MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HIKINA WHAKATUTUKI

Discussion Document

Options for establishing a consumer data right in New Zealand

August 2020

newzealand.govt.nz

Permission to reproduce

Important notice

The opinions contained in this document are those of the Ministry of Business, Innovation and Employment and do not reflect official Government policy. Readers are advised to seek specific legal advice from a qualified professional person before undertaking any action in reliance on the contents of this publication. The contents of this discussion paper must not be construed as legal advice. The Ministry does not accept any responsibility or liability whatsoever whether in contract, tort, equity or otherwise for any action taken as a result of reading, or reliance placed on the Ministry because of having read, any part, or all, of the information in this discussion paper or for any error, inadequacy, deficiency, flaw in or omission from the discussion paper.

ISBN 978-1-99-001938-8 (online)

How to have your say

Submissions process

The Ministry of Business, Innovation and Employment (MBIE) seeks written submissions on the issues raised in this document by 10am Monday 5 October 2020. Your submission may respond to any or all of these issues. Where possible, please include evidence to support your views, for example references to independent research, facts and figures, or relevant examples.

Please include your contact details in the cover letter or e-mail accompanying your submission.

You can make your submission:

- by sending your submission as a Microsoft Word document to ***consumerdataright@mbie.govt.nz***
- by mailing your submission to:

  Consumer Data Right Project Team
  Commerce, Consumers and Communications
  Ministry of Business, Innovation & Employment
  PO Box 1473
  Wellington 6140

Please direct any questions that you have in relation to the submissions process to ***consumerdataright@mbie.govt.nz***

Use and release of information

The information provided in submissions will be used to inform MBIE's policy development process, and will inform advice to Ministers.

MBIE intends to upload copies of submissions received to MBIE's website at www.mbie.govt.nz. MBIE will consider you to have consented to uploading by making a submission, unless you clearly specify otherwise in your submission. If your submission contains any information that is confidential or you otherwise wish us not to publish, please:

- indicate this on the front of the submission, with any confidential information clearly marked within the text; and
- provide a separate version excluding the relevant information for publication on our website.

Submissions remain subject to request under the Official Information Act 1982. Please set out clearly in the cover letter or e-mail accompanying your submission if you have any objection to the release of any information in the submission, and in particular, which parts you consider should be withheld, together with the reasons for withholding the information. MBIE will take such objections into account and will consult with submitters when responding to requests under the Official Information Act 1982.

The Privacy Act 1993 establishes certain principles with respect to the collection, use and disclosure of information about individuals by various agencies, including MBIE. Any personal information you supply to MBIE in the course of making a submission will only be used for the purpose of assisting in the development of policy advice in relation to this review. Please clearly indicate in the cover letter or e-mail accompanying your submission if you do not wish your name, or any other personal information, to be included in any summary of submissions that MBIE may publish.

Contents

Glossary

API	Application programming interface. A set of routines, protocols, and tools for building software applications that specifies how software components should interact.
ACDR	The Australian Consumer Data Right.
CDR	Consumer Data Right.
Consumer	Any individual or entity who purchases, or intends to purchase, goods or services from another party.
Consumer data	Data relating to a particular individual or entity.
Data holder	An entity that holds consumer data.
Fintech	Financial technology business.
GDPR	The European Union's General Data Protection Regulation.
IT	Information technology.
MBIE	Ministry of Business, Innovation and Employment.
Open sector	A sector where consumers can authorise access and control of consumer data through third parties.
Product data	Data about the products and services offered by a particular supplier.
PSD2	The European Union's Payment Services Directive.
Read access	Where a third party can only read and display consumer data.
Screen scraping	Where a consumer signs in to their online account (e.g. online banking) through a third party's interface.
Write access	Where a third party can change consumer data with the consumer's consent.

1 Introduction

Purpose of this discussion document and context

1. The Ministry of Business, Innovation and Employment (MBIE) is seeking input on whether to develop a consumer data right (CDR) in New Zealand to give individuals and businesses greater choice and control over their data.

What does this discussion document do?

2. This discussion document seeks feedback on whether a CDR is needed in New Zealand and, if so, how it should be designed. The discussion document is divided into three key parts:

    a. Does New Zealand need a consumer data right? This section includes a discussion of consumer data portability, the benefits, costs and risks associated with a CDR, and the potential scope of a CDR.

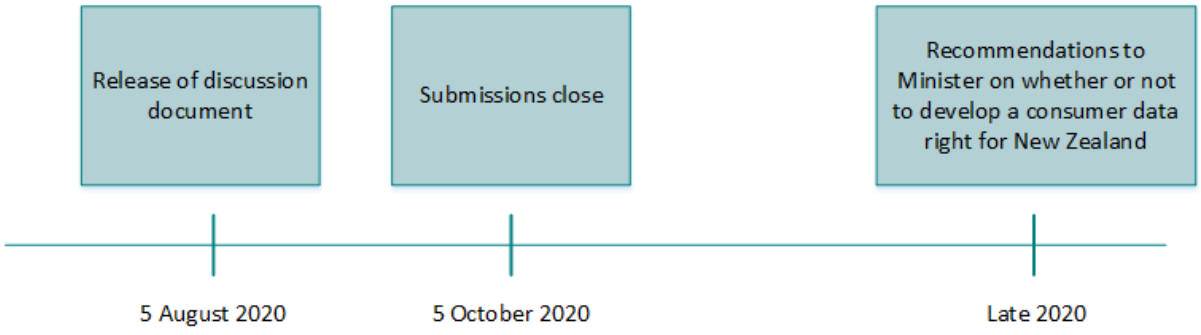
    b. What form could a consumer data right take? This section contains a discussion and our initial analysis of the options we have identified for the overall approach to establishing a CDR.

    c. How could a consumer data right be designed? This section includes a discussion on the elements that may be necessary in establishing a CDR.

