markets Authority (2021). The future oversight of the CMA's open banking remedies. https://www.ukfinance.org.uk/system/files/Open-Banking-Phase-II-report-FINAL.pdf.

regulatory regime that can apply across the entire economy but tailored for the needs of specific sectors.

While the bulk of these initiatives are in their relatively early stages, New Zealand is in the advantageous position of being able to learn from the overseas' experience. The key learnings from these are discussed above and we have incorporated these lessons into our analysis of the assessments of the potential CDR models for New Zealand.

Strategic alignment and Government's priorities/direction

Implementing a CDR will contribute to Government's digital work programme. The CDR will help grow the digital economy by stimulating digital innovation and facilitating the growth of businesses generating value for customers from digital data. This is the focus of one of the work streams of the Digital Technologies Industry Transformation plan to promote data driven innovation by raising awareness of the value of open data and encouraging greater use.

A CDR will also feed into the ambition of the Digital Strategy for Aotearoa, which is in the early stages of development and will be released later in 2021.

Counterfactual

In the absence of intervention, we do not expect there would be material changes to the status quo. This assumes that there are no government-led interventions to promote data portability, for example, through an amendment of the Privacy Act. It also assumes that there is no credible threat of interventions in specific sectors.

Long-term negative consequences would be likely under the status quo, as New Zealand would lag further behind other countries actively facilitating data portability, with consequential lost opportunities to grow productivity and the digital economy.

2.2 Regulatory systems already in place, and connections to on-going work.

Regulatory system

There is currently no single dedicated regulatory framework for data portability in New Zealand. Nor is there a general right for consumers to direct that organisations share information which relates to them on request.

Collection, storage, and handling of personal information is currently regulated by the Privacy Act 2020, although that Act is not well placed to govern the exchange of data and data portability. This can contribute to undermining privacy rights in an increasingly digital environment.

Information Privacy Principle 6 provides that individuals are entitled to receive upon request:[22]

- confirmation of whether the agency holds any personal information about them; and
- access to their personal information.

While the Act allows a consumer to request, in general terms, the form which information must be provided in (e.g. in digital or hard copy), it does not allow a consumer to prescribe at a detailed level the form in which this data must be provided (e.g. a certain file type formatted in a particular way). This means consumers cannot necessarily use the Act to compel data holders to provide

[22] Privacy Act 2020, section 22.

information in an accessible, high-utility form. The Act also does not contain a general right for consumers to direct organisations to share information which relates to them on request. Further, given the large volumes of data that organisations now collect about individuals, a lack of consistent format can make it challenging to modify or delete personal information in practice.[23] The right to access data is at risk of becoming increasingly less effective and useful if individuals are not able to obtain their data in a form that enables them to make further use of the data.

The Privacy Act's framework is based on an organisation having a legitimate business purpose for collecting, disclosing or using the information and the relevant individual authorising the collection, disclosure or use. In effect, organisations (holding or receiving data) must make the individual aware of the purpose, and have reasonable grounds to believe that the individual has authorised the use of the personal information.

Many consumers are unlikely to be fully aware of how much data is being collected about them, or how it is being used. It is common practice for businesses to seek broad authorisations to collect information in a way that only gives the consumer the option to select "I agree to the Terms and Conditions", accompanied by lengthy, legalistic documents. Individuals that are unwilling to share their personal information on these terms, become unable to access the product or service. Insights from behavioural economics show that consumers are typically reluctant to click through to such documents and may be unable to understand the content even when they do. Rather than giving consumers the genuine opportunity to control the way their information will be used, these processes are akin to non-negotiable contracts. The consumer has no choice if they want the services, despite not having a clear understanding of what they are agreeing to.

In addition, the Privacy Act does not expressly require consents to expire after a defined period of time, though reliance on an old authorisation may undermine an entity's claim of reasonably believing an authorisation to hold the information exists. The Privacy Commissioner has confirmed that an individual can withdraw authorisation, though this is not expressly provided for in the Privacy Act. The Privacy Commissioner has advised that reliance on an authorisation that has been withdrawn would undermine a data holder's claim to reasonably believing an authorisation to collect and use the information exists, though the implications of doing so are not expressly stated in the Act. There is no requirement in the Privacy Act to notify an individual when their personal data is shared with a third party. Information Privacy Principle (IPP) 1 provides that personal information can only be collected for a lawful purpose, and IPP 10 provides that information collected for one purpose cannot be used for another purpose, but it does not place further limits on the purposes or uses for which information can be collected.

The Office of the Privacy Commissioner (OPC) wrote in its 2020 Briefing to the Incoming Minister that technological, social and other developments affecting privacy have continued apace since the policy work for the Privacy Act 2020 was undertaken, and highlighted data portability as a key emerging issue for further reform.

Sector-specific regimes

Beyond the Privacy Act, most of the frameworks in New Zealand that apply to data collection and use are sector-specific, which predate the emergence of the data-driven economy. Their ability to keep pace with and adequately address the technological, social, and other developments that influence how data is collected and used is limited. Regulators in the electricity and telecommunications sectors have powers that allow them to mandate certain forms of data

[23] OECD (2013), The OECD Privacy Framework. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

portability which apply to intra-sector data exchanges. However, none of the regulatory systems were designed with data portability in mind. This means those regulatory systems are not well placed to respond to issues related to data portability, which tend to be cross-cutting and can range from pricing, to access requirements to information security standards, to tailoring consent for consumers with varying needs. It also means that no single body has regulatory oversight and responsibility for the governance of data portability settings in New Zealand.

Businesses operating in other regulatory regimes are starting to make use of data portability in order to satisfy their obligations. One such example is under the Credit Contracts and Consumer Finance Act 2003 which was amended in 2020. From 1 October 2021, lenders will be required to carry out detailed affordability checks before entering into consumer credit contacts. Recently, ANZ announced an open-banking deal with Bud which will allow it to collect and verify income and expense information direct from a prospective borrower's bank accounts, significantly reducing compliance costs.

Connection to existing issues or active work

Regulation of Merchant Service Fees

MBIE is also leading work on regulation to reduce merchant service fees, in response to concerns that fees charged in New Zealand are out of step with overseas jurisdictions and markets are not functioning in a way that delivers the best outcomes for consumers, merchants and the New Zealand economy.

Some of the competition benefits from having the data portability in the financial services sector are expected to assist with resolving some of the issues identified in this work. For example, establishing data portability in the financial services sector will reduce some of the barriers to entry that new payment methods face. As such, this may result in the emergence of alternative, more consumer and merchant friendly or lower cost retail payment systems. The CDR will therefore complement the work on regulating MSF.

Digital Identity Framework

DIA is leading work on the creation of a Digital Identity Trust Framework. This is a policy and regulatory framework that sets and applies standards for security, privacy, identification management and interoperability; and enforces the standards through accreditation of participants and governance of the rules. In February 2021, Cabinet approved proposals to establish the Trust Framework in legislation. The aim of this work is to address gaps in regulation and accelerate the development and update of digital identity services that are secure, trusted and interoperable.

During consultation, many stakeholders expressed a desire to see elements of the Digital Identity Trust Framework integrated into the CDR, wherever possible, to maximise certainty and reduce compliance costs for business. Other elements of the Digital Trust Framework that could be leveraged in the CDR include the data standards body, and accreditation.

Officials from MBIE have been meeting periodically with the Department of Internal Affairs, to ensure the CDR design takes into account decisions made on the DITF, to identify areas for cooperation between the two projects, and to avoid duplication of the systems.

Open banking

The development of the consumer data right follows the Government's work programme on open banking. To date, this work has largely been industry-led. MBIE has been involved in the

governance of the Payments NZ API Centre as an observer on the API Council, and along with other departments has played a facilitative role to ensure that our regulatory settings do not deter innovation in the open banking or broader financial technology (FinTech) sector. We have engaged officials considering open banking and FinTech from the Reserve Bank, Financial Markets Authority and the Treasury during the development of these proposals.

2.3 Policy problem / opportunity

Policy problem, causes, and impacts

In section 2.1, we canvassed the various initiatives taken by regulators and the private sector to facilitate the sharing of consumer data, to produce public and private benefits. While these efforts have been significant, the actual use of data in New Zealand remains less than optimal, and some data sharing initiatives have not been implemented. This is because the efforts have a number of limitations and underlying problems, and international experiences suggests these alone will not allow the New Zealand economy to maximise the effectiveness of how it uses consumer data.

As has been identified by the OECD, systemic problems related to data infrastructure, availability, quality and timeliness, combined with a lack of coherence of policy frameworks and guidelines, and the lack of resources to facilitate safe, responsible and lawful access and sharing of data, mean that exchanging data remains challenging.[24]

The key issues, which we do not expect to materially improve under the status quo are:

- Many potentially beneficial data transfers are not occurring. This has a number of flow-on impacts: consumers and businesses are missing out on beneficial innovations or are not using the products and services that would best serve their needs, competition is limited by barriers to switching and to entry for new participants in many markets.
- Data exchanges that occur are not always in the best interests of consumers, and the methods of obtaining and transferring data are sometimes insecure, exposing consumers to unnecessary risks.

Together, these are leading to poor consumer outcomes and causing New Zealand to miss out on economic development opportunities.

These problems (the subset of issues contributing to the problems, and their impacts) are discussed in greater detail below.

The assessment of the problem is based on submissions received on MBIE's 2020 discussion document, engagement with stakeholders, and research into the state of data sharing in New Zealand markets and international jurisdictions.

Problem 1. Many potentially beneficial data transfers are not occurring and data transfers that are occurring are not always in the best interests of consumers

Background

Evidence that potentially beneficial data exchanges are not occurring include the slow progress on

[24] OECD (2019), Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, https://www.oecd-ilibrary.org/science-and-technology/enhancing-access-to-and-sharing-of-data_276aaca8-en.

industry-led data sharing initiatives, low levels of search and switching,[25] and innovations and products not reaching market. Reviews into the behaviour of Australian and UK banking consumers have shown that consumers have a tendency to remain with one provider for all of their needs in a particular market, despite the presence of other providers offering more competitive products.

The credible threat of regulation has been a driving force behind the data sharing progress made in the electricity and telecommunications sector, which is discussed in section 2.1. Also noted in that section is the role Payments NZ has had in leading the development of open banking in New Zealand. However, banks have made little progress implementing the standards.

In December 2019, the previous Minister for Commerce and Consumer Affairs wrote a letter to the financial sector indicating dissatisfaction with the speed of progress toward achieving open banking, noting that at the current pace, the full benefits to consumers would not be realised.[26] The Minister requested to see urgent progress being made on the development of common standards for APIs and building the APIs to enable a range of products and services delivering value safely and securely for customers. The response from banks and other industry participants was positive, with most indicating that they see greater potential value in increased data sharing for consumers and their own businesses, and expressing a commitment to do the necessary work to implement those standards. Despite this sentiment, we have yet to see significant progress building APIs to the standards amongst the majority of the banks.

As of 31 March 2021, seven of the nine major banks that are Payments NZ members had no indicative timeframes for when they would be ready to provide APIs built to the agreed standards relating to accessing bank account information. Further, as of the same date, there had been minimal implementation of partnerships between API providers and third parties. As a result, this industry led work has not had a material impact on the volumes of data flowing within the sector. Payments NZ is now exploring how it can facilitate these partnerships.

Existing regulatory settings offer consumers limited choice and control over who can access their data and how it can be used. This limits their ability to influence the progression of data sharing initiatives. The degree of influence is further reduced among traditionally vulnerable groups (such as the elderly, disabled, or ethnic and racial minorities), who tend to have low interaction with markets and are among the least able to access products that are accommodative of their needs.

There are a number of underlying reasons why potentially beneficial exchanges are not occurring, or why some of the transfers occurring are not in the best interests of consumers.

Issues contributing to the problem

Competitive constraints are limited by the high transactional costs and complexity associated with transferring data

Competitors require access to consumer data to provide tailored product recommendations, and to product terms and conditions to compete on price and quality. In competitive markets,

[25] United Kingdom Competition and Markets Authority (2016). Retail banking market investigation, Final Report. https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf; Commerce Commission (2020). Mobile Operators should improve consumer choice through easier comparisons. https://comcom.govt.nz/news-and-media/media-releases/2020/mobile-operators-should-improve-consumer-choice-through-easier-comparisons; Electricity Price Review (2019). Final Report. https://www.mbie.govt.nz/dmsdocument/6932-electricity-price-review-final-report.

[26] Hon Kris Faafoi, Open Letter to API Providers, December 2019 Open letter to API Providers regarding industry progress on API-enabled data sharing and open banking (mbie.govt.nz)

consumers should be able to compare the rates and services on offer from different companies with a realistic prospect of being able to move to a new provider if desired.

There are high degrees of friction associated with the access to, and movement of data in New Zealand. At present consumers switch providers at low rates, especially in the financial sector. Businesses perceive the threat of existing customers switching to their competitors as low, which reduces competitive constraints and creates an incentive for them to direct more resource to winning new business than improving the experiences of existing customers.

This is corroborated by investigations from Electricity Price Review and Consumer New Zealand, which found that consumers found it hard to shop around for the right product or service, and subsequently ended up paying more for services as a result. The same barriers exist in other sectors, as corroborated by studies in the telecommunications sector which cite a lack of easy comparison tools, inadequate information and complex product offerings.[27]

It can be a complex undertaking to differentiate between available products to determine which best serves a consumer's needs. There can be a high degree of variability between competing products, making it challenging for consumers to draw meaningful comparisons between offerings. For customers who then decide they want to switch to a product offered by a different provider, this requires further time and effort. In this situation, many will default to choosing an institution with which they already have a relationship, one with which their peers have a relationship, or is well known. That is, consumers tend not to respond to differences in price and quality, because of the onerous process to switch providers.

