MATTR Limited
12 Madden Street
Auckland, New Zealand

mattr.global
info@mattr.global

Options for establishing a consumer data right in New Zealand

Submission in response to the Ministry of Business, Innovation and Employment consultation document

Submission on discussion document: *Options for establishing a consumer data right in New Zealand*

Name	Emily Fry (Emily.Fry@mattr.global)
Organisation	MATTR

Responses to discussion document questions

MATTR welcomes the opportunity to comment on the New Zealand Consumer Data Right Consultation.

At the end of this document, under the section titled "other comments" we have provided an alternative approach to the advancement of consumer data portability rights in New Zealand. We invite your consideration of this approach and would welcome the opportunity to discuss further with you.

Our response to questions 1-26 below are based on the options provided in the discussion document.

Does New Zealand need a consumer data right?

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

There are a number of core problems preventing greater data portability that are not analysed in the discussion document. A foundational basis for the data portability considered in the discussion document is digital identity. In our view, the proposed benefits of CDR will not be realised without first enabling an interoperable digital identity eco-system.

i. First, the **existing state of digital identity services and infrastructure hinder 'at scale' consumer data portability**. Identity services typically sit in the middle of data portability interactions, between an individual requesting access to their data from an entity or wishing to share or transfer that data to a third party. For example, Europe's open banking-style legislation, the Second Payment Services Directive ("PSD2") requires using a Secure Customer Authentication ("SCA"), which authenticates the identity of customers and their right to make transactions, prior to making electronic payments. SCA is based on the use of two or more elements: (i) knowledge (something only users know); (ii) possession (something only users possess, such as cell phones that can receive codes); and/or (iii) inherence (something only the users have, such as fingerprints).

   The existing RealMe identity service lacks the flexibility to support the demands of a broader data portability infrastructure in terms of both adoptability (across ecosystem participants) and consumer usability. This problem encourages the establishment of *more centralised* identity verification services that do not align on standards. In turn this adds significant cost and complexity to the achievement of data portability goals.

   By contrast, a better approach to data portability would start with the concept of portability as it relates to identity data, including identity credentials such as driver's licenses and passports. This appropriately falls under the remit of the New Zealand Digital Identity Trust Framework **("DITF")**, (recently ***confirmed by Cabinet***) which recognises and supports *decentralised* and user-centric digital identity standards and solutions. This would help to address one of the major potential challenges exposed by data portability, namely the amplification of risks to privacy and security, (as identified in the table under paragraph 16 of the discussion document). A decentralised and user-centric digital identity approach supported by the rules of the DITF would allow

consumers to have more control over their own personal identity attributes and data in a verifiable, privacy enhancing and secure format by design.

ii. A second and further challenge to data portability that is not fully explored in the discussion document is around the **use of common data standards and schemas.** In our view these best sit in delegated legislation. There are several reasons why they are important.

Common open data standards and schemas reduce the barriers to entry. Common data standards and schemas (promulgated through policy and regulation) help to establish a level playing field for providers. Where such data standards and schemas are not established collectively, they risk being determined by one single provider/integrator that a dominant provider chooses. This can be problematic for several reasons. In the banking context) the provider/integrators are fintechs, which are not subject to robust sectoral-specific security and privacy requirements like banks are. Early stage fintechs may choose standards and schemas on the basis of financial incentives over other criteria such as privacy, security, and trust factors that lead to long term macro-economic benefit at scale. To mitigate this and consumer data simply switching between a relatively small set of providers, we recommend a policy directive on common, open data standards and schemas – such as ***this*** common data definition and schema governance approach, and agreed global standards (***Decentralised Identifiers*** (DIDs) and ***Verifiable Credentials*** (VCs)).

We would argue that these standards must place the subject of the data (either the consumer or entity to whom the data relates, depending on the scope of the CDR) at the centre of the model, with the ability to exercise control over who and what gets access to their data and under which circumstances. Recent developments in the decentralised identity space at organisations such as World Wide Web Consortium (W3C) and Decentralised Identity Foundation (DIF) have been focused on establishing a set of technical standards to support secure data portability. These technical standards (whilst initially conceived to solve the complex problems associated with secure, portable, consent driven, user-controlled *identity* data) are effectively standards that can support verifiable data of any kind. Adoption of these technical standards will mitigate many of the risks outlined in the discussion document and in turn promote trust, reach, flexibility amongst other assessment criteria.