3. The discussion document contains a high-level analysis of the options that we have identified to establish a CDR in New Zealand. The discussion document does not contain quantified cost benefit analysis and it does not contain analysis of how a CDR could be implemented in New Zealand. More detailed analysis will be completed as part of the policy development process as much of the detail is yet to be determined.

Process and timeline

4. Please provide submissions by 10am Monday 5 October 2020. Input on this document will be used to inform government on whether a CDR should be developed in New Zealand. The anticipated timelines for this work are set-out below.



2 Does New Zealand need a consumer data right?

5. Many businesses across the economy collect and hold significant volumes of data when providing goods and services to consumers. The collection and use of data has accelerated as consumers increasingly transact and participate in society online.

6. Various innovative products and services have emerged that utilise data to benefit consumers by helping them manage their finances, compare product offerings, or more easily switch among different product providers. These products and services can be especially useful in sectors or markets where there are high search and switch costs[1] such as insurance or banking. We are only beginning to understand the potential uses of data and these are likely to rapidly expand over time.

In the United Kingdom (UK), consumer data portability has been applied as 'open banking' to:

- use bank data to forecast how much someone will be able to save at the end of the month, and automatically move the amount into savings
- automatically round up purchases each time someone shops, and investing the difference
- separate bill money from spending money to help people keep track of their finances
- provide access to different bank accounts and credit cards in one place.

What is a consumer data right?

7. We use the term 'consumer data right' or CDR to describe a statutory ability for consumers to securely share data that is held about them with trusted third parties. This transfer of information is known as 'data portability'. The third party could be another product provider or a separate entity such as a fintech. The data would be shared in a consistent machine-readable format so that it can be utilised by the third party for the consumer's benefit.

8. 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) and Australia through its Consumer Data Right (ACDR).

9. Other jurisdictions have introduced data portability regimes in specific sectors, such as the United Kingdom which has specifically addressed data portability in the banking sector through 'open banking'.

[1] 'Search costs' refers to the costs or time associated with a consumer searching for a new product or supplier or comparing similar products from different suppliers (e.g. comparing different insurance policies). 'Switch costs' refers to the costs, time or disruption associated with a consumer switching to a new product or supplier.

Australian Consumer Data Right (ACDR)	General Data Protection Regulation (GDPR)
• The ACDR was introduced in 2019 and provides a cross-sectoral data portability right. The Australian Treasurer determines which sector the ACDR should apply to via a designation. The detailed rules are then designed taking note of the particular risks and requirements of the sector. • The first sectors to be designated were the banking and energy sectors, with phase one of open banking going live on 1 July 2020. • More information is available at: ***https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0***	• The GDPR came into effect in 2018 with the aim of strengthening data-protection rights for all individuals within the EU. It gives individuals the right to receive a copy of their personal data in a structured, commonly used and machine-readable format and transfer this data to a trusted third party. • The GDPR only applies to personal data, and the data portability aspect extends only to 'provided' or 'observed' data (and not 'derived' data). • More information is available at: ***https://gdpr.eu/***

Consumer data portability is limited in New Zealand

10. In New Zealand, the Privacy Act 1993 protects the collection, use and disclosure of personal information – that is information about an identifiable individual. The Act provides for individuals to access personal information held about them, and the Health Act 1956 provides a similar ability in respect of health information.

11. There have been some sector-led initiatives in New Zealand to promote data portability, including in the banking and electricity sectors. However, progress has been relatively slow and these initiatives do not appear to be delivering the full range of positive outcomes for consumers as yet.

Banking sector	Electricity sector
• Consumer data portability in the banking sector is known as 'open banking'. This has been led by the industry in New Zealand through the Payments NZ API Centre. • There has been progress in developing industry API standards, but very limited implementation of the standards or partnerships between API providers and third parties. • The Minister of Commerce and Consumer Affairs, Hon Kris Faafoi, recently signalled his concerns with the current pace and scope of work in implementing open banking in New Zealand[2]. • More information is available at: ***https://www.apicentre.paymentsnz.co.nz***	• A form of data portability already exists in New Zealand for electricity consumption and related data. • Consumers are able to compare pricing plans in order to determine which plan might be best for them. • Changes have recently been approved to improve the process for consumers to share their consumption data with organisations they trust. • More information is available at: ***https://www.ea.govt.nz/operations/consumer-services/provide-a-service-with-electricity-data/consumption-data/***

[2] Open Letter to API Providers regarding industry progress on API-enabled data sharing and open banking, from the Minister of Commerce and Consumer Affairs, Hon Kris Faafoi, December 2019 ***https://www.mbie.govt.nz/assets/open-letter-to-api-providers-regarding-industry-progress-on-api-enabled-data-sharing-and-open-banking.pdf***

12. During the response to the COVID-19 pandemic the digital transformation of the economy has been accelerated as greater volumes of business and commerce are conducted online. This also coincided with a rapid shift to contactless payments in traditional stores, exacerbating concerns about the impact that merchant service fees are having on businesses, particularly smaller retailers, and the lack of competition in the provision of retail payment services[3]. Establishing a CDR in the banking sector would enable the development of alternative contactless payment solutions that could provide greater convenience and security when consumers are shopping in stores or online. This could help contribute to the ongoing COVID-19 recovery effort by reducing payment fees charged to retailers. This is just one possible example of where a CDR could lead to new products and services being developed to benefit individuals and businesses.