Research in Australia has consistently found that the time and effort involved in providing information to a competing provider is a significant factor in the observed low rates of switching in the retail banking market. It is reasonable to also attribute the low rates of switching among New Zealand banking consumers to this factor. Similarly, the European Commission identified that difficulties in transferring personal data effectively locks consumers into an application or service, and acts as a barrier to competition.[28] With increasing use of an online provider, the increasing amount of data collected by a provider becomes an obstacle for changing services, even where cheaper, more personalised or more secure offers become available. The costs of change become so high for the consumer that changing providers becomes extremely difficult, and impossible in some cases.

Other impediments to consumers responding to differences in price and quality include the need to rearrange recurring payments and direct debits, and the inability to port bank account numbers between different providers. For example, in electricity and broadband markets, there will be situations in which a customer is locked into a contract and the penalty for breaking the contract is higher than any prospective cost savings under an alternative provider. Higher rates of switching are observed in the New Zealand telecommunications market, relative to other sectors, because of initiatives like mobile number portability (discussed in section 2.1) that promote competition and reduce barriers.

[27] Commerce Commission (2021). Summary of views expressed, consumer representative group workshop, Improving retail service quality for telecommunications consumers. Project no 13.07/16384. (https://comcom.govt.nz/__data/assets/pdf_file/0018/251415/Improving-retail-service-quality-Consumer-workshops-summary-30-March-2021.pdf)

[28] European Commission (2012). Commission Staff Working Paper, Impact Assessment, SEC (2012) 72 final.

High cost of negotiating agreements and transferring usable data

Businesses are aware that the information they hold about their customers, and that misuse of that information, can lead to damage or financial loss. At present, businesses direct the requirements and conditions that third parties must meet before entering into data sharing arrangements. These include terms setting down the third party's obligations in relation to the data. As part of this process, a business must assess each third party to determine the likelihood that the third party will be able to safeguard and securely handle that information, and the risks to the business should the third party fail to do so. This is time consuming and costly for both parties.

Some businesses may use this as an excuse to not share data, or delay the implementation of data sharing initiatives, if they perceive data sharing will reduce their market share.

Equally, third parties that are smaller or new entrants may lack the resources to build the integrations that are needed to connect to multiple institutions. For some, the cost of accessing the data in a manner that facilitates its digital use is prohibitive, if they cannot partner with other third party businesses to spread those costs. This illustrates the value of creating a role for intermediaries, which can build platforms that integrate with data holding businesses and aggregate the data held by those businesses. The intermediary can obtain data in a manner that facilitates its digital use by third parties at lower cost.

Perceived or actual threat of reputational harm from sharing data with third parties

Banks also reported concerns that the sharing of customer data creates reputational risks, as customers may hold the bank responsible if their data is compromised, even if customers approved the sharing of data. This potential reputational risk decreases banks' appetite to share data with less well established, or smaller businesses.

In Europe, the RSA Data Privacy & Security Report, which surveyed 7500 consumers in Europe and the US, found that 62 per cent of respondents said they would blame the company for their lost data in the event of a breach, not the hacker.[29] Of US respondents, 72 per cent said that they would boycott a company that appeared to disregard the protection of their data.

We have also heard that there is uncertainty about where liability would rest if incorrect information is transferred. For example, if a lender relies on incorrect data while assessing a loan application, it is unclear who, if anyone, is at fault. These risks can deter businesses from sharing data with third parties.

Limited data standardisation within markets and adoption of technology to share the data

Standardised processes reduce the cost and improve the efficiency of data exchange processes. One of stakeholders' most frequently cited barriers to the implementation of data sharing was the lack of common data standards, as it creates challenges for the importation of data from other providers. Standardisation of data is a condition for interoperability, which cannot be guaranteed through commonly-used machine readable formats alone.

New Zealand lacks consistently applied data standards and processes for sharing, storing and using information in a digital environment. The identification, authentication and other security measures put in place by companies vary. Legislation and data standards may exist for some sectors but they are found in a variety of places, while some of these requirements are legally binding, some are non-binding guidance or best practice. Consequently, organisations vary in how they manage information, creating inefficiencies and undermining the trust and confidence in the digital identity ecosystem for individuals, the private sector and government agencies.

In the financial sector, a lack of standardisation is causing inefficiencies and fragmentation. The Minister of Commerce and Consumer Affairs' letter to the industry expressed concerns about this, noting:

- providers are using differing standards, meaning third parties are still required to build APIs for each provider they deal with (i.e. the costs associated with bilateral engagement have not been reduced)
- some providers have signalled they don't intend to offer the full scope of standards planned for release by the industry group, meaning some providers which require to access from all banks won't be able to offer their services
- providers are bringing APIs to market at different times
- the costs incurred by providers and third parties using different processes, contractual terms, and security standards, which is time consuming and costly to third parties.

As noted in Section 2.1, Payments NZ has been developing common standards that will help to enable open banking, however there has been little progress in data holders building APIs to these standards. Even when common standards have been developed, data holders may still delay the progress of data sharing initiatives.

Businesses able to unilaterally refuse to share data

Neither third parties nor consumers to whom information relates can compel a business to share information. Third parties must satisfy a business they have the capacity to securely handle data about that business' consumers before a business will consider releasing the information. As such, third parties are entirely dependent on a business' willingness to share information. Businesses are able to unilaterally refuse the provision of any or all of the data they hold to a third party, and are not obliged to provide reasons for the decision to do so.

The ability to unilaterally refuse to share data raises serious competition issues, as it means information flows across the economy are being driven by safeguarding the commercial interests of incumbent businesses, and with the potential to inhibit competition. It is likely that there are ongoing instances of unilateral refusals by business to share data with third parties, though exactly how often this occurs in New Zealand is unknown. There is a perverse incentive on businesses to act in this uncompetitive manner, and little threat to them for doing so.

Consumers report a lack of trust and confidence in sharing their data

New Zealanders are concerned about their online privacy, which can make them less inclined to disclose data or allow it to be shared. In an April 2020 survey, New Zealand's Office of the Privacy Commissioner conducted a survey on New Zealanders' concerns about sharing data and privacy.[30] More than a half of respondents surveyed were concerned about the protection of personal information. Respondents were most concerned about unauthorised sharing of their personal information by businesses, theft of their banking details, and security of their personal information online. Across almost all of these privacy issues, those aged over 60 were more likely to register as 'very concerned' than younger age groups. These findings mirror the conclusions of a 2017 survey conducted by the Office of the Australian Information Commissioner, in which many respondents

[29] RSA (2019). Data Privacy and Security Report. https://www.rsa.com/content/dam/en/e-book/rsa-data-privacy-report.pdf

[30] Office of the Privacy Commissioner (2020). Privacy Concerns and Data Sharing. https://privacy.org.nz/assets/DOCUMENTS/Privacy-concerns-and-sharing-data-OPC-reportApr-20.pdf

reported that they regard Australian financial institutions highly and trust the organisations with their personal information. [31] A majority of people (79 per cent) were uncomfortable with businesses sharing their personal information with other businesses.

The OECD has recognised that individuals are often in a position where they cannot access the information needed to make good judgments about the trustworthiness of organisations seeking consent to collect their personal data.[32] The paper notes that digital economy regulators have an essential role to define safe conditions for data collection, storage, analysis, use, and re-use.

Respondents in the RSA Data Privacy & Security report said that they would be more likely to use a business' products and services if it could prove that it takes data protection seriously.[33] This is consistent with lost security and identity information (passwords, driver licence details etc) being among the top concerns for 76 per cent of respondents.

Although consumers' reported concerns relating to the use and access of personal information are legitimate, it is important not to overstate their significance. It is unclear whether these concerns actually deter consumers from engaging with software platforms, or materially influence the choices they make about product and service offerings. The OECD cites research which found that measures of trust are weak predictors of actual trusting behaviours (the trust paradox), and that what online users do tends to be at odds with what they say.[34] Australian research found that consumers do not translate these concerns into using the basic privacy protections that are available to them (for example, adjusting the privacy settings on a social media account) and continue to divulge information to organisations and governments.[35] We also note that consumer preferences adapt over time, and while consumers might be sceptical of new technology, privacy concerns may reduce over time as data portability becomes normalised.

Regulatory gap: initiatives prioritised and pursued at discretion of businesses

The data sharing initiatives being progressed in the banking and financial sector do not have the express aim of improving consumer empowerment and autonomy over their personal information, and businesses have absolute discretion over which initiatives to develop and adopt. By contrast, in the telecommunications and electricity sectors, the regulator has directed service providers to progress data sharing initiatives with the goal of improving consumer outcomes.

This has resulted in the progression and adoption of data sharing initiatives that, rather than being aligned with the best overall consumer outcomes, deliver benefits within, but not across, organisation boundaries. This may be because they allow for the outsourcing of the organisation's compliance requirements, for example, ANZ's partnership with BUD.

Anecdotal feedback from MBIE's consultation on regulating merchant service fees highlighted a perception that Payments NZ may not be entirely independent. Its members' interests (banks and

[31] Office of the Australian Information Commissioner (2017). Australian Community Attitudes to Privacy Survey report. https://www.oaic.gov.au/engage-with-us/research/2017-australian-community-attitudes-to-privacy-survey/report/.

[32] OECD (2021). Working Party on Measuring the Digital Economy, Working Group paper, Measuring trustworthiness of digital environments and new technologies.

[33] RSA (2019). Data Privacy and Security Report. https://www.rsa.com/content/dam/en/e-book/rsa-data-privacy-report.pdf

[34] OECD (2021). Working Party on Measuring the Digital Economy, Working Group paper, Measuring trustworthiness of digital environments and new technologies.

[35] Office of the Australian Information Commissioner (2017). Australian Community Attitudes to Privacy Survey report. https://www.oaic.gov.au/engage-with-us/research/2017-australian-community-attitudes-to-privacy-survey/report/.

other financial institutions) can be in tension with the best outcomes for the end users/consumers of those institutions. Further constraints on the effectiveness of this industry-led work is the voluntary nature of the API initiatives, and the discretion banks have to cherry pick which initiatives to adopt. In addition, the API standards do not regulate the fees that banks can impose on third parties for access to the personal data they hold, meaning imbalances in negotiating pricing and access persist.

Data analytics has the potential to harm customers

Data sharing is expected to contribute to a rise in data analytics, as a result of the more widespread availability of information. The use of machine learning algorithms to conduct risk assessments and make associated decisions relating to credit and insurance has many benefits, but also comes with the risk of unintended or undesirable consequences.[36] These can include bias or errors, which may in turn contribute to inadvertent discrimination and financial exclusion. For example, in insurance, it may lead to the exclusion of people who are deemed to carry risks of a certain nature. There are also potential consequences for consumers who choose to opt out of data sharing, such as risks of being excluded or receiving less advantageous pricing. Currently, there is no purpose built regulatory framework to manage these risks.

Statistics New Zealand has developed an Algorithm Charter 2020 which commits government agencies to carefully manage how algorithms will be used, to strike the right balance between privacy and transparency, prevent unintended bias, and reflect the principles of the Treaty of Waitangi.

Consumers lack the confidence and capability required to change providers and assess options

The various market reviews (discussed above) found that consumers tended to remain with their current providers, even where they were paying too much for a product, because of the multiplicity of barriers that exist to accessing and accessing information about different offerings, making informed decisions on the basis of that information.[37] This also suggests that consumers are often unable to represent their interests in the market and influence the direction of innovation to outcomes that would deliver the greatest benefits to consumers.

Gaps in consumer knowledge about their rights and accessibility of schemes

Research suggests that there are many circumstances in which a consumer will not pursue a breach involving their personal information. These behaviours are driven by a lack of capability and knowledge, among other factors. A survey on online privacy conducted in Australia indicated that only a half of responds were able to identify an organisation which they were aware they could report the misuse of information to.[38] Further, the research showed there was a clear lack of understanding about what kinds of misuses of personal information could be complained about.

---

[36] OECD (2020). Financial Consumer Protection Policy Approaches in the Digital Age: Protecting consumers' assets, data, and privacy. www.oecd.org/finance/Financial-Consumer-Protection-Policy -Approaches-in-the-Digital-Age.pdf.

[37] Commerce Commission (2020). Mobile Operators should improve consumer choice through easier comparisons. https://comcom.govt.nz/news-and-media/media-releases/2020/mobile-operators-should-improve-consumer-choice-through-easier-comparisons; Electricity Price Review (2019). Final Report. https://www.mbie.govt.nz/dmsdocument/6932-electricity-price-review-final-report. United Kingdom Competition and Markets Authority (2016). Retail banking market investigation, Final Report, 2016. https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf.

[38] Office of the Australian Information Commissioner (2017). Australian Community Attitudes to Privacy Survey report. https://www.oaic.gov.au/engage-with-us/research/2017-australian-community-attitudes-to-privacy-survey/report/.

This suggests that consumers are not equipped to seek to uphold their rights in current data exchange practices, which is an undesirable outcome from a consumer protection perspective.

Problem 2. Methods of data exchange are sometimes insecure

Background

The transfer of personal data from one provider to another creates security and privacy risks, which have the potential to cause physical harm, emotional distress, and financial and reputational loss to consumers and businesses alike, where data transfer is compromised. The limits of the regulatory regimes already in place are discussed in section 2.2 (above, 'Regulatory systems already in place, and connections to on-going work').