Current regulatory settings may hinder data portability

13. We have heard a number of concerns about how current regulatory settings, or a lack of settings in some cases, may be hindering consumer data portability, for example:

    a. data holders are often reluctant to share information with third parties even when the individual has authorised it, or require a higher threshold of identification from the consumer than when they originally became a customer, due to privacy concerns[4]

    b. in practice, data holders may choose to refuse access to data in order to protect a competitive advantage

    c. there are generally no requirements for data to be shared in a consistent format across a sector

    d. data holders and third parties must hold bi-lateral agreements for the sharing of data which is inefficient (i.e. a fintech that relies on access to a consumers' bank data will need to enter into individual contracts with each bank)

    e. there is a lack of transparency around the fees that data holders can charge third parties for accessing application programming interfaces (APIs).

14. We have also heard that some third parties in the financial services sector are utilising less secure methods of accessing consumer data in the absence of a CDR. For example, some are using 'screen scraping' where a consumer effectively logs into an online account (e.g. online banking) via a third parties' interface. This could pose a risk to consumers as it does not limit the use of the data, and may also be a breach of the bank's terms and conditions.

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

[3] Businesses are charged a 'merchant service fee' by their bank for accepting online debit, contactless debit card, and all credit card transactions. Merchant service fees vary depending on the volume and size of transactions. According to a Retail NZ survey from 2019, the mean merchant service fees are 1.1 per cent for contactless debit card transactions and 1.5 per cent for credit card transactions, however there can be large variance in the fees paid (*http://retail.kiwi/system/resources/W1siZiIsIjIwMTkvMDUvMjAvNm11cDk2M3Znal9SZXRhaWxOWl9QYXItZW50c1JlcG9ydDIwMTkucGRmIl1d/RetailNZ-PaymentsReport2019.pdf*).

[4] The Privacy Act 1993 provides for personal information (relating to an individual) to be accessed by that individual, and for it to be disclosed with a third party on a limited number of grounds, including where the agency (data holder) believes that the disclosure was authorised by the individual. Verification of an individual's identity can be achieved through a digital identity service, such as RealMe.

What are the benefits of a consumer data right?

15. Establishing a CDR would give consumers greater choice and control over their data in new ways with trusted third-party providers. This will give rise to new products and services, allow consumers to compare products more easily, seamlessly switch product providers and transact with greater convenience. This will increase competition and innovation which, in turn, will benefit consumers by leading to reduced prices and improved product offerings.

16. We have identified a number of benefits, costs and risks for establishing a CDR which are summarised in the table below.

Benefits	Costs/Risks
Enables innovation and grows the digital economy by allowing third parties to develop tools for consumers that use their data to match or create products and services that better suit them. Data holders may also have access to new consumers and markets.	**Increased security and privacy concerns** as consumer data may be accessed by more companies there may be an increased risk of a data breach, and it may be difficult to determine where liability rests.
Facilitates competition by allowing consumers to multi-home services (e.g. to have access to services from multiple providers in one place), access innovative products and services, increasing transparency of pricing and other factors to more easily compare products and services, and potentially encouraging the unbundling of products and services.	**Implementation costs for government and industry** may be significant. It would require extensive changes to information technology (IT) systems to make data available. Depending on how a CDR is designed, these changes could be significant for smaller businesses (as data-holders), and large businesses that have multiple IT systems.
Increased productivity by reducing search and switch costs and allowing products to interact more with other services (e.g. cloud-based accounting using bank data to reconcile multiple bank accounts).	**May impose barriers to entry** by requiring businesses to hold consumer data in a particular way so that it can be shared in the appropriate format.
Strengthened privacy and data protections by improving security when data is shared, giving individuals and businesses greater control over the information held about them and the ability to use this data for their benefit.[5]	**May delay innovation** in sectors where progress has been made if those sectors choose to wait for regulatory intervention, or choose not to invest in new data-gathering methods due to the concern that they may be required to share this data or incur costs in making data available.
Consumer welfare will be improved by strengthening existing privacy rights for individuals, and giving consumers greater control of their data. Consumers will have the power to make more informed buying decisions through greater transparency, and will be able to access a wider range of products and services. Consumers will also be able to seamlessly switch product providers without losing data.	

[5] The Privacy Commissioner recommended a 'data portability' right in its Report to the Minister of Justice in 2017, ***https://www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/OPC-report-to-the-Minister-of-Justice-under-Section-26-of-the-Privacy-Act.pdf***

2	Do you agree with the potential benefits, costs or risks associated with a consumer data right as outlined in this discussion document? Why/why not?
3	Are there additional benefits, costs or risks that have not been explored in the above discussion on a consumer data right?

What is the scope of a consumer data right?

17. We consider that there may be a rationale for the government to introduce a CDR to foster greater consumer data portability and realise the consumer welfare and economic benefits. We would like to explore this further to better understand the costs and benefits of a CDR.

Consumer data

18. A CDR will apply to information relating to a particular consumer that is the end user who purchases a good or service from a supplier. This 'consumer data' can include information about a range of facets of our daily lives, including our purchasing preferences, travel destinations, spending or savings history, energy consumption or health records.

19. We consider that a CDR should apply equally to any end user of a product or service. This will mean that individual consumers as well as businesses and other entities will receive the benefits of a CDR. For businesses, especially small and medium-sized enterprises, a CDR could make it easier to carry out accounting or file taxes, obtain finance or insurance, and receive payments for goods and services.

20. Our initial view is that only 'provided' or 'observed' data would be subject to the CDR. 'Derived' data – that is data that has been created by a data holder through the application of insights and analytics – should generally be excluded from the definition of 'consumer data'. This is because this type of data has been derived by the data holder through proprietary means which may be commercially sensitive. Excluding this information from a CDR will help to ensure that data-holders are not discouraged from developing new methods of collecting and analysing data. It is worth noting, however, that derived data may still be considered 'personal information' for the purposes of the Privacy Act 1993 if it relates to a natural person, and that individuals could therefore request this information under that Act.

Product data

21. In addition, we consider that a CDR should incorporate information about the products or services offered to consumers by a business. This 'product data' could include information about the fees and interest rates for savings accounts provided by a particular bank or different prices for electricity plans. While strictly not about a specific consumer, this data can be used to help consumers make more informed decisions by making it easier to compare and switch between different products, which could provide significant benefits in markets with high search costs (e.g. insurance). Some of this information may currently be publicly available on the websites of suppliers or on government registers such as the Disclose Register under the Financial Markets Conduct Act 2013, though a CDR could extend beyond information that is already available in the public domain.

22. Some overseas jurisdictions are considering extending regimes like a CDR to anonymised market-level data. While this could provide useful insights, such as the market share of

particular providers, and could increase competition in certain sectors, our current thinking is that any CDR would not apply to market-level data as this is less likely to be used by consumers.

Read access and write access

23. There are two main forms of consumer data portability:

    a. 'read access' refers to the transfer of data a company holds about a consumer to a third party at the consumer's direction and with their consent. The third party can read the consumer's data, but they cannot modify it. For example, read access in the electricity sector could allow a consumer to share their usage history with a third party in order to help determine the best provider and pricing plan for them.

    b. 'write access' refers to enabling a third party to change or add to data about a consumer at their direction and with their consent. Write access could be used by consumers to authorise third parties to apply for, manage and change products on their behalf through an API or other means.

24. We consider that a CDR should provide for both read access and write access in order to reduce switching costs and fully realise the benefits for consumer welfare as set out in the table above on page 10. Some examples of where write access could be beneficial, include the ability to:

    a. open accounts with new service providers and close accounts with existing providers quickly and easily through a third party

    b. transfer data, such as bank transaction data or payment data from one provider to another

    c. update contact details or personal information across multiple service providers

    d. use an app or accounting software to arrange payments from a bank account.

25. There are some risks associated with write access that will need to be taken into account when designing a consumer data right. For example, there will need to be a high degree of trust in order for consumers to allow a third party to change data on their behalf, and the additional functionality could pose a heightened security risk.

4	What would the costs and benefits be of applying the consumer data right to businesses and other entities, in addition to individuals?
5	Do you have any comments on the types of data that we propose be included or excluded from a consumer data right (i.e. 'consumer data' and 'product data')?
6	What would the costs and benefits be of including both read access and write access in a consumer data right?

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

What are the outcomes that we are seeking to achieve?

26. A CDR could have positive outcomes for consumer welfare and economic development.

Consumer welfare	Economic development
• Strengthening existing privacy rights and giving consumers greater choice and control of their data. • Enabling innovation that provides consumers with a wider range of products and services that better meet their needs. • Increasing access to more affordable products and services by facilitating competition, and reduced search and switching costs.	• Increasing business productivity by accelerating the velocity with which data moves through the economy. • Contributing to the growth of the digital economy by enabling the development of new and innovative sectors of the economy (e.g. fintech) that use consumer and product data.

27. A CDR will help to achieve these outcomes by reducing barriers for consumers to use their data by sharing it with trusted third parties. This will enable third parties to develop new and innovative products and services that make it easier for consumers to make informed decisions. In turn, this innovation will facilitate competition, economic development and improve consumer welfare.

28. We suggest the following criteria for assessing any options for establishing a CDR:

    a. **Trust.** How well will the option strengthen privacy rights and maintain the security of consumer data while it is being used and shared?

    b. **Reach.** How well will the option enable multiple sectors to become 'open'[6] thriving data sharing economies? An option which enables multiple 'open' sectors presents significant economic development opportunities, greater competition and productivity for the long term benefit of consumers.

    c. **Speed.** How quickly will data portability become widespread throughout the economy, allowing the benefits to be realised?

    d. **Cost.** How well will the costs of implementing a CDR be minimised so that the costs do not outweigh the benefits?

[6] The use of 'open' in this paper differs from its use when discussing 'open data'. Whereas 'open data' refers to data that anyone can use and share, in an 'open' sector that would be enabled through a CDR a consumer's data is still secure and can only be accessed by trusted third parties with the consent of a consumer.

e. **Flexibility.** How well will an option allow for solutions to be tailored to the needs of a sector, and allow sector-led solutions to be developed before regulatory intervention?

7	Do you have any comments on the outcomes that we are seeking to achieve? Are there any additional outcomes that we should seek to achieve?
8	Do you have any comments on our proposed criteria for assessing options? Are there any additional factors that should be considered?

Options to establish a consumer data right

29. We have identified four main options for the high-level approach to designing a CDR. Each option is summarised below along with the pros and cons. At the end of this section on page 18 there is a brief summary of our initial analysis of each option against our assessment criteria. We have not included quantified cost benefit analysis as this will depend on the detailed design of any CDR.

Option one: Status quo

30. Under this option, the government would not introduce a consumer data right and the development of consumer data portability would be left to individual businesses or sectors.

31. There may be some progress in sectors where there is a consensus, however it is likely that progress would continue to be slow overall.

Pros	Cons
• Would not require regulatory intervention or government investment. • Sectors that are already making some progress in developing data portability could continue to do so (e.g. electricity). • Sectors will be able to develop solutions to address sector-specific concerns.	• Does not strengthen the ability for individuals to use or share their data. • Barriers to entry for new entrants will remain because of the need to have bi-lateral agreements with data holders. • Reliance on voluntary participation and standards likely to reduce effectiveness of sector-led initiatives and may allow for certain industry participants to hinder data portability to retain market positions. • The economic opportunities associated with a CDR will be hindered as it is likely to lead to inconsistencies in the approach taken within individual sectors and across different sectors of the economy. • Does not strengthen existing privacy rights and will not address privacy or security concerns that have emerged.