In terms of digital security risks, data sharing typically requires opening information systems so that data can be accessed and used by legitimate users or third parties. This increases the risk of data breaches, because the more accessible an individual's personal data, the greater the likelihood that information can be accessed and shared inappropriately by a third party. Data sharing can also expose potential vulnerabilities in an organisations information systems.

Digital security is an increasingly important issue for all governments and industry sectors as the likelihood and severity of digital security incidents has grown in recent years.[39] The financial services sector is particularly at risk of digital security incidents, because of the potential value of the data and information stored by service providers.

Methods of obtaining and transferring data are sometimes insecure, and expose consumers to unnecessary risks. The reasons for this are discussed below.

Issues contributing to the problem

Regulatory frameworks are fragmented, limited in scope and not fit for purpose

In section 2.2, we discussed the limitations of the Privacy Act in giving consumers an effective right to access their data (particularly where this relates to seeking data in a form that enables a consumer to make further use or understanding of the data). Key limitations of that Act include it does not allow consumers to prescribe the form in which data must be provided in detailed terms, it is based on broad authorisations (meaning consumers are unlikely to be fully aware of how much data is being collected about them or how it is being used), it does not have an express requirement for consents to expire after a defined period of time, and does not require data holders to notify an individual when their information is shared with a third party.

That section also canvases the fragmented nature of the other applicable regulatory systems in this space. For example, while regulators in the electricity and telecommunications sectors have powers that allow them to mandate certain forms of data portability which apply to intra-sector data exchanges, none of those systems were designed with data portability in mind, which limits their ability to respond to the cross-cutting nature of issues that can arise. It also means no single body has regulatory oversight and responsibility for governance of data portability settings in New Zealand.

The remainder of the regulatory framework in this area is fragmented.

Other methods of data transfer are not regulated, and give rise to security concerns. For example, Fintech data sharing initiatives have emerged with business models that rely on 'screen scraping'

[39] OECD (2020). Financial Consumer Protection Policy Approaches in the Digital Age: Protecting consumers' assets, data, and privacy. www.oecd.org/finance/Financial-Consumer-Protection-Policy -Approaches-in-the-Digital-Age.pdf.

technology to access consumers' data from their existing banking accounts. Screen scraping is a computer software technique for extracting information that is shared on websites. In practice, this involves a third party (e.g. FinTech or data aggregator) using a customer's access credentials (e.g. internet banking username and password) to access information about a consumer stored on a website (e.g. bank accounts). Data is 'scraped' from the online interface.

Screen scraping poses security concerns for a variety of reasons:

- *There are no practical limits on the data collected*: the technique downloads much more information than is needed simply because the information is available (they take the whole page, even if they just want a line item because that's what they have access to). We note that this practice may be inconsistent with IPP 4, which in effect, requires parties to collect and hold the minimum amount of data required to fulfil their purpose.
- *Consumers compromise the security of their data and their privacy*: Many consumers are unaware that when they provide their authentication information (e.g. debit card information) to a screen scraping software, this may breach the terms and conditions on which the bank has provided the debit card which generally prohibits the disclosure of credentials and passwords to third parties. There is an open question about whether this absolves the bank from liability if the credentials are compromised. In Australia, the legal position regarding liability for the consequences of providing account login details to a 'screen scraper' is unclear.[40]
- *The 'scraped' data is more vulnerable to a security breach*: the information being scraped is often passing from banks to smaller / newer organisations that may not have comparable information security infrastructure to securely store customer information (because these organisations tend to not be subject to prudential obligation in the same manner as banks), meaning the information is at heightened risk of a hacking or security breach.

In Australia, the Farrell Review found that in some cases, the way in which a request for a customer's bank credentials was made meant that customers were not aware that they had given their login details to someone other than their bank.[41]

'Download' methods of data sharing (of which screen scraping is one) do not allow for data holders to impose standards over the data being obtained. This includes the identity of the user, the scale and scope of the data used, and the extent to which the information derived from the data could reveal sensitive or personal information. These methods expose consumers to a multiplicity of risks. Whereas APIs are built to standards that specify who can access the data, the kinds of data that can be accessed, and the volume that can be transferred. Accordingly, data transferred through such applications is more likely to be secure against attack or interception. It is unclear whether screen scraping is a less costly way of third parties collecting data, relative to APIs. Either way, it is likely that the widespread uptake of screen scraping has been driven by a lack of alternative, effective technologies that enable third parties to extract customer data.

The sharing of data raises a range of questions about expectations and entitlements to privacy, such as the point in time at which the privacy assumptions implicit in the initial use of data stop

[40] Farrell, Scott. (2017) Report of the Review into Open Banking. https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf.

[41] Farrell, Scott. (2017) Report of the Review into Open Banking. https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf.

applying in subsequent uses.[42]

Gaps in redress and liability: unavailability of remedies for loss suffered

Unregulated methods of data sharing, like screen scraping, have raised murky questions around liability in other jurisdictions.[43] In Australia, businesses have reported uncertainty about whether and the extent to which original data holders remain liable for misuses or the poor implementation of safeguards by the data recipient. In New Zealand, if the data is personal information, the individual would likely have recourse under the Privacy Act. However, there may still be some uncertainty on the part of consumers as to which party is liable if an individual suffers a loss due to an insecure data exchange. We also understand that consumers may often seek recourse from the original data holder, rather than the third party accessing the data. To date, we are not aware of any data breaches that have occurred as a result of information collected via screen scraping in New Zealand.

While specialised dispute resolution schemes already exist in many sectors, for example, banking utilities, and telecommunications, their jurisdictional mandates are limited. Some stakeholders pointed to scenarios in which a consumer would have no recourse to any dispute resolution scheme because of the clear limits on their jurisdiction. For example, the Utilities Disputes Scheme has no ability to compel a service provider to adopt a particular process for handling or storing information. Equally, during consultation it was noted that there could be issues for which multiple bodies have overlapping jurisdiction.

Consumers are not well equipped to give consent or make privacy assessments.

The Privacy Act (IPP 3) requires agencies to take reasonable steps to ensure that the individual concerned is aware of a number matters, including the purpose for which information is being collected and the intended recipients of the information. Research conducted for the UK Financial Consumer Panel found that in many cases consumer consent was not well informed, with most people either not reading terms and conditions or privacy notices, or not understanding them if they did.[44] Research found that consumer consent is unlikely to effectively protect them from harm. They also found that consent cannot be regarded as 'informed' when it is based on long and complex contractual terms. Although New Zealand's Privacy Act is not premised on the notion of consent, parallel concerns arise about the ability of consumers to genuinely and meaningfully manage and limit the terms on which their information is accessed and used.

Even if the consumer is aware of how information will be used, relying on users to make security assessments is a fairly onerous burden for the average consumer. A majority of consumers are not well placed to assess a third party's privacy or security standards. Given the sensitivity of information about individuals that is collected, and the limits in consumer capability, there is a case for applying higher protections and obligations on entities that handle data.

[42] OECD, Working Party on Data Governance and Privacy in the Digital Economy (2021). Data Portability: Analytical Report, Mapping data portability initiatives and their opportunities and challenges. DSTI/CDEP/DGP(2021)1.

[43] Farrell, Scott. (2017) Report of the Review into Open Banking. https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf.

[44] Financial Services Consumer Panel (2018). Consumer Panel Position Paper: Consenting adults? Consumers sharing their financial data. https://www.fs-cp.org.uk/sites/default/files/final_position_paper_-_consenting_adults_-_20180419_0.pdf.

Problem 3. New participants locked out of markets

Background

The "cold start problem" describes the difficulties new digital product or services entrants face in drawing high quality inferences about customers due to the lack of data.[45] We see evidence of non-incumbent providers and new entrants struggling to attract customers away from incumbent firms and increase their market share, especially in the banking and finance sector. This is corroborated by the fact that consumers have a tendency to remain with their existing provider, even in the presence of more competitive deals elsewhere (illustrated by the Commerce Commission's telecommunications market study findings). We have also been told that some businesses have chosen to leave the New Zealand market due to high barriers to entry and expansion, driven by an inability to access data.

There are several factors contributing to the high barriers to entry for new participants.

Issues contributing to the problem

Incumbency advantages, arising from market power and information asymmetries, create commercial disincentives to sharing data

Incumbent providers have market power over their existing customers and in some markets, such as banking, they have systemic importance. The Australian and UK reviews into their retail banking sectors similarly found that existing providers benefit from strong incumbency advantages. These incumbency advantages are present in many markets but may be more pronounced in markets with a high differentiation in the concentration of power.

Incumbents are able to use the data they hold about their customers for the business' exclusive benefit, for example, to gain insights about a consumer's preferences and needs or to develop targeted marketing or advice, which puts non-incumbent providers and new entrants at a significant competitive advantage. The ability of competing providers and new market entrants to attract customers from incumbent firms depends on their being able to assess the suitability of prospective customers and offer products that suit their needs at more competitive prices. The difficulties associated with acquiring information about a customer from their existing provider put competitors and new entrants at a disadvantage.

Consumers similarly require information about competitor offerings to make better decisions and seek out products that are well suited to their circumstances. The various market reviews (discussed above) found that consumers tended to remain with their current providers, even where they were paying too much for a product. This is because of the multiplicity of barriers that exist to access and accessing information about different offerings, and making informed decisions on the basis of that information.[46]

Information asymmetries, market structure, and a lack of transparency combine to give incumbent providers a significant competitive advantage in many markets. In turn, these factors coalesce to

[45] OECD, Working Party on Data Governance and Privacy in the Digital Economy (2021). Data Portability: Analytical Report, Mapping data portability initiatives and their opportunities and challenges. DSTI/CDEP/DGP(2021)1.

[46] Electricity Price Review (2019). Final Report. https://www.mbie.govt.nz/dmsdocument/6932-electricity-price-review-final-report. Commerce Commission (2020). Mobile Operators should improve consumer choice through easier comparisons. https://comcom.govt.nz/news-and-media/media-releases/2020/mobile-operators-should-improve-consumer-choice-through-easier-comparisons; United Kingdom Competition and Markets Authority (2016). Retail banking market investigation, Final Report, 2016. https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf.

create strong commercial disincentives on incumbent providers to share data, create barriers to entry for new participants in many markets.

Lack of transparency in pricing, access, quality of available products and services

The pace at which innovation occurs depends on the accessibility of information about existing products and services within a market. During consultation, many stakeholders expressed views about the lack of transparency in the pricing, access to, and information about the quality of available products and services. There were concerns that the lack of transparency contributes an uneven playing field which entrenches the position of incumbent providers. This is because competitors are required to engage in bilateral engagement to access the information they require to compete and innovate, which is a costly exercise.

Beyond product disclosure statement obligations, there are few obligations on businesses to make available product data or requirements as the way in which that data must be provided. The Electricity Authority has required retailers to make available information about generally available tariffs, and the telecommunications regulator is looking to follow suit.

The format in which data is shared can influence its competitive impact. Start-ups and new entrants tend to have access to limited resources to devote toward the processing and extrapolation of data, relative to incumbent service providers. There are no obligations on incumbents to provide data in a format that facilitates its digital use, and some stakeholders reported receiving information in a form that was difficult to use. In the current environment there is an incentive for incumbents to share data in a format that has low utility or accessibility to their competitors, as a means of preserving their competitive advantage and inhibiting innovation.

Businesses able to unilaterally refuse to share data

As previously discussed, we expect that the ability of businesses to unilaterally refuse to share data is preventing beneficial data exchanges from occurring. If this uncompetitive activity is occurring at significant levels, it risks affecting the system as a whole.

Nature and scale of harm and loss experienced as a result of these problems

New Zealand is missing out on innovative products and services (i.e. economic and social benefits) that rely on the exchange of consumer data

Presently, the uneven level playing field in various markets restricts the development of the market as a whole. High barriers to entry put new entrants and external businesses at a competitive disadvantage, preventing them from competing to provide (competitive and over the top) products and services. Coupled with the small size of the domestic market, stakeholders reported that the barriers to entry in New Zealand are causing some new entrants to bypass the market altogether. We expect there will be a continued trend of existing players exiting the market in favour of offshore markets where the scale of benefits are greater and the regulatory settings seek to level the playing field and increase competitive constraints, rather than being heavily tilted in favour of incumbent firms.

Reduced competition, coupled with the lack of standardisation and coordination, cost of bilateral negotiations, and high degree of economic friction associated with the movement of data are likely to result in a loss of innovation in New Zealand, which hampers economic growth.

Poor consumer outcomes because of regulatory gaps and market barriers

Lower levels of innovation means that consumers have fewer products, services, and providers from which to choose, which can preclude them from realising improvements to their customer

experiences. An abundance of evidence from across the economy suggests that New Zealand consumers and businesses could be getting a better deal on the services and products they are using, from banking to telecommunications. This occurs because many consumers lack the information and capability needed to make informed comparisons, and because the difficulties in transferring personal data effectively lock consumers into using a particular application or service.

Consumers' autonomy over their data is undermined by the inability of many to give informed consent, and challenges in accessing information held digitally in a form that is reusable by the consumer or a third party.

Poor outcomes are likely to be particularly acute for these consumers with lower education or on lower incomes.[47] These consumers tend to have fewer interactions with the market, meaning they exert weaker market forces and innovation is less likely to be responsive to their needs.[48] This feedback loop perpetuates poor outcomes for those consumers, who are more likely to remain locked into contracts with providers offering products or services that are not well suited to their needs. It follows that reducing asymmetries has the potential to significantly improve consumer outcomes, particularly in the banking sector, and particularly for certain vulnerable groups.[49]

Evidence suggests that, rather than occurring in a way that seeks to maximise consumer benefit or enhance the customer experience, innovation is predominantly driven by a desire to protect the commercial interests of incumbent providers.