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

Option two: A sectoral-designation approach

32. Under this option a high-level framework would be established in legislation that would apply across the entire economy, but the CDR would only apply to sectors or markets that had been designated through secondary or tertiary legislation. This option is a sectoral designation approach similar to the ACDR.

33. The scope of a designated sector and the data holders within the sector to which the designation would apply would be determined during the designation process. Once a sector has been designated, the detailed rules would be designed and applied in relation to the particular risks of the sector.

34. Using a sectoral-designation approach would create a framework that would allow consumers of a designated sector to safely share data relating to them with trusted third parties. The generic framework could be governed by a set of general rules, and independent bodies could set standards for sharing information, carrying out accreditation of third parties and enforcement. These elements are discussed further in chapter 4.

Pros	Cons
• The sector-designation approach means that the design and implementation can be carefully tailored to designated sectors as opportunities emerge. • It would allow for a CDR to be applied in sectors where there is likely to be the greatest consumer benefit sooner than would be possible under an economy-wide approach. Though it will require the legislative framework to be set before the detailed rules and standards are developed. • Fewer barriers to entry and third parties will no longer need to have bi-lateral arrangements with data holders. • Enables a consistent CDR to be rolled out sector by sector and across sectors. • It could act as a regulatory backstop and encourage more industry-led solutions. • Could provide opportunities for alignment with the Digital Identity Trust Framework[7] and the ACDR. • Would allow the CDR to apply to individuals and businesses, and to 'product data' improving its effectiveness.	• Likely to be significant implementation costs for the government and designated sectors but these will be partially offset by overall efficiency gains. • There may be some difficulty easily defining sectors as businesses offer products across different sectors or markets. • Using a designation approach could lead to some sectors of the economy utilising the CDR long before others, however those sectors where there is the greatest need will likely be designated sooner. • Focusing on sectors where there is likely to be the greatest benefit means that existing privacy protections would not be strengthened in sectors that have not been designated.

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

[7] The Digital Identity Trust Framework is under development and will be a standards-based regulatory regime that will govern the operation of the digital identity eco-system and will provide for an accreditation process for digital identity providers.

Option three: An economy-wide consumer data right

35. A number of overseas jurisdictions have sought to improve consumer access and use of data through an extension of existing privacy protections. This includes the economy-wide general data protection approach in the EU's GDPR which was introduced in 2016 and came into force in 2018. The GDPR is intended to strengthen the data-protection rights of individuals by giving them the right to receive a copy of their personal data in a structured, commonly used and machine-readable format and transfer this data to a trusted party.

36. A similar approach in New Zealand on the GDPR would require providing data portability rights in legislation. This could involve giving consumers specific tools for protecting, accessing and using data held about them, as well as a system of fines for violating these. This CDR would apply across the entire economy, rather than to specific sectors, but it would be primarily focused on data about individuals and not information about businesses, or 'product data'.

Pros	Cons
• It would encourage all businesses and consumers to manage data in a safe and secure manner. • All sectors would reap the competition, privacy and consumer benefits of a CDR to some extent. • Would ensure consistency across the economic landscape. • Strengthens the ability of consumers to use the personal information held about them by creating an obligation for data holders to transfer data in a machine readable format.	• As this would establish an economy wide right, the design of the requirements and subsequent implementation would take a significant amount of time. • Requiring data to be provided to third-parties in a machine readable way may have major implications for businesses. These costs may be disproportionate to the benefits received, particularly for smaller businesses or in certain sectors of the economy. • May require significant enforcement mechanisms to ensure compliance with high-level principles, which could act as a barrier to entry. • Reliance on high-level principles might make this difficult to implement in practice and could require additional regulation to achieve an effective CDR. • May not fully realise the benefits of a CDR as it would be limited to information relating to individuals only and may not apply to businesses or 'product data'.

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

Option four: Sector-specific approach

37. Under this option, distinct CDRs could be designed for specific sectors as the need arose. This differs from Option two in which there is an overarching legislative framework that can be applied across different sectors. This option could involve sector-specific legislation that may incorporate some of the aspects of Option two, such as shared standards within a sector, or an

accreditation regime. This option would effectively be an extension of sector-led initiatives that are underway in New Zealand.

38. A sector-specific approach in New Zealand could be similar to the EU and UK approach to open banking, including the Payment Services Directive 2 (PSD2). PSD2 is an EU directive that specifically requires banks to open consumer data to third-party account information service providers and payment initiation service providers if required to do so by the user.

Pros	Cons
• May be a quicker and more cost-effective approach in the short-term for establishing a CDR in a specific sector of the economy. However, likely to be time consuming and inefficient at achieving a CDR across multiple sectors. • May improve the efficiency of the current approach by filling gaps within industry-led initiatives (e.g. it could establish an accreditation regime for a particular sector which may reduce costs for third-parties). • A regulatory backstop may encourage more industry led solutions. Would allow CDRs to be established where there is the greatest need, giving consumers greater choice and control of their data in those sectors.	• A lack of an over-arching legislative framework would reduce the overall effectiveness of this option as it reduces the likelihood of multiple 'open' sectors being interoperable. • Unlikely to fully realise the benefits of a CDR across the economy or across multiple sectors and may not incentivise new methods of collecting and using data. • Would not address privacy and security concerns in multiple sectors. • Could be significant implementation costs for businesses operating within a particular sector.

12	Do you have any comments on the discussion of Option four: Sector-specific approach?
13	This discussion document outlines four possible options to establish a consumer data right in New Zealand. Are there any other viable options?