2.5 Stakeholder views

Who are the stakeholders and what is the nature of their interest?

There are multiple groups of stakeholders with varying interests:

- businesses that hold data about consumers or themselves
- individuals and business consumers
- third party entities that wish to access consumer data for innovative purposes – alternative products, services, and business models e.g. FinTechs
- government departments with an interest in data portability or interoperability initiatives
- regulators with responsibility for the performance of markets that will, or are likely to be subject to a CDR designation

What consultation has already taken place and with whom?

In August 2020, MBIE released a public consultation document "Options for establishing a consumer data right in New Zealand" which sought feedback on whether there was a case for introducing a CDR in New Zealand and the different approaches to data sharing available. We

[47] United Kingdom Competition and Markets Authority (2016). Retail banking market investigation, Final Report, 2016. https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf.

[48] United Kingdom Competition and Markets Authority (2016). Retail banking market investigation, Final Report, 2016. https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf.

[49] Farrell, Scott. (2017) Report of the Review into Open Banking. https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf.

received 59 submissions from a wide range of stakeholders including business from various sectors, Crown entities, and advocacy groups.

In addition, we have had ongoing meetings with a range of stakeholders that represent a range of interests, including large commercial banks, energy providers, electricity retailers, and FinTechs.

Key themes from the submissions, and how the consultation has affected the policy proposals, are discussed in the Options identification section.

Consultation with Māori and the nature of their interests

When considering the design principles that would form part of a New Zealand framework for a CDR, officials began examining the nature of Māori interest in data and data sovereignty. In some interpretations of te ao Māori, information is tapu (sacred) and the association of information to a person gives in mauri (life force). This viewpoint advocates for increased protections and governance over Māori data, due to the significance and preciousness of data.

To understand the impact and intersection of this interest with the consumer data framework better, a question was included in the consultation document which asked submitters how, in their view, Te Tiriti o Waitangi should shape the introduction of a CDR in New Zealand.

Many submissions expressed support for inclusion of the Treaty principles in the scheme. Some went further by suggesting data sovereignty and tino rangatiratanga be embedded in the creation of a CDR, including its component parts, to create a framework that reflects a te ao Māori approach to data. In particular, they emphasised consent and privacy related aspects of the CDR framework. It should be noted this was not specific consultation with Māori.

There is a question of whether consumer data and the potential Māori interest falls under Article 2 of Te Tiriti (protection of taonga) or Article 3 (ordinary rights of citizens).

Further consultation is planned

We intend to continue to consult with interested members of the various stakeholder groups as the policy development process progresses to inform future Cabinet decisions. This will include engagement with Māori consumers and Māori businesses to develop an understanding of the particular benefits and risks a CDR framework poses, as well as the nature of the Treaty interest, to inform the CDR frameworks detailed design.

Objectives sought in relation to policy problem

What are the objectives or outcomes?

The overall objectives for establishing a CDR are to improve consumer experiences and outcomes, and to deliver economic benefits to New Zealand.

This requires that the regulatory system:

- improves the value and utility of consumer data by giving consumers meaningful control over their data
- creates opportunities for beneficial innovation in products, processes, and business models, resulting in greater choice and convenience for consumers
- enables healthy competition between incumbents and new entrants or competitor providers

through the use of consumer data

- ensures that consumer data is secure and protected, without imposing unnecessary costs on participants

is cost-effective, balancing compliance burden against the need to incentivise businesses to collect data

Criteria used to evaluate options against the status quo

The criteria we use to evaluate the options are:

- Trust and confidence – consumers can trust the ability of system participants to handle their data securely and ethically, and that recourse exists where data is misused in a way that causes consumers to suffer loss.
- Efficient and fair – distribution of costs and compliance burden allow for entry to and expansion of markets and encourages competition, while being proportionate to potential risks.
- Scale and potential reach – empowers consumers to participate in data portability and grants them meaningful control over their data, supports variety and speed of innovation, delivers benefits that span organisational and sector boundaries, is able to adapt effectively to future innovation.
- Certainty, predictability, transparency – the settings which allow for tailored and flexible approach to data sharing in markets, while giving system participants clarity about their obligations.

The criteria are equally weighted. They are materially similar to the criteria that were used in the 2020 consultation paper of which submitters were broadly supportive. Feedback on the consultation paper included comments that a clearer articulation of the problem definition was required. We have since refined the problem definition. It was necessary to refine the criteria to better reflect the objectives we are seeking to achieve, desirable regulatory design characteristics, and assess the extent to which each proposal would be effective in overcoming the current barriers preventing data portability. The criteria were also refined to better allow us to take into account the experiences of other jurisdictions, for example, the 'scale and potential reach' criterion allows for an assessment of whether a particular model could be rolled out across the entire economy or would be limited in reach.

There are trade-offs to be made in weighing up the options against the criteria. For example, more stringent security requirements for data handling may come at expense of reduced entry or ability to participate for smaller players.

The options considered in this RIS are analysed against these criteria, using the status quo as a baseline.

Section 3: Options identification

What options are available to address the problem?

Summary of options

The following options have been identified to address the problem discussed in Section 2. We have organised the options into three broad categories.

1: Types of data and functionality under a CDR
Option 1.1: Personal Information only
Option 1.2: Include information about entities as well as individuals
Option 1.3: Exclude 'derived data'
Option 1.4: Include 'product data'
Option 1.5: Provide for 'action initiation'
2: Options for regulatory approach
Option 2.1: Economy-wide, principles-based approach
Option 2.2: Sector-specific regulation
Option 2.3: Sector-designation approach
3: Options for components of a regulatory framework
Option 3.1: Accreditation regime
Sub-option 3.1a: Tiered accreditation regime
Option 3.2: Safeguards to ensure trust and confidence
Option 3.3: Enhanced consent framework
Option 3.4: Shared data standards

Status quo / counterfactual

As discussed in Section 2.3, barriers to achieving data portability across the economy are likely to persist in the absence of intervention. This forms the status quo for the purposes of this regulatory impact statement.

All options have been assessed by reference to the status quo as a baseline, against the criteria identified below.

Are these options mutually exclusive?

The options have been organised into these three broad categories as it will be possible to select option(s) from each category. Within each category we have noted where options are mutually exclusive

Relevant overseas experience

Several countries have regulated to provide for or improve existing rights of consumers to access, share and use their data to their advantage. Among those, Australia, the European Union, and the

United Kingdom have adopted different approaches to achieving data portability. There is still a paucity of quantitative evidence about the effectiveness of the various approaches. Further, the impact of each will be influenced by the regulatory culture and environment.

The range of options developed for these proposals have been drawn from the measures implemented in other jurisdictions, and take into account evidence available about the effectiveness of those measures.

Non-regulatory options

Non-regulatory options have not been discussed, because, as discussed in section 2.3:

- the level of benefit to consumers by industry-led initiatives is likely to be modest
- the initiatives progressed by industry are likely to be those that offer the greatest benefit to the organisation rather than being aligned with best consumer outcomes
- these are unlikely to deliver benefits that span organisation boundaries or sectors of the economy, and
- strong commercial disincentives to data sharing mean progress on initiatives is likely to continue at a slow pace and to only occur in some parts of the economy.

Given that industry-led initiatives have the potential to deliver moderate benefits to some consumer groups, decisions taken on the design of a CDR should not prevent these options from being progressed in parallel to regulatory intervention and where possible, should seek to leverage, or at a minimum complement, that work.

Options not considered at this stage

Some regulatory tools have been carved out of this RIS and will be assessed in a second RIS later in 2021. These include regulatory and governance arrangements, funding, the liability and compliance framework, and consumer redress mechanisms.

1: Types of data and functionality under a CDR

Options 1.1 to 1.4 relate to the types of data that could be included in a CDR, while option 1.5 relates to the functionality that could be enabled. Options 1.1 and 1.2 are mutually exclusive. The remaining options are not mutually exclusive, and any suite of options could be combined with either option 1.1 or 1.2.

Options 1.1 and 1.2 will define the "consumers" whose data can be shared under the CDR (i.e. whether the CDR relates to individuals alone, or individuals and other entities such as businesses).

The data that businesses hold about consumers (**consumer data**) fall into three broad categories:

- **provided data** is data which the customer has provided to the data holder (e.g. contact information)
- **observed data** is data which the data holder has observed about the customer (e.g. transaction or usage history)
- **derived data** is data which has been derived from provided or observed data (e.g. an account balance or a credit score based on a customer's transaction history).

Option 1.3 relates to excluding derived data from the CDR. Option 1.4 relates to including information about products offered by a business, such as interest rates or fees, in the CDR (**product data**). These options have been discussed in terms of the marginal impact over and above option 1.2.

Option 1.5 relates to the functionality that could be enabled through a CDR. It has been discussed in terms of the marginal impact over and above enabling 'read access' under options 1.2 to 1.4. The extent of benefits, costs and risks will depend on the other options discussed in this RIS.

Option 1.1: personal information only

Under this option data that relates to readily identifiable individuals would be subject to the CDR, but data relating to entities such as businesses or trusts would not be. In effect, this would cover the same data that is currently treated as 'personal information' for the purposes of the Privacy Act 2020. This is a similar approach to that taken under the GDPR.

This option is mutually exclusive to option 1.2.

Benefits - How will this option address the problem or opportunity? How will this option deliver the identified objective(s)?

This option would make it easier for individuals to access or share their data. This could reduce switching costs for consumers, and partially reduce search costs by being able to share data with comparison tools. In turn, this would promote innovation and facilitate greater competition.

It would align with existing privacy legislation which would benefit businesses that currently have systems and processes in place relating to their handling and storage of personal information about their customers. Some submitters, who generally viewed data-portability as strengthening existing privacy legislation, favoured this approach.

Costs and risks

This option would impose costs on businesses that hold data about individuals, though the extent of those costs will vary as outlined elsewhere in this paper. Consideration of how information relating to multiple individuals (i.e. a joint bank account) should be treated will be necessary.

Unlike option 1.2, limiting the CDR to personal information means it would not apply to legal entities, such as businesses (including small businesses) and trusts. There is an opportunity cost associated with excluding businesses, which is discussed in more detail below. This could result in the potential benefits of the CDR being somewhat muted.

Option 1.2 Include information about entities as well as individuals

Under this option data that relates to entities such as businesses would also be subject to the CDR. In effect, any end-user of a good or service would be able to request that their data be shared with a trusted third party.

Benefits - How will this option address the problem or opportunity? How will this option deliver the identified objective(s)?

This would extend some of the consumer-benefits associated with a CDR to businesses, including small-businesses. In particular, this could reduce search and switch costs, make it easier for small businesses to obtain capital or debt, and simplify accounting practices. Increasing the scope in this way would increase the overall impact of the CDR.

Submitters noted that many small businesses often do not have sufficient bargaining power and face some of the same issues as consumers in negotiating deals (e.g. for lending or utilities) so giving them access to their data through the CDR could provide significant benefits.

Costs and risks

The costs associated with this option are similar to those in option 1.1, though it is unclear whether there will be significant additional costs associated with including data about entities in the CDR. Some submitters suggested that these costs would be significant, while others suggested that they would only be marginal. For example, there is some additional complexity and risk that may be associated with including data about entities, including the ability to obtain consent when there may be multiple account holders. However, these complexities also exist in relation to information held by individuals, such as individuals that hold a joint account, and could be addressed by providing for nominees to consent to data being shared or through guidance.

Option 1.3 Exclude 'derived data'

This option would exclude derived data from the CDR so that those who hold it would not be required to share it in a machine readable format. If the derived data related to an identifiable individual, it would still be treated as personal information and subject to the Privacy Act, so data holders may still be required to provide it to the individual concerned.

An alternative option, which is discussed further in Section 3.2, would involve excluding derived data on a case-by-case or sector-by-sector basis. This is the approach taken in the ACDR where derived data is included in the overarching primary legislation, but a subset of it was excluded in the banking designation.

The ACDR designation for the banking sector excludes "materially enhanced" data, meaning that entities otherwise required to share data are not required to share materially enhanced data. This distinction was drawn because some forms of derived data might be materially enhanced through the use of insights or analytics (e.g. an assessment of a person's ability to service future loan repayments) while others might not require the application of analytics (e.g. determining a person's age based on their date of birth). Materially enhanced data is also known as 'value-added' data, as the data holder has increased the value of it.

In Singapore, the yet-to-commence data portability requirement gives data holders ('porting organisations') the ability to choose not to transmit certain types of data, including derived personal data or other data that may be commercially sensitive.

Benefits - How will this option address the problem or opportunity? How will this option deliver the identified objective(s)?

Excluding derived data from the CDR could help to strengthen intellectual property rights and incentivise innovation. In some cases, derived data could be commercially sensitive and requiring it to be shared in a machine-readable format could allow another party to determine the method for creating the data, undermining the original data holder's intellectual property rights. If derived data is included in the CDR, it could deter businesses from developing new methods of analysing data in the provision of products or services, which could have flow on impacts for consumers.

Many submitters supported this view and advocated for derived data to be excluded from the CDR.

Costs and risks

If derived data relates to an identifiable individual it will likely be considered 'personal information' for the purposes of the Privacy Act. This means that individuals would still be able to request access to this data under the Privacy Act, even if it was excluded from the CDR. Some submitters, including the Office of the Privacy Commissioner, suggested that this was a reason to incorporate derived data in the definition of a CDR to ensure the consistent treatment of consumer data and allow consumers to benefit from their derived data.