Initial analysis of options against assessment criteria

	Option one: Status quo	Option two: Sectorial-Designation	Option three: Economy-wide	Option four: Sector-specific
Trust	× Trust in the regime at a sector and an economy-wide level is likely to be adversely impacted. Privacy and security concerns will remain, and third parties may be reluctant to develop solutions without being assured that they can access data.	✓✓The establishment of an accreditation regime, shared standards and privacy safeguards will foster consumer and business trust. This trust may prompt other sectors to become open via their own initiatives or through the CDR.	✓ Improving an individual's access to their data will improve consumer trust by strengthening existing privacy rights. However, without an accreditation regime for third parties or additional safeguards concerns around the security of data may remain.	~ This option may rely on existing privacy protections and the use of different standards across sectors may adversely impact trust among consumers and third parties.
Reach	× Relying on individual sectors to develop their own solutions is likely to see a divergence in the standards used by each sector (and possibly within sectors), and does not promote data portability across sectors.	✓ While the option wouldn't necessarily apply across the entire economy, allowing sectors to work with regulatory agencies to develop a fit-for-purpose CDR could enable thriving open sectors. A legislative framework that can be applied could also lead to a CDR that is interoperable across multiple sectors (e.g. allowing a consumer to share data across sectors). Would also be able to apply to businesses, and to 'product data'.	✓ More likely to lead to open sectors than the status quo, however excluding businesses and 'product data' will reduce the overall effectiveness. A high-level access regime may be difficult to implement and could require additional regulation to achieve fully open sectors. This reduces the potential reach of this option.	× This option is likely to be successful at leading to individual open sectors, but the lack of an over-arching framework will reduce the likelihood of interoperable sectors.
Speed	× Will allow individual sectors or businesses to develop their own solutions. However, progress is likely to continue to be slow due to competing interests.	✓ This option is more likely to see the development of secure data portability sooner than under the status quo because the detail is designed for specific sectors. It would allow for the CDR to be rolled-out gradually across the economy as the need arose.	~ Slower than other options as the requirements would need to be applied across the entire economy and would need to be developed before the regime could be implemented. However, the economy-wide roll out may lead to a CDR being available sooner than under the status quo.	✓ Will remove some of the barriers that are preventing the industry-led approach from being successful, and so it may be relatively quick in the short term. However, the development of open sectors across the economy would be slow over the long term.
Cost	~ While it would not require government investment, it would not be cost-effective for those sectors that do take steps towards enabling consumer data portability. For example, third parties would need to have separate bi-lateral agreements with data holders.	✓ This option will require significant implementation costs (e.g. the Australian government has forecast AUD 90 million over five years to implement the ACDR). However, some of these will be offset in part by the efficiencies gained at a sector and economy-wide level (e.g. having a centralised accreditation body will reduce the need for third-parties to have bi-lateral arrangements with each data holder).	~ Creates implementation costs for the government and the entire economy. While these costs may be lower than under Option two, they might be disproportionate in sectors that might not see the same extent of benefits from a CDR, or where sectors are making progress toward data portability.	× The implementation costs for this option may be lower than under other options in the short term, but a lack of a consistent approach within sectors or across the economy will reduce the potential for economies of scale and cost-effectiveness of this option overall.
Flexibility	~ Would continue to allow sectors to develop their own solutions, but will not address existing concerns or barriers to their successful implementation.	✓ Would provide for rules that could be tailored to the specific sector and would not preclude industry-led solutions from being developed. Could provide a regulatory backstop for when industry-led solutions are not adequate, though there is some risk that sectors may stop development in favour of waiting for regulation.	× As this would apply across the entire economy there is some risk that there may be inconsistencies with the consumer data portability that has been progressed in certain sectors without government intervention. May not allow for the needs of specific sectors to be taken into account.	✓ Would provide for CDRs to be highly tailored to the specific sector, and will support those sectors that have made progress towards enabling data portability without impacting other sectors where there may not necessarily be benefits.
Overall assessment	× The status quo is unlikely to meet our assessment criteria. Without some form of regulatory intervention it is unlikely that the consumer welfare and economic benefits of a CDR will be realised.	✓✓ This option appears to be the most likely to meet our criteria and address the problems that have been identified. While imposing significant implementation costs, this option is likely to lead to improved consumer welfare and economic benefits.	✓ An economy-wide approach may meet our criteria of reach and trust, but is unlikely to meet the remaining criteria. We consider that it would be effective at strengthening existing privacy rights but its limitations reduce the likelihood of this option achieving the full consumer welfare and economic benefits of a CDR.	~ A sector-specific approach will meet our criteria of speed and flexibility, but will fail to meet other criteria. While it might lead to individual open sectors, the potential benefits of a CDR will be diminished due to the lack of interoperable open sectors.

14	Do you have any comments on our initial analysis of the four options against our assessment criteria?
15	Do you agree or disagree with our assessment that Option two is most likely to achieve the best outcome using the assessment criteria?

4 How could a consumer data right be designed?

39. This chapter discusses how a CDR might be designed, should the government decide to establish one. Our discussion of these elements is focused on the sectoral-designation approach discussed in chapter three, given our preliminary view that it is the option most likely to meet our assessment criteria. However many of the elements discussed could apply to the other options.

40. If government were to establish a CDR through a sectoral-designation approach, a high-level framework would be set in legislation and specific sectors would be 'designated' into the regime via secondary or tertiary legislation. Much of the detail would be set during the designation process in consultation with the relevant sector. This would allow the settings to be tailored to the specific needs and risks of the sector.

Design of a consumer data right

41. The overall design of the framework is yet to be determined, however we have identified a number of areas that the legislation could cover, including:

    a. establishing a CDR that can be designated to specific sectors through secondary or tertiary legislation

    b. providing for the type of data and the types of data holders within a sector, included in the CDR to be set during the designation process

    c. providing for detailed rules for accessing and transferring data to be set during the designation process

    d. establishing an accreditation regime for third parties

    e. strengthening privacy safeguards

    f. establishing an enforcement regime and methods for consumer redress.