While including derived data might deter businesses from developing innovative tools that utilise consumer data, an outright exclusion of derived data might have a similar impact as it could result in a lack of innovative tools being developed that use derived data. It may also reduce the ability for consumers to access information which is strictly 'derived data' but has not been materially enhanced by the data holder. This may adversely impact the control that consumers have over their data, and undermine trust and confidence in the CDR.

Option 1.4 Include 'product data'

Under this option, the CDR would apply to 'product data' as well as 'consumer data' as described above. That is, data that relates to the products and services offered by businesses. For example, this could include information about the offering, terms and conditions, price and charges associated with certain products.

Benefits - How will this option address the problem or opportunity? How will this option deliver the identified objective(s)?

While this information does not relate to an identifiable individual or entity, it will increase the value proposition of a CDR. It will allow consumers to easily and accurately compare products and services from multiple suppliers and, when coupled with consumer data, will make it easier to determine where customers may be able to get a better deal. It will provide greater transparency, as the information may not otherwise be readily available or easily comparable. This will be particularly beneficial in sectors where there are high search and switch costs or where product comparisons are inherently complicated.

These benefits are likely to lead to further benefits in the form of increased competition which could lead to a reduction in costs, or increased innovation, as businesses seek to differentiate their offerings.

Costs and risks

This would impose costs on businesses that would be required to make information available about their products and services. The scale of these costs will vary greatly depending on the scope of the CDR. Similarly, there will be a cost to government in determining what information is required to be shared and the manner in which it must be shared.

Some submitters raised a concern that including product data could deter innovation by product suppliers which may focus their attention on scoring favourably on certain metrics (i.e. charging low fees) rather than improving their product offering. We consider that this could be addressed through the development of the detailed requirements.

Option 1.5 Provide for 'action initiation'

Under this option, the CDR would allow third parties to create new data or initiate an action based on the data received if directed by the consumer to do so. This is referred to as 'action initiation' or 'write access'.

In a practical sense, read access could allow consumers to view accounts held with multiple providers, while action initiation could allow a third party to move money between those accounts (on the consumers' consent).

Benefits - How will this option address the problem or opportunity? How will this option deliver the identified objective(s)?

Providing for action initiation will unlock many more of the possible benefits associated with a CDR. For example, read access will allow consumers to compare products from multiple providers, and action initiation will allow the consumer to apply for an account with a new provider. Submitters noted that this will reduce switching costs, increase innovation and facilitate competition. It could particularly benefit new entrants or smaller incumbents to improve their market share and ability to compete by attracting new customers which otherwise might not have moved to their service due to switching costs.

Within the payments sector, action initiation could allow for new methods of payments to emerge. This could benefit consumers and small businesses by providing for more convenient, cheaper payment solutions, which could in-turn provide competitive constraints for existing providers.

Without the ability for third parties to initiate actions the potential use cases of a CDR are significantly reduced. In Australia, the CDR has been limited to read access to date, but the recent Inquiry into the Future Direction of the CDR recommended that it be broadened in scope to enable action orientation.[50]

Costs and risks

Submitters noted that providing this additional functionality increases the cost for data holders' businesses operating in the regime and potential risk. It would be necessary to provide some additional safeguards to mitigate the risk of consumer harm that could result from a third party fraudulently carrying out actions on a consumer's account, and reduce the costs for businesses in verifying the validity or requests. For example, businesses would need to find new methods of opening a new account with a request that has been made by a third party on the consent of a consumer, and not directly from the consumer themselves.

It is difficult to assess the marginal costs and risks associated with this option over and above the options discussed in this paper. Further, these risks may be mitigated, in part, through the additional safeguards discussed in Section 3.3.

[50] Future Directions for the Consumer Data Right (2020) Inquiry into Future Directions for the Consumer Data Right - Final Report | Treasury.gov.au

1: Impact analysis: Types of data and functionality under a CDR

		Criteria				
		Trust and confidence	**Efficient and fair**	**Scale and potential reach**	**Certainty, predictability, transparency**	**Overall assessment**
	Status quo	**0** N/A	**0** N/A	**0** N/A	**0** N/A	N/A
Options identified	**Option 1.1: Personal information only**	**0** This option will have a negligible impact on trust and confidence.	**+** Compliance costs will be minimised for data-holders by aligning the definition of CDR data with that used in existing privacy frameworks.	**+** Benefits of any CDR will only be realised by individual consumers, and businesses that serve them. The inclusion of derived data may adversely impact innovation unless it was explicitly excluded.	**+** Participants and consumers would have clarity around what data is within scope of the CDR. Further, the definition will align to existing privacy frameworks which could increase the predictability.	**+** Alignment with existing privacy frameworks would increase certainty for participants, but the narrower scope would likely limit the potential wider economic benefit of a CDR.
	Option 1.2: Include information about entities and persons	**0** This option will have a negligible impact on trust and confidence.	**++** There may be additional costs associated with incorporating data about entities, though it is unclear what the extent of this will be. Some submitters suggested they would be significant, others suggested it would be marginal. However, given the additional benefits associated with allowing businesses and other entities to access their data, any additional costs will be justified.	**++** Will significantly broaden the potential scale and reach of a CDR by including data sets about businesses and other entities. In particular, Small-Medium Enterprises will stand to benefit as they suffer some of the same power imbalances as individual consumers.	**0** Would provide some certainty to participants and consumers, though the misalignment with existing definitions could lead to some confusion and additional complexity.	**+/++** There would be some additional cost and complexity associated with this option, but these are likely outweighed by the additional benefits of allowing businesses (particularly SMEs and trusts) to participate in the CDR. This option is therefore favoured over option 1.1
	Option 1.3: Exclude derived data	**0** This option will have a negligible impact on trust and confidence.	**0** As this data is not typically made available in a machine readable format currently, although generally stored in a machine readable format, excluding it from the CDR is unlikely to have an impact.	**-** May reduce the likelihood of innovation being adversely impacted in respect of 'materially enhanced' derived data. Conversely, it could reduce the ability for individuals to access information that they might otherwise have access to and could deter competition by preventing access to potentially rich data sources.	**0** Excluding derived data would provide some certainty to data holders who would know that any intellectual property rights associated with materially enhanced derived data are not at risk. However, there is likely to be some confusion about what falls within the scope of 'derived data', which could reduce the certainty and transparency.	- There may be some benefits to excluding derived data form the CDR, particularly as it would protect data holders' intellectual property rights. However, it will add complexity, reduce uncertainty, and there is a risk that it could deter innovation by restricting access to potentially rich data sets. It is more desirable to consider exempting derived data, or subsets of derived data, on a sector-by-sector basis.
	Option 1.4: Require the disclosure of product data	**0** This option will have a negligible impact on trust and confidence.	**+** Would impose some additional compliance costs for data holders who would need to make this information available. However, it will make it easier for new entrants by enabling them to compare their product offerings and will facilitate greater competition.	**+** Would increase the potential scale of and reach by providing for price-comparison and other like services, which could help consumers compare and switch between different products and services.	**0** Including product data may create uncertainty about which information would need to be made available under any CDR without providing more detail about what products, and information, included.	**0/+** There may be some challenges associated with clearly defining the data that is in scope, and setting the requirements for what must be disclosed, but ultimately this will benefit consumers and facilitate greater competition and innovation.
	Option 1.5: Provide for action initiation	**0** This option will have a negligible impact on trust and confidence.	**+** Would increase additional compliance costs for data holders and other incumbents in order to develop ways of mitigating the heightened risk of allowing action initiation. However, action initiation is likely to significantly increase innovation and competition so these costs are likely justified.	**++** Would drastically increase the functionality of the CDR and give consumers even greater control of their data. Would support much greater innovation and competition.	**-** There may be some heightened uncertainty for data holders, and businesses that may rely on instructions from data recipients (e.g. to open an account) which would need to consider how they can carry out these instructions while complying with existing obligations under other regulatory regimes.	**+/++** Without providing for both read access and action initiation it is unlikely that the benefits of a CDR will be fully realised. There are additional risks that will need to be managed, though these are outweighed by the potential benefits.

Preferred option(s)

Our preferred option is a combination of options 1.2, 1.4 and 1.5. This will mean that the CDR can apply to data relating to all consumers, whether individuals or other entities such as businesses and trusts. It will allow consumers to pair their data with product data to receive accurate comparisons, and to initiate actions on their behalf, which will reduce search and switch costs and incentivise innovation and competition.

Key:

++	much better than doing nothing/the status quo
+	better than doing nothing/the status quo
0	about the same as doing nothing/the status quo
-	worse than doing nothing/the status quo
- -	much worse than doing nothing/the status quo
[text]	preferred option

2: Options for regulatory approach

Having considered the different regulatory approaches used in overseas jurisdictions we have identified three primary options for regulatory intervention. These options are not mutually exclusive.

Option 2.1: Economy-wide, principles-based approach

Under this option, a principles-based data portability right would be established in legislation to build upon existing privacy frameworks. This would give consumers the ability to access or request that data held about them be shared in a structured and machine readable format. It could also establish some additional safeguard principles that would protect how data is stored, handled and shared. These are discussed further in Section 3.3.

Some overseas jurisdictions have taken a similar approach, including the European Union through its General Data Portability Regulation and, more recently, Singapore through changes to its Personal Data Protection Act. These interventions have generally been focused on personal information, rather than information relating to entities or product information.

Some submitters, including the Office of the Privacy Commissioner, noted that this option could be coupled with a sector-specific regulation described in option 2.2, as has occurred in some overseas jurisdictions.

Benefits - How will this option address the problem or opportunity? How will this option deliver the identified objective(s)?

This option would increase the ability of consumers to access their data across the entire economy. This could increase awareness among consumers of the value associated with their data, and their ability to access or share their data. In turn, this increased awareness could drive greater consumer demand for products and services that utilise their data and potentially greater scrutiny among consumers of how businesses are using and sharing their data.

An economy-wide right would stop businesses preventing consumers from accessing their data, but in the absence of common data standards or barriers on charging for access to data, the ability for consumers to fully utilise the data they obtain could be limited, because businesses could continue to provide it in a format that does not facilitate its digital use. New entrants may continue to struggle obtaining data and producing new products and services which use that data.

Some submitters noted that a principles-based approach would enable the machinery necessary to operationalise data portability, such as shared data standards, to be developed at a sector level, and for work that has been carried out to date to be used.

Costs and risks

This option would require all businesses to change their data handling and collection practices to enable data to be shared in a machine-readable format. This could impose significant costs on businesses, markets or sectors where there is not yet a demonstrated benefit from enabling data portability. These costs have been found to have an adverse impact on competition in the EU following the implantation of the GDPR.[51] There is a risk that imposing these costs across the economy could deter businesses from collecting data to avoid compliance costs that could be associated with an economy-wide right. This could deter innovation, and limit competition, both

[51] Gal, Michal and Oshrit Aviv (2020). The Competitive Effects of the GDPR. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3548444

among data-holders and, in-turn, third parties who could suffer from reduced volumes of data being available.

A purely principles-based approach, without additional levers available under options 2.2 and 2.3 would be unlikely to address concerns of new participants being locked out of the market. It would likely rely on industry-led solutions that could exacerbate power imbalances, and data-portability initiatives may only really materialise when there is consensus among a sector. As noted above, power-imbalances could persist, and new entrants may be unable to access data in a consistent format. Incumbents may also introduce new barriers to obtaining data, such as prohibitive pricing models for access data through APIs or onerous partnering agreements. In addition, new entrants would need to continue obtain bi-lateral agreements with data holders which is inefficient and can deter innovation.

Option 2.2: Sector-specific regulation

Under this option, each individual sector or market would be subject to a bespoke, specific regulatory regime. The bespoke model would be developed to address the actual level of data portability within a specific sector or market. This option could be progressed alongside, or instead of, an economy-wide right, and is similar to the approach taken in the UK to achieve open banking.

Any sector-specific regime could introduce shared technical standards for the sector, accreditation of third parties, additional privacy safeguards, and a liability and enforcement regime, as described below, though the precise settings would depend on the needs of a given sector or market. These would apply to the particular sector. In contrast to option 2.3, which would establish an overarching legislative framework, under this option individual regulatory regimes would be established in primary legislation for each sector, with detailed requirements set in secondary legislation.

Benefits - How will this option address the problem or opportunity? How will this option deliver the identified objective(s)?

Sector-specific regulation would give consumers within a given sector the ability to share their data. It could complement an economy-wide right, increase consumer trust and confidence in sharing their data within the system through accreditation of third parties.

The bespoke model would allow for the regulatory framework to be designed in a way that addresses the peculiar barriers to data portability which exist in a target sector.

Developing specific regulation/legislation for specific sectors will provide a high-degree of flexibility. There would be greater control of the type of data that would be required to be shared, and the ability to exclude certain types of data. It would also mean that regulatory intervention would only occur when industry-led initiatives have failed to deliver benefits to consumers, reducing unnecessary costs on businesses.

Under this option, it would also be possible to regulate or prohibit unregulated data exchanges within a particular sector (e.g. screen scraping) if there was found to be significant consumer harm.

Costs and risks

In the short term this could be a cost-effective option to achieve data portability in a single sector. However, as it appears as though similar regimes would be established in multiple sectors, this option is likely to be less cost-effective for government and the wider economy over the long

term. Further, it may be difficult to adjust multiple regimes as the need arose to adjust to new technologies or initiatives.