42. These factors are discussed in more detail below.

Designation process

43. Under a sectoral-designation model, primary legislation could establish the ability for a sector to be 'designated' through secondary or tertiary legislation (e.g. through regulations), and would set out the procedural requirements for any such process. The designation process may include an assessment of the likely impacts on consumers and the relevant sectors, as well as an analysis of the costs and benefits of designating a particular sector.

44. Sectors could be designated where there would be overall consumer welfare benefits. For example, where there are high barriers to entry, strong public interest, high search and switching costs, or untapped economic development opportunities.

Scope of a designation

45. In a designated sector, data holders would be required to grant access to data to third parties (on the consumer's consent), and it would need to be provided in a specified format. It is envisaged that the exact type of data and data holders (e.g. the types of businesses within a sector) to be included will be determined during the designation process. We recommend an industry data-specification process to review and reach an agreement on exact definitions of consumer data and product data for the industry.

46. A data-specification process allows for greater flexibility and the ability for the scope of CDR to move with developments in technology and data. For example, in some sectors, such as those where there are high search costs (e.g. insurance), the need for product data may be greater than in other sectors. It also allows for any CDR to be adjusted to recognise regulatory settings within the sector to avoid any potential overlap.

Rules and data standards

47. Primary legislation could allow for detailed rules and data standards to be set through secondary or tertiary legislation. A set of rules and data standards that can be applied across a designated sector is vital to the operation of a data portability regime.

48. A set of detailed rules would effectively set out how the data portability regime will function. It may establish, among other things, the types of data that can be shared and the timeframes for the sharing of data. It could also set some limitations on the prices that may be charged by data holders for accessing data so they are not excessive and do not restrict access by third parties. In addition, a set of data standards would determine the technical detail of how information is shared between data holders and third parties in a given sector.

Accreditation regime

49. An important element of promoting confidence in a CDR is ensuring that consumer data is only shared with entities that are able to hold the data safely and securely. This could be achieved through an accreditation model such as the one used for the ACDR, in which accreditation is undertaken by a centralised body. Once accredited, a third party can interact with any of the other accredited parties.

50. An accreditation regime improves the security and privacy of consumer data and removes the need for third parties to have multiple bi-lateral agreements with separate data holders, greatly improving the efficiency of the regime. Care will need to be taken to ensure that the accreditation regime does not exacerbate competition concerns by deterring innovative businesses from entering the market. One way that this could be achieved is if the accreditation regime allows for intermediaries to provide some of the systems or infrastructure that may be necessary to obtain accreditation.

51. Primary legislation could outline the processes and standards for accreditation and provide for the accreditation of a third party to be removed in certain situations, such as insolvency. It would likely also determine which body or bodies manage the accreditation process.

Privacy safeguards

52. While the security of consumer data will be protected through an accreditation regime, it may also be necessary to establish some additional privacy safeguards in primary legislation to strengthen existing privacy rights. These could go beyond the existing high-level privacy principles to enable the secure portability of consumer data to trusted third parties. For example, the ACDR establishes a range of privacy rights and obligations for users of the scheme, including the requirement for informed consent to collect, disclose, hold or use relevant data.

53. In order to ensure that access to consumer data is only shared when it has been authorised by the consumer, and that it is only used for the intended purpose, it is necessary to create a framework where consumer consent is required before information is transferred. A key part of obtaining an individual's consent to share data is confirming the identity of the individual. This will be made easier through the creation of a Digital Identity Trust Framework which is being progressed by the Government. The Digital Identity Trust Framework is intended to accelerate the development and update digital identity services that are secure, trusted and interoperable.

54. Consumers may require a certain degree of financial or digital literacy to ensure that they understand the potential risks posed by consenting to their data being shared and used by a third party. This could pose a particular risk for vulnerable consumers. The onus will likely fall on the organisation seeking consent to achieve a balance between providing the necessary information and ensure adequate understanding so that the consumer can provide informed consent while avoiding 'notice fatigue'.

Liability, enforcement and redress

55. Primary legislation may establish a liability and enforcement regime for the CDR. This could include setting out a range of offences, penalties or other enforcement tools that will apply to a designated sector, and setting out who is liable in the event of a breach.

56. In addition, it will also need to establish a means for consumers to report issues, and access redress in the event of a dispute between a consumer and a third-party or data holder. This may be achieved through the designation process whereby the sector specific dispute resolution service is empowered to resolve disputes in that sectors' CDR (e.g. if the electricity sector was designated, Utilities Disputes may be the relevant dispute resolution provider).

16	Do you agree with the key elements of a data portability regime as outlined in this section? Are there any elements that should be changed, added or removed?
17	Do you have any feedback on our discussion of any of these key elements?
18	Are there any areas where you think that more detail should be included in primary legislation?
19	How could a consumer data right be designed to protect the interests of vulnerable consumers?

Further design considerations

Māori data sovereignty

57. We have identified that the establishment of a CDR may interact with the concept of indigenous data sovereignty, and the notion that Māori data is taonga to be held, protected and used by Māori. Taonga are protected by Article 2 of Te Tiriti o Waitangi. The Waitangi Tribunal has indicated that taonga are subject to the Treaty principles and the Crown is obliged to actively protect taonga, consult with Māori in respect of taonga, and recognise Māori rangatiratanga over taonga.

58. Should government decide to establish a CDR, it should be developed in a way which builds trust and value for Māori. We will use the principles of Te Tiriti o Waitangi and engage Māori to ensure this is achieved.