This option may exacerbate concerns of data portability initiatives being developed in silos, which could result in a lack of interoperability between frameworks. This could increase the cost of data-portability initiatives as a whole and limit the potential benefits of data portability. A lack of an over-arching framework, as discussed under option 2.3, may solidify these concerns further.

It may be difficult to clearly define sectors, particularly when businesses operate across multiple sectors. This would also likely lead to concerns of 'reciprocity' as businesses from other sectors may be able to obtain data through a sector-specific regime but not have the requirement to share data themselves. This may create new power imbalances, particularly if the businesses receiving data hold their own large data sets. If these businesses were then to offer products or services within the designated sector, it could shift the power imbalances, rather than address it, and fail to promote good consumer outcomes.

Under this option, and option 2.3, data holders may seek to recoup the costs required to implement the data sharing from third parties. This could limit the benefit of the CDR by creating an additional barrier to those already identified. To mitigate this risk, it will be necessary to introduce restrictions on the fees that data holders can charge third parties.

Option 2.3: Sector-designation approach

Under this option, a primary legislative CDR framework would be established that empowered a responsible Minister to apply the CDR gradually across sectors or markets within the economy through a designation instrument (secondary legislation). This approach would be very similar to the ACDR. It is envisaged that eventually, like option 1, the CDR could apply across large portions of the economy.

The key difference from option 2.2 is that under this option there would be an overarching legislative framework that would be applied to individual sectors or markets. This would guide the development of data portability in individual sectors, leading to greater interoperability and consistency across sectors or markets.

The ability to designate a sector as subject to the CDR would rest with the responsible Minister. During the designation of a particular sector or market it would be possible to specify the scope of the CDR, as discussed later, taking into account the nature of the sector or market and the data portability initiatives that exist.

The framework could comprise shared technical data standards, accreditation of third parties, additional privacy safeguards, and a liability and enforcement regime, as described below. During the designation process it would be possible for certain aspects of the framework to be adjusted as necessary depending on the sector in which it is applied. Importantly, this model would provide for interoperability which would allow data to be shared across sectors.

Benefits - How will this option address the problem or opportunity? How will this option deliver the identified objective(s)?

This option would improve the ability for consumers, within a designated sector and eventually across significant portions of the economy, to access and share their data.

Rather than relying on individual sectors to develop the means of operationalising the sharing of data, as would be the case under option 2.1, this option would involve more government intervention. In time, having a consistent framework that is applied across multiple sectors will

improve the interoperability of data-sharing across sectors. This will unlock new opportunities to share data across sectors, which could be particularly beneficial to businesses who operate within one market subject to the CDR that are looking to enter a new market which is also subject to the CDR.

This option would provide for the existing settings or features of a sector to be taken into consideration in applying the CDR to it, including the scope of the CDR in a given sector (e.g. what types of data would be appropriately subject to a CDR given any idiosyncrasies of the sector). This flexibility would allow the CDR to build upon existing work that has been carried out within sectors to achieve data sharing. It would also allow for the CDR to be designed to complement any existing regulatory obligations that apply to that sector, which would increase certainty and predictability for businesses.

New entrants would no longer need to obtain bilateral agreements with individual businesses, and shared data-standards, tailored for individual sectors, should be relatively cost effective to implement when compared to the status quo.

The Productivity Commission recommended that the Government establish a CDR using a sectoral-designation model in its Frontier Firms Inquiry final report, noting that consistency with the Australian's CDR regime could aid trans-Tasman and international interoperability.[52]

Costs and risks

This option will be more costly in the short-term for government and businesses within a designated sector, but overtime we anticipate that it will be less costly than the status quo.

One issue that has arisen in Australia is the concept of 'reciprocity', which is the ability of businesses that sit outside a designated sector to access data through the CDR while not being required to share equivalent data themselves. As noted above, if adopted, this could result in a new power imbalance if large multi-national firms started providing services within a designated sector. We consider that this risk could be addressed, in part, through the designation of a sector (i.e. in determining the scope of a designation).

There have been indications from Australia that the cost of access to the market for new entrants to meet new privacy safeguards and accreditation requirements could be prohibitive, this is discussed further below. These costs would also likely be an issue under option 3.2.

[52] New Zealand Productivity Commission (2021). New Zealand firms: reaching for the frontier Firms. https://www.productivity.govt.nz/assets/Documents/Final-report-Frontier-firms.pdf.

2: Impact Analysis for regulatory approach

		Criteria				
		Trust and confidence	**Efficient and fair**	**Scale and potential reach**	**Certainty, predictability, transparency**	**Overall assessment**
	Status quo	**0** Trust and confidence in data sharing is likely to continue to be relatively low. Consumers' ability to share data in a way that benefits them is somewhat limited, and there are hidden risks associated with sharing data.	**0** Costs would continue to disproportionately fall on new entrants who are required to enter into bilateral agreements with each individual data holder, which is inefficient and expensive.	**0** The scale and reach of data portability initiatives will continue to be limited. Sector-led initiatives may only ever deliver minimal benefits to consumers due to commercial incentives and risk aversion, and there is unlikely to be interoperability across sectors.	**0** Will continue to adversely impact certainty and predictability for consumers and new entrants.	**0** The status quo, where data portability is driven by individual sector-led initiatives, will not meet our assessment criteria and will fail to meet the objectives we are seeking to achieve.
Options identified	**Option 1: Economy-wide right**	**+** Would increase consumer trust in their ability to share their data, and if coupled with additional privacy safeguards may increase trust and confidence in how data will be handled. Would be somewhat limited though without ex-ante protections (e.g. accreditation of data recipients) that would be possible under the alternative models.	**-** While this option would spread the cost of compliance across all agencies that hold data, these costs would be imposed regardless of where there is a demonstrated benefit. There is evidence to suggest it could have negative effects on competition in some markets by deterring the collection of data in order to avoid additional compliance costs.	**+** Would improve the ability for consumers to access their data, which could drive greater demand for products or services that use that data. However, would rely on industry-led initiatives or, as has occurred overseas, sector-specific regulation to fully realise the potential benefits.	**+** All data holders would be subject to the same obligations regarding the handling and sharing of data. However, there may be a lack of certainty and transparency in the methods for setting standards for data sharing. The development of industry-led initiatives could pose additional complexity for businesses operating across multiple sectors.	**+** An economy-wide right would significantly improve the ability for individuals to access and share the data held about them, but the reliance on industry-led initiatives to operationalise this may reduce the overall effectiveness of this option.
	Option 2: sector specific regulation	**+/++** Would increase trust in the ability to share data within specific sectors, and for the data to be protected. However, at a cross-sector level, trust may be adversely impacted if different obligations or standards exist in different sectors.	**+** Focusing on the needs of specific sectors will ensure that costs are maintained at a reasonable level and will be spread evenly. Some of the costs incurred by data holders in building APIs could be recouped from third parties. Could impose barriers for new entrants looking to move into existing markets.	**+** Would increase the scale and potential of data-portability initiatives within individual sectors. However, the risk of divergent standards emerging could reduce the potential reach by impacting interoperability. This is expected to reduce the competition and innovation benefits and increase costs for businesses operating in multiple sectors.	**0** While there would be flexibility to adjust the regime to the needs of a sector, there would be problems for businesses operating across multiple sectors which could result in different data handling processes emerging, or divergent standards.	**+/++** Mandating data sharing in certain parts of the economy will provide some benefits within those sectors where a need has been identified. However, it could lead to costs where businesses operate across multiple sectors (or enter new sectors).
	Option 3: Sector-designation approach	**++** Would greatly improve trust and confidence, initially within specified sectors but gradually across the entire economy, in part due to the additional safeguards and protections, and interoperability of this approach.	**+** A flexible framework will ensure that costs fall evenly and they remain proportionate to the needs and risks of each sector. This will increase competition and innovation by levelling the playing field for new entrants	**++** In time, the ability for third-parties to operate across multiple sectors of the economy, and the interoperability enabled by a consistent framework will significantly increase the scale and reach of data portability initiatives.	**+** As with option 2.2, there would be flexibility which would allow the precise settings to meet the needs of a sector. However, the consistency of the overarching enabling framework will provide greater certainty and predictability to businesses operating across multiple sectors.	**++** Would give consumers confidence to share their data in a similar way in all designated sectors. Applying a consistent framework across the economy should enable interoperability between sectors, while rolling it out gradually will ensure that costs are apportioned fairly and enable the framework to adjust to the needs of each sector.

Preferred option(s)

Our preferred option is a sector-designation approach. This options is the most likely to lead to widespread data within, and across, sectors or markets of the economy. We consider that this option is the most likely to address the barriers that we have identified, and achieve our desired outcomes.

Key:

++	much better than doing nothing/the status quo
+	better than doing nothing/the status quo
0	about the same as doing nothing/the status quo
-	worse than doing nothing/the status quo
- -	much worse than doing nothing/the status quo
[text]	preferred option

3: Options for components of regulatory framework

The options described in this section are individual components of a sector-designation regulatory framework contemplated in Section 3.2. Each option is intended to address particular problems that we have identified in Section 2. The options are designed to be complementary to one another.

We have not included analysis of options relating to dispute resolution, liability and enforcement framework (including consideration of direct rights of action), education and awareness programme, institutional arrangements or cost recovery. These will be discussed and analysed in a second RIS that will support secondary policy decisions.

Option 3.1: Introduce an accreditation regime

Introducing an accreditation regime would require data recipients to demonstrate that they can safely deal with defined obligations relating to consumer data. This could include requiring company directors to meet 'fit and proper' person standards, adherence to information privacy and security standards, and obligatory membership of a dispute resolution body. Accredited data recipients may be subject to enforcement action if they breached their obligations.

Decisions on the particular conditions that must be met in order for third parties to obtain accreditation, as well as how the accreditation regime would be funded will be considered as part of a second-phase of policy decisions in late 2021.

Benefits – How will this option deliver the identified objective(s)? How does it address the problem or opportunity?

Requiring accreditation of entities before they are able to receive consumer data would promote consumer trust in sharing their data, because of the knowledge that participants are subject a range of security and governance requirements. Consumers are likely to have greater confidence in a system where there is clear access to a remedy if they suffer loss caused by a system participant misusing their data. The imposition of adequate security measures through the accreditation process will also assist to ensure the integrity of data and privacy of data subjects.

Consumers are more likely to share data in a system in which they have higher trust and confidence. We would therefore expect accreditation to engender higher levels of uptake and participation among consumers, which would in theory increase the rates of competition and innovation enabled by the CDR.

Most other jurisdictions that have opted to regulate data sharing through sector-specific or sector-designation models have adopted this approach (alongside other regulatory tools). This lever would not be available through an economy-wide, principles based model.

An accreditation regime would improve the security of data sharing methods relative to existing unregulated methods that are used, to the extent that data exchanges were regulated. This is because it would impose rules around information security, clarify responsibilities and manage risk.

Accreditation is likely to benefit third party businesses seeking to access consumer data by standardising the conditions they must meet to be able to receive data, rather than this being a matter for bilateral negotiation with each business from which they request data. Although there would be an upfront cost involved in meeting accreditation, in theory, the costs to third parties would be smaller over the longer term. This is because third parties would not have to continue to

invest resources into negotiating and then developing varying information security protocols and other standards with data holders. The scale of cost savings in the longer term would depend on the level at which the bar for accreditation is set, and whether a risk based or generalised approach is taken.

Similarly, shifting the onus of assessing the capability of a third party to safeguard and securely handle information to a regulator, rather than having it sit with incumbents, will relieve the costs on incumbents to independently approve entities before entering data sharing agreements. This would be expected to facilitate efficiency, create more opportunities for entry, and improve trust.

The introduction and enforcement of robust technical standards for data encryption and APIs has been proven to be effective in mitigating security risks. The US, UK, and EU have published guidance notes for organisations on the encryption of data. The imposition of adequate security measures through the accreditation process will also assist to ensure the integrity of data and privacy of data subjects. This was a key objective in the establishment of Australia's regime.

Costs and risks

Accreditation has the potential to further tilt the playing field in favour of larger, established institutions if the accreditation standards are overly onerous or cost-prohibitive for new or smaller players to meet. A small minority of dominant or established market participants are more likely to have the capital to invest in necessary systems, and to play a role in determining what the standards are. Further, where these players are already operating in regulated markets, they may have a 'first starter' advantage and have already made investments in data security systems, which are of an adequate standard to satisfy the CDR system accreditation requirements. Unregulated, newer, or smaller entities are unlikely to have made commensurate investments in infrastructure, meaning the initial cost of accreditation for such entities could be proportionately higher, and for some may pose a barrier to entry. The scale and impact of the costs would be affected by whether a risk-based or standardised approach was taken to the accreditation. The spread of costs under a universal accreditation regime is likely to be inefficient, whereas a risk-based accreditation regime allows for a fairer distribution of costs among players.

Businesses may seek to recoup the costs associated with accreditation in ways that would impact consumers and other end uses (e.g. by increasing prices of goods or services). This may adversely affect the efficiency and fairness of the regime, and could inhibit its reach if the prices are sufficiently high to deter consumer participation.

The standardisation of functions and requirements under an accreditation regime risks reducing variety and features in the market place, which could adversely impact consumer choice and innovation. Over time, this may limit the impact of the regime.

How has consultation affected this option?

There was broad support from stakeholders for the introduction of an accreditation framework or comparable tool to ensure control over access to data and management of the associated risks. Some stakeholders expressed concerns about the scale of compliance costs, and encouraged officials to learn from the experiences of Australia, where the initial bar for accreditation was set at a level that precluded uptake.

Sub-option 3.1A: Tiered accreditation

A tiered accreditation regime involves a risk-based approach to setting the conditions (in particular, security protocols) that data recipients must meet in order to receive consumer data.

The measures a third party would be subject to would be determined by the risks associated with the data they are seeking to hold and the vulnerability of the third party. For example, an intermediary with limited data access may be required to demonstrate lower standards for accreditation, but would be granted only restricted data access rights. A similar recommendation for a tiered accreditation system was made following the 2020 review of the ACDR. This was recognised as a key lever for facilitating the participation of third party service providers in the regime.

Benefits - How will this option deliver the identified objective(s)? How does it address the problems?

A risk-based approach would avoid the need to impose security protocols on smaller third parties, who lack capital and human resource, where it would be unreasonable or unnecessary to do so. The benefit of this approach is that would mitigate the risk that accreditation posed a cost-prohibitive barriers to participation for new entrants or smaller players. Tiered accreditation would therefore increase the likely scale and reach of the CDR, in a more efficient and fair manner. It is also likely to achieve greater scale and reach than under a universal accreditation framework.

Costs and risks

A risk-based/tiered approach to accreditation is more complex than a generalised approach, due to the different levels of scrutiny applied to participating entities. The complexity or uncertainty could be offset by developing prescriptive rules and supporting guidance around the approach to conducting risk-based assessments.

Option 3.2: Information and consumer protection safeguards

The information security risks associated with the facilitation of data flows mean the implementation of appropriate safeguards through a CDR is imperative. Protection of individuals against such risks is fundamental to the consumer-focused design of the framework. Fostering consumer trust in the regime and in businesses' commitment to data protection and privacy is likely to be critical to the utility and efficacy of a CDR. Consumers need to be confident system participants will handle their data securely. A lack of confidence will impact the uptake and efficiency of the framework.

To establish trust and ensure the protection of data and privacy, a fit-for-purpose and adaptive suite of safeguards must apply to data sharing. We consider that the following measures could be adopted to safeguard information and consumers when using the CDR:

- Requiring adherence to information security standards.
- Information protection safeguards, including an authorisation and verification framework, and an obligation to maintain a record of consents.
- Consumer protection safeguards, including limits on the permissible uses of consumer data and an obligation to produce a CDR policy.

The measures will supplement the enhanced consent framework, and requiring adherence to information security standards via an accreditation framework. The regulatory impact of those tools considered separately.

Benefits - How will this option address the problem or opportunity? How will this option deliver the identified objective(s)?

The process of authorisation, authentication, and notification will enhance the integrity of data and privacy of data subjects, improving the security of data transfers. It would also assist

individuals to understand how their personal data is being collected, processed and used, and give them more meaningful control over their data.

Authentication is a two-fold obligation on data holders, requiring them to (i) authenticate a consumer's consent to a data transfer, and (ii) verify the identity of an accredited data recipient. To the extent this authentication could leverage off of existing mechanisms, such as the Digital Identity Trust Framework, rather than requiring the creation of a bespoke tool, this could mitigate the costs on participants. This may also empower consumers to more readily exercise their rights of participation. Authorisation is granted to the data holder, by the consumer, to permit them to share data with an accredited recipient.

Notification involves the data holder informing the consumer when a data transfer has been executed. Notification provides confirmation to a consumer that their CDR data has been collected in accordance with their valid request. A mandatory notification system would also be expected to incentivise businesses to be more mindful of the dispersal of consumer data which they hold, because of the potential reputational risks. A comparable example is the introduction of notifications by Apple for iPhone users, accompanied by options for users to share more or less data and share it on their terms.

Maintenance of a dashboard or record of data transfers would improve consumers' level of control over and understanding of the uses of their data. In Australia, data holders must notify consumers by updating a dashboard that records the data transfers of the consumer's data that it has initiated. The notifications must detail the types of data consented to and collected, and list all the accredited recipients that have been transferred the consumer's data from the particular data holder.

Obliging data holders and accredited data recipients to produce a CDR policy would encourage businesses to be more mindful of the processes they have in place for the handling of consumer data, which would improve the overall security of the regime. The policy document must identify the risks and processes the organisation will adopt to limit inappropriate or unauthorised access to CDR data environment, and outline how the organisation will meet the overarching governance requirements for the security of CDR data.

Constraining the use of shared consumer data, as has been done in Australia, is another practice that would contribute to the robustness of the privacy framework. Permissible uses of consumer data would be limited to those prescribed in the CDR rules and otherwise authorised by law.

Costs and risks

Requiring adherence to overly high privacy and security standards increases compliance costs which can introduce or raise barriers to entry. Higher digital security and privacy costs can reduce returns on investment, which may reduce incentives to invest in data and innovate in some markets. If the cost of compliance with privacy and security obligations are too high, the proposals could have unintended negative effects on innovation by lowering the incentives to invest, and on competition (by discouraging market entry). Adherence is likely to be particularly onerous for small businesses, which may detract from the efficiency and fairness of the way costs are allocated between participants. High costs may deter new entrants or smaller players, which could limit the scale of impact the CDR achieves.

How has consultation affected this option?

There was resounding support among stakeholders for a secure framework to safeguard the privacy and confidentiality of consumer information. Many stakeholders considered that the

success of the CDR would be contingent on the robustness of these safeguards, given its role in gaining the trust and confidence among consumers needed to facilitate their participation.

Some stakeholders noted the complexities of the multi-regulator approach adopted in Australia, and urged officials to ensure the consistency of any such safeguards with New Zealand's existing privacy legislation.

Option 3.3: enhanced consent framework

This option would introduce a consent framework to ensure that data is only shared when a consumer has provided informed consent by imposing obligations on data holders and recipients. This framework will operate in addition the existing requirements of the Privacy Act. To enable the consent framework to be effective, data holders must comply with the data sharing request when data recipients have secured consent, and must not intervene to prevent the sharing of data.

The enhanced consent framework will require that:

- consumer consent be given voluntarily, expressly and with sufficient specificity to the particular terms, and must not be indefinite
- data recipients provide consumers information to inform their consent which is consistent, simple, comprehensible, specific and timely
- consumer consent can be amended or withdrawn with the data holder or data recipient at a later date
- that data holders and recipients cannot request consent for terms which undermine the overall intent of the consent provided by the customer.

Benefits – how will this option deliver the identified objectives or address the problem?

The introduction of a consent framework with obligations on the parties collecting and using data under the CDR will allow individuals to derive value from their data without overly compromising their privacy and data security. This is likely to increase trust and confidence in the CDR.

The consent frameworks requirement for consent to be informed will level the information asymmetry which exists between consumers and businesses requesting data currently. Consumers will have clarity to what they are agreeing to which could help ensure privacy and security, and can use their consent to act to achieve their interests, increasing consumer trust and confidence. While the Privacy Act provides important protections which focus on the purpose of collection and authorisation, there are some consumer protection requirements we consider would be essential to a CDR that are not explicitly provided for in that Act. These include the requirement that consumer consent be informed and limited, and the express expiry of consumer consent.

The consent framework could ensure that consumers have clarity about the precise terms they agreed to by making terms specific. The requirement that consent be specific could strengthen the Privacy Act requirement that only the information necessary for the established lawful purpose is collected.

Obligations like the requirement to authenticate identity could also prevent wrongful or coercive consents, as will restrictions on what terms can be included in consent processes.

A consent framework could supplement the existing protections in relation to CDR data by enhancing privacy safeguards and empowering consumers by putting in place further protections such as requirements for consent to expire after a set time period and that the consent relate to

specific terms. Enabling a lapse of consent or withdrawal of consent may prompt consumers to reconsider the products and services they are currently using. This could facilitate more consumers switching services and better consumer outcomes.

Costs and risks

A CDR consent framework that expanded on the existing obligations in the Privacy Act would impose a cost on businesses to create processes to adequately inform and engage consumers to ensure consent is truly voluntary, specific and informed. Additional costs could deter participation or diminish the benefits of a CDR to businesses. On balance, the costs to businesses are reasonable given the necessity of protections for security and privacy reasons, particularly in light of the information asymmetry.

However, it is possible that significant amounts of information given to consumers, as well the need to make a number of specific consents which must be renewed following expiry, could cause decision fatigue and have the opposite effect of empowering consumers. This could further embed the problem identified that consumer outcomes suffer when consumers stick to their initial providers for services against evidence of better deals. Without the impetus of greater consumer switching to preferable products, innovation and competition may not increase or improve.

Despite of the increased access to comprehensible information, consumers might still lack an awareness of the risks they are consenting to. However, requirements for how information should be communicated could help address this lack of understanding (e.g. by requiring risks be made transparent).

The significant amount of information and greater awareness of risk could undermine trust in data sharing more generally. However this risk is preferable to the status quo, where consumers share data with a lack of awareness of the end use. This is also balanced out by the obligations which enable transparency and clarity of the consent request terms and the implications of agreement.

The framework could have obligations to protect vulnerable consumers from manipulation and coercion. It may be that in some cases, parties should be deemed not capable of giving consent. These protections must be carefully balanced, otherwise consumer control over their data will be diminished in comparison to the status quo.

How has consultation affected this option?

A number of stakeholders raised consent processes as an element of how privacy and security should be protected. Stakeholders emphasised that a robust consent framework which enables the fullest control to consumers is necessary for an effective and trusted CDR.

Stakeholders noted that consent processes should be suitably rigorous to balance the need to protect consumers while not compromising the user experience or imposing significant costs on business.

Some stakeholders gave specific comments on elements like consent durations (e.g. annual expiry dates), how data literacy might contribute to informed consent, and who would bear responsibility for collecting consent.

Option 3.4: shared data standards

Standard data formats and ways that data is shared are essential for information to be accessible and usable at least cost. In the absence of these standards, each data holder may adopt their own systems for providing data in machine-readable format, and these may not be well designed or

documented. Data recipients would therefore need to build, maintain and update customised systems for retrieving and processing data from dozens of data holders, adding cost and making data sharing unworkable in many instances.

Under this option, a set of data standards would determine the technical detail of the format and how data is shared between data holders and data recipients in sectors subject to a CDR. These data standards would be developed by a data standards body. New Zealand would aim to align its data standards with equivalent international standards, in order to ease the development of IT systems, and provide interoperability between the systems used by New Zealand and overseas businesses.

Cabinet decisions around the structure and funding of CDR data standards bodies will be sought at a later date.

Benefits – how will this option deliver the identified objectives or address the problem?

Common data standards would promote beneficial sharing of consumer data by greatly reducing the costs to data recipients of requesting data and processing data. This will increase the benefits for consumers through more innovation and reducing barriers to entry in some markets.

Common data standards can also reduce the risk of insecure data transfers, by mandating the use of secure communication methods.

Costs and risks

There would be significant fiscal cost associated with developing and maintaining common data standards. The Australian Government has provided funding of AUD $15.9 million over five years to Data61 (part of the Commonwealth Scientific and Industrial Research Organisation) to act as the data standards body for the ACDR.[53] These costs may be reduced where:

- data standards have already been developed by industry – such as standards developed by Payment NZ's API Centre, or
- common data standards that have been developed in other countries and can easily be implemented in New Zealand.

There are also likely to be significant costs on data holders. These include one-off costs to build IT systems that conform to the data standards, and ongoing operating costs for maintaining and updating those systems as data standards are revised.

[53] Australian Treasury, Consumer Data Right Overview, p. 13, September 2019, available at treasury.gov.au/sites/default/files/2019-09/190904_cdr_booklet.pdf