Vulnerable consumers and accessibility issues

59. On page 21 it is noted that care will need to be taken to ensure that vulnerable consumers understand the scope of any consents they grant for access to their data. In addition, it will be necessary to consider how the needs of disabled people or those with accessibility issues are met. We will consider the specific needs of disabled people and accessibility requirements further during the ongoing development of any CDR.

Interoperability with overseas jurisdictions

60. Overseas jurisdictions have taken different approaches to enabling consumer data portability. For example, the GDPR is focused on expanding existing privacy protections to improve the ability for consumers to access and use their data. Meanwhile, the ACDR has established a framework and infrastructure to enable consumer data portability to be rolled out gradually as needed across the economy.

61. There may be some benefits in aligning any CDR in New Zealand with similar requirements in overseas jurisdictions. For example, the Australian and New Zealand Productivity Commissions identified a number of areas where a trans-Tasman approach to open banking and data portability could benefit both countries[8]. This included by making it easier for firms to obtain finance for trans-Tasman trade activities, broadening the market for emerging fintech firms and encouraging increased competition in trans-Tasman financial services.

20	Do you have any suggestions for considering how Te Tiriti o Waitangi should shape the introduction of a consumer data right in New Zealand?
21	How could a consumer data right be designed to ensure that the needs of disabled people or those with accessibility issues are met?

[8] *Growing the digital economy in Australia and New Zealand: Maximising opportunities for SMEs*, Australian and New Zealand Productivity Commissions, January 2019 ***https://www.productivity.govt.nz/assets/Research/b32acca009/Growing-the-digital-economy-in-Australia-and-New-Zealand_Final-Report.pdf***

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

Legislative design

62. If government were to progress a CDR it would intersect with various aspects of New Zealand's statute book, including competition, consumer and privacy law. Competition, consumer and privacy law have varied objectives and would interact with a CDR in different ways.

	Competition law	Consumer law	Privacy law
Purpose	Competition law is intended to promote competition and prohibit anti-competitive behaviour.	Consumer law is intended to promote consumer confidence and enable informed decision making by consumers.	Privacy law is intended to protect the collection, use and disclosure of personal information.
Alignment	A CDR will help to promote competition in designated sectors. Some of the aspects of the CDR, such as the power to designate sectors or requiring the disclosure of product information, align with the Commerce Act.	A CDR will benefit consumers by allowing them to use data to make informed decisions. Some aspects of the CDR, such as the data-sharing requirements, align with the Fair Trading Act, though other aspects, such as accreditation, may fall outside the scope of existing legislation.	A CDR will strengthen existing privacy protections and give individuals greater choice and control over their data. However, a CDR might require more active protections and facilitators than the current high-level privacy principles. Further, privacy law is limited to individual data and not data about other entities, such as businesses, or 'product data'.

63. Given that the legislative framework of a CDR intersects competition, consumer and privacy law, it may sit better in a stand-alone Act. This would provide greater flexibility to support existing laws, avoid misalignment and reduce any overlap or duplication.

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

Institutional arrangements

64. Some of the elements of a CDR discussed above will likely need to be overseen by one or more government agencies or other independent bodies. There may be separate bodies to set rules, data standards, oversee accreditation, carry out enforcement and resolve disputes between consumers and third party data holders.

65. The ACDR uses a multi-regulator approach. The Australian Competition and Consumer Commission is the lead regulator, develops rules and carries out accreditation of third-parties.

The Office of the Australian Information Commissioner is tasked with enforcing the privacy safeguards established by that regime, and a separate body was established to develop the technical standards for data sharing.

66. A similar approach could be followed here where multiple regulators play specific roles. Alternatively, a separate regulator could be established to oversee the regime as a whole. There may be pros and cons to either approach. The involvement of multiple regulators would allow each regulator to bring their knowledge and expertise to a particular aspect of a data portability regime. However it could lead to some inefficiencies, and there may be economies of scale gained through having a single regulator.

24	Do you have any comments on the arrangements for establishing any new bodies to oversee parts of a consumer data right?
25	What are the pros or cons of having multiple regulators, or a single regulator, involved in a consumer data right?

Monitoring and evaluation

67. If government decides to proceed with the establishment of a CDR it will be important to put in place a monitoring and evaluation plan to measure if the CDR is meeting our stated outcomes of improving consumer welfare and economic development.

68. Our monitoring and evaluation plan will be informed in part by the design of any CDR. However, we would like feedback on how we could measure the effectiveness of a CDR. For example, we could measure the number of third parties utilising consumer data portability, or the level of growth in relevant sectors, or use insights from consumer surveys.

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

5 Conclusion

69. Our preliminary view is that that there is a case for government intervention to promote more widespread secure data portability through a CDR that could be applied across a range of sectors of the economy. This will help give consumers access to a wider range of products and services that better meet their needs by reducing barriers to sharing and use of data by trusted third parties. In turn, this will promote competition, innovation, economic development and good outcomes for consumers.

70. Based on our initial analysis, the best option to achieve this appears to be a sectoral-designation approach similar to the ACDR. This would see a CDR established in legislation in New Zealand, which would provide a framework that can be applied flexibly across different sectors as the need arises. Much of the technical detail would then be determined through the designation process.

71. Any regime would require funding both to establish the regime and to provide sufficient resources to any agencies or regulators that are involved. It is anticipated that this may be initially funded from the Crown, however there will be a separate policy process to determine who should fund the aspects of a CDR (i.e. whether it should be Crown funded or third-party funded through fees or levies).

Next steps

72. Following consultation on this discussion document, we will consider the submissions and will provide advice to the new government following the 2020 general election on whether regulatory intervention is required to achieve widespread secure data portability in New Zealand through a CDR.

73. Should government decide to progress with a CDR, additional consultation with interested parties and agencies will be conducted as we develop the key features of a CDR.