3: Impact Analysis for components of a regulatory framework

		Criteria				
		Trust and confidence	**Efficient and fair**	**Scale and potential reach**	**Certainty, predictability, transparency**	**Overall assessment**
	Status quo	**0** Trust and confidence in data sharing is likely to continue to be relatively low. Consumers' are afforded some protection through the Privacy Act, but there are limited controls on the nature of entities able to access information.	**0** New entrants and smaller players would continue to be disadvantaged by the costs associated with overcoming barriers to entry to the market, which decreases participation and innovation.	**0** The scale and reach of data portability initiatives will continue to be limited as new entrants move offshore or bypass the New Zealand market. Barriers to entry and other commercial incentives will constrain access to markets.	**0** Outside of the Privacy Act, there will continue to be a lack of transparency around standards, pricing and cost.	**0** The status quo, where consumers are relatively unprotected and high costs pose barriers to entry and expansion for new entrants, will not meet our assessment criteria and will fail to meet the objectives we are seeking to achieve.
Options identified	**Option 3.1: Accreditation regime**	**+** Bolsters consumer trust in ability of system participants to securely handle data, and confidence in access to remedies in the event of loss.	**+** Imposes costs on businesses. At the same time, reduces barriers to entry for new and smaller players, and reduce imbalance of bargaining power held by incumbent providers.	**+/0** Improves access to markets which could increase levels of competition and innovation. However, costs of accreditation could deter participation in CDR in favour of unregulated data sharing methods, reducing benefits to consumers.	**+/0** Rationalisation of obligations and standards in single system would improve certainty. Introduction of additional regulatory obligations would increase complexity.	**+** This option would impose high initial costs on businesses, which could be prohibitive for new entrants. Overall, the costs of intervention are outweighed by the improvements to trust, confidence and integrity, and to improving market access for new entrants.
	Sub-option 3.1A: Tiered accreditation	**+** Bolsters consumer trust in ability of system participants to securely handle data, and confidence in access to redress in the event of loss.	**++** Obligations can be tailored according to risk-based assessment of entities, which results in a fairer allocation of costs and ensures smaller players are not burdened with high compliance costs.	**+** Reduced barriers to entry would allow for greater uptake among new entrants, which could drive greater competition and innovation in turn.	**+/0** Rationalisation of obligations and standards in single system would improve certainty. Introduction of additional obligations would increase complexity, more so in a tiered accreditation system. However, complexity could be mitigated through other means (e.g. the issuance of guidance).	**+/++** The imposition of costs under this option would be more efficient than under Option 3.1, and it may be more effective in reducing barriers to entry, meaning it is more likely to achieve stated objectives and deliver greater impact.
	Option 3.2: Information and consumer protection safeguards	**++** Strengthens consumer trust in confidence in the integrity and security of data exchanges, and give consumers better control over their data.	**+** Compliance costs may increase barriers to entry. Reduced profits for regulated parties could decrease investment and discourage participation.	**-** Compliance costs may maintain high barriers to entry, which could deter competition and innovation in turn. More robust protections for consumers and information may promote greater uptake among consumers.	**0** Introduction of obligations across multiple frameworks risks creating regulatory uncertainty and complexity. Rationalising regulatory framework, including liability and obligations of participants, would improve certainty and transparency.	**+** This option would increase overall compliance costs on businesses, due to compliance obligations under multiple frameworks. These costs are outweighed by the benefits to consumer trust and confidence, which are critical to achieving overall reform objectives.
	Option 3.3: Enhanced consent framework	**++** Empowers consumers to have agency over the movement and use of their data by giving comprehensible information, more awareness and greater control.	**0/+** Will impose compliance costs and potential barriers to entry. Reduces an information asymmetry between data holders/recipients and consumers and implements a framework to create consistency.	**0/+** By ensuring consumers are informed, the consent framework could encourage competition by better enabling switching. Greater autonomy over data could encourage wider consumer participation.	**++** The consent framework ensures the transfer of data will be made more transparent to consumers, and that transfers will be predictable and consistent.	**+** This option enhances the existing framework to provide more express protections to ensure consumers have trust and confidence to engage in the CDR. The compliance costs it imposes are outweighed by the benefits.
	Option 3.4: Shared data standards	**+** Data standards would provide more consistent and robust security.	**+** Shared data standards greatly reduce the costs to data recipients requesting and processing data, though they impose significant costs on data holders.	**++** Shared data standards are critical to uptake of CDR within designated sectors.	**++** Provide a much clearer and more certain path to accessing data for consumers and data recipients.	**+/++** Shared data standards are critical to CDR working in an effective manner. Without shared data standards, commercial and technical barriers to data sharing are likely to remain.

Preferred option

Our preferred option is to introduce a tiered accreditation regime, information and consumer protection safeguards, an enhanced consent framework, and shared data standards. Together these options will ensure the security and integrity of data transfers, while promoting trust and confidence in the framework from the consumer point of view. We consider they are the most effective combination to overcoming existing commercial barriers to entry, and together, are likely to deliver the greatest impact against the criteria and reform objectives.

Key:

++	much better than doing nothing/the status quo
+	better than doing nothing/the status quo
0	about the same as doing nothing/the status quo
-	worse than doing nothing/the status quo
- -	much worse than doing nothing/the status quo
[text]	preferred option

Section 4: Conclusions

Preferred package of options

Preferred package

Our preferred option will establish a CDR that allows all consumers, including individuals and other entities such as businesses, to share their data. It will allow this consumer data to be combined with data about the products, such as interest rates or fees, and will provide for 'action initiation'.

Our preferred option for the design of a CDR framework is the sector-designation model. This is because a sector-designation model allows for a tailored approach to regulating individual markets, with more flexibility to manage the costs on participants and leverage the existing data sharing initiatives that are functioning effectively. The scope of the CDR will be set during the designation process. This will allow the responsible Minister to specify the types of data that are within scope of the CDR, and the type of functionality that is enabled by the CDR. Overall, this approach is likely to deliver a higher level of benefits to consumers, businesses, and the economy relative to an economy-wide approach.

Our preferred combination of regulatory tools are the introduction of a tiered accreditation regime, information and consumer protection safeguards, an enhanced consent framework and data standards. These tools are complementary, and can be employed together to ensure the security and integrity of the data sharing regime, and minimise risk. The combination will promote consumer trust and confidence in the regime, which is critical to its success, while allowing the costs and compliance burden on businesses to be carefully managed. Of the various combinations, these tools (particularly the tiered accreditation framework and data standards) will achieve scale and specificity. A majority of stakeholders were generally supportive of measures that would ensure data could be transferred safely and securely. Data standards will help to overcome the high transactional costs of data sharing at present, by standardising access and increasing transparency.

The combination of regulatory tools are expected to result in fairly significant implementation and enforcement costs for the regulator. As regulation is expected to improve consumer outcomes and enable New Zealand to access more innovation, we consider these costs are justified.

Preferred combination of regulatory tools

The table below summarises how our preferred combination of options address the problems outlines in Section 2. For the purposes of the below table, Problem 1 has been split into two parts in order to reflect that some options only address one of the two aspects of the problem.

Preferred options		***High level policy problem***			
		New participants locked out of markets	Potentially beneficial data exchanges not occurring	Methods of data exchanges are insecure or sub-optimal	Data exchanges occurring are not aligned with best consumer outcomes
	Option 1.2: information about entities and individuals	✓	✓		

	Option 1.4: product data	✓	✓		
	Option 1.5: provide for action initiation	✓	✓	✓	✓
	Option 2.3: sector-designation model	✓	✓	✓	✓
	Sub-option 3.1A: tiered accreditation	✓		✓	✓
	Option 3.2: information and consumer protection safeguards	✓		✓	✓
	Option 3.3: Consent framework			✓	✓
	Option 3.4: Shared data standard	✓	✓	✓	✓

Some uncertainty over impacts of the preferred options

The preferred option involves designating markets as subject to the regulatory system through secondary legislation. This inevitably results in a level of uncertainty over which markets may be designated in future.

To mitigate the impacts of uncertainty, work is underway to determine a pipeline of the initial sectors that will be designated under the CDR so that market participants have time to prepare for regulation. We envisage that the regulation would in the medium term be applied to those sectors in which there is evidence of low levels of competition and scope to improve consumer outcomes, or where work has already begun to implement data sharing regimes.

There is also a high-degree of uncertainty regarding the potential costs of such a regime, which will be impacted by factors such as the number of sectors designated, the rate at which they are designated, the level of data portability already occurring in a sector, and the institutional and governance arrangements. Decisions on these matters will be made later in 2021.

Affected parties ***(identify)***	**Comment: nature of cost or benefit (eg ongoing, one-off), evidence and assumption (eg compliance rates), risks**	**Impact** ***$m present value, for monetised impacts; high, medium or low for non-monetised impacts***
Additional costs of proposed approach, compared to taking no action		
Regulated parties	• Initial implementation costs incurred by data holders subject to a designation, which would need to put systems and processes in place to handle, collect and store data in accordance with the requirements of the CDR framework. Costs would also be incurred to update systems to reflect any changes in standards and to implement APIs. • Data recipients would face costs to obtain accreditation if they chose to operate under the CDR (these may be offset by the benefits associated with accreditation) • Ongoing compliance costs to maintain consistency with obligations and standards • Incumbents may face greater competition from new entrants.	High In Australia, Westpac has estimated the cost of implementing open banking as between AUD $150 and AUD $200 million. In Australia, the costs of accreditation has been estimated at between AUD $50,000 to AUD $70,000.
Overall economy	Not estimated. Economic costs are discussed in the rows relating to regulated and other parties.	Not estimated
Regulators	Initial and ongoing establishment, implementation, and enforcement costs.	Medium-High The Australian government had allocated AUD $100 million over five years to the CDR, and recently announced AUD $111.3 million over two years to accelerate the rollout of the CDR. We anticipate that the costs will be significantly lower in New Zealand as we leverage existing arrangements and build economies of scale.
Other parties	Risk of higher prices if regulated parties pass on accreditation and compliance costs.	Medium

Total Monetised Cost	Not estimated	Not estimated
Total non-monetised costs	It is difficult to estimate the costs or quantify the likely impact of the CDR as the extent of these will vary significantly depending on decisions about the design of the regime, and its implementation. For example, if the CDR was to be applied to a sector or market with common data standards that businesses have built, but there was no accreditation regime, the costs to regulated parties might be low overall. Similarly, decisions regarding the institutional arrangements will alter the cost to the Government. Accordingly, the costs and impacts will be considered in more detail as decisions on the more detailed design, and implementation, are made.	High

Expected benefits of proposed approach, compared to taking no action		
Consumers	• Greater choice and control over their data. • Access to a wider range of products that are better suited to them. • Increased ability to compare and switch between different product providers. • Productivity gains for small-medium business who choose to share their data through a CDR.	High
Regulated parties	• New entrants and smaller participants able to more easily enter markets. • Certainty and standardisation reduce the cost and improve the efficiency of data exchange processes. • Businesses increase profitability by deriving insights from data to develop products that fulfil more of their customer's needs. • Businesses can partner with third parties to achieve economies of scale, by sharing performance and usage data (among other things).	High
Overall economy	• Accelerates progress toward the digital transformation of the economy • Likely to grow New Zealand's productivity	High

Regulators	• Regulators would be better placed to enact data sharing regimes that meet the needs of consumers and specific sectors. • Regulatory functions might also be improved within designated sectors if participants are able to access richer data sources (e.g. to enable consumer lending).	Medium
Total Monetised Benefit	Not estimated	Not estimated
Total non-monetised benefits	As above, it is difficult to assess the benefits of a CDR until decisions have been made on the more detailed design, and implementation. Accordingly, the benefits will be considered in more detail in future Regulatory Impact Statements to support further decisions. However, our assessment is that the benefits outweigh the costs based on the information that we currently have to hand. We also consider that our preferred option provides sufficient flexibility to minimise costs where possible, through utilising existing initiatives or building economies of scale.	High

Further comments

Robustness of evidence supporting this assessment

These issues have been identified on the basis of submissions received on the MBIE discussion document, consultation with external stakeholders, and international reporting from jurisdictions that have implemented a CDR or general data portability regime, or research related to the digital economy and data. We discuss the robustness of evidence of the problem and quality of data available in section 1 (Key Limits or Constraints on Analysis).

Section 5: Implementation and operation

Implementation of the proposals

How will the proposals be implemented?

Primary legislation will need to be introduced to establish the CDR framework. There is not an existing Act that could appropriately host this regulatory framework, therefore we consider that a new standalone piece of legislation is required.

In time, secondary legislation will be required to designate sectors, set the standards and make rules to give effect to the CDR.

There will be a second round of Cabinet decisions sought later in 2021, which will seek approval to outstanding design issues, and a potential pipeline for implementation.

Who will be responsible for implementation?

Further work is required to determine which agency would be best placed to regulate the CDR. We expect Cabinet decisions on the regulatory arrangements will be sought in late 2021.

When will the proposals come into effect?

Parliament must pass primary legislation for the framework to be enacted. After this has happened, the regulator will require time to establish its new functions.

At this stage, there is likely to be some delay before markets are subjected to the CDR through secondary legislation. Regulated parties will need sufficient notice of when the proposals will come into effect to prepare their systems. We intend to seek Cabinet agreement to a proposed timeline for sectoral implementation. This will provide more clarity to sectors as to when they are likely to be regulated.

Communications

The parties who will be subject to regulation are generally well informed about and engaged with the possibility of future regulation. As such, there is little risk of regulated parties being unaware of their future obligations. We would expect the regulatory agency to issue communications to provide further information to regulated parties.

Implementation risks

We are well placed to assess and respond to potential implementation risks given our proposed approach is similar to that used in Australia. We have considered the implementation issues experienced there and designed our proposed approach with these in mind. The most significant implementation risk remains, however, which is the ability for businesses within designated sectors to comply with requests for data in the manner contemplated in this RIS.

Section 6: Monitoring, evaluation and review

Monitoring, evaluation and review

Monitoring

As the lead policy agency for the competition and consumer protection regulatory systems, MBIE intends to monitor, evaluate, and review the regulatory framework in line with the Government's expectations for regulatory stewardship. The design of the designation model supports good regulatory stewardship, because it provides the ability to monitor, review, and adapt the regulatory framework in response to emerging issues and trends in particular markets and across the economy, meaning it can continue to be fit for purpose. As part of our regulatory stewardship role, we will take a proactive approach to identifying any issues by periodically consulting with key stakeholders on the impacts of the proposals and looking to overseas jurisdictions.

The impact of the proposals could be assessed by a range of measures including the size of the FinTech sector (should the CDR be applied to the banking or financial services sector) and the rates of search and switching in a given sector. We intend to conduct monitoring through close partnerships with other interested agencies.

Evaluation and review

MBIE will continue to monitor data sharing over time to ensure the regulatory framework is having the intended effects.

There are no plans to formally review the framework, though there would be an opportunity to do so through MBIE's role in periodically reviewing the laws which we are responsible for administering. An earlier review could take place if we were alerted to serious unintended effects of the framework, such as the sustained misuse of consumer data causing loss, or systemic adverse effects on competition. We would evaluate whether the regulation has been effective using criteria substantially similar to that used in this RIS.

Building the evidence base will help New Zealand and other countries to better understand the effectiveness of intervention and the scale of benefits realised by the selected approach (refer OECD working paper, Section C).[54]

[54] OECD, Working Party on Data Governance and Privacy in the Digital Economy (2021). Data Portability: Analytical Report, Mapping data portability initiatives and their opportunities and challenges. DSTI/CDEP/DGP(2021)1.