Adopting such standards would also allow a shift away from achieving interoperability only within existing sectoral boundaries (such as banking or insurance). It would allow for data portability between traditional and new category players or across sectors – and potentially even across borders (see our response to Question 22 below). This could in turn unlock new kinds of services or commercial opportunities for innovative entities and businesses.

These standards can support consent driven direct interaction between parties with user-controlled ability to understand what data is being shared and full auditability trails, whether within a specific sector or where the boundaries between sectors may be blurred.

On a related note, there must be an emphasis on consistency in data schemas and formats to unlock greater technical portability. Para 13.c of the discussion document rightly notes that there are generally no requirements for data to be shared in a consistent format across a sector. This acts as a significant barrier to interoperability. By contrast, the use of ***JSON Linked Data*** (JSON-LD) in the context of ***W3C Verifiable Credentials*** allows us to retain the semantic context of data and establish data norms to support interoperability whilst achieving secure, privacy-driven and consent-driven data portability. This is critical to enable consumers to maximise the value and utility of data related to them and their activities cross-contextually.

Cost of integration and interoperability have the potential to be a substantial barrier to entry for new and smaller participants. There is a need for standards to help reduce barriers to entry and support safe, secure onboarding. These adoption considerations need to incorporate existing internet infrastructure investments and readily available and understood tools. Many of these considerations have already been contemplated in the context of digital identity and will be equally valid in the case of data portability.

iii. Third, the **lack of trust in data exchange** is another key barrier to greater data portability. As the discussion document notes, in the context of banking it is common for service providers to cite concern over privacy and identity verification in the context of data sharing. Lack of clarity around liability and AML regulation (which failed to consider advances in technology) are also problematic. Much of this is captured in a recent report commissioned by Digital Identity NZ (DINZ).

Here, accreditation is a helpful tool. The DITF proposes an accreditation scheme for ecosystem participants (including service and infrastructure providers). This could potentially be leveraged to accredit service and infrastructure providers in a CDR context. This would promote a consistent and streamlined approach to accreditation, and will minimise the administrative burden for consumers in the face of a future proliferation of accreditation of data holders and third parties.

Depending on which option is pursued for the introduction of a CDR, the DITF can support the scheme by helping to establish the accreditation schemes, and common standards required. There is also a strong need for a liability framework to protect participants in a verifiable data ecosystem when they are operating within the boundaries of the accreditation framework. There will be the need for the modernisation of this legislation over a time period to ensure that these barriers to adoption are removed. As such, it is recommended that accreditation scheme and common standards are stipulated in secondary or tertiary, rather than in primary legislation.

In sum, the range of technical factors outlined above must be addressed in this consultation. They represent very real barriers to the realisation of widespread benefits from data portability.

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?*

We partially agree with the benefits and costs/risks set out at para. 16.

A. Benefits

We broadly agree with the benefits outlined in the table under para 16. However, the realisation of the benefits is highly dependent on how the CDR framework is designed and implemented, and the extent to which it addresses issues we discuss below. In MATTR's view the proposed CDR, along the lines of option 2 or a sectoral-designation, overlooks three key concepts which must be addressed to realise the stated benefits.

1. **<u>Alignment with digital identity.</u>**

The relationship between the DITF and CDR needs to be explicitly addressed. In our view, there are **two core elements** that are **common** across the two frameworks**.**
These are:

a. A common approach to data standards and schemas
b. A common approach to accreditation of tools

These two elements underly both **consumer consent,** and the **mechanisms and tools** by which consent is provided and trusted. As the CDR makes clear, the CDR framework is **only activated** if the consumer provides their consent. It is therefore vital that there is robust governance of how consent is managed, which rightly sits underneath the DITF

On page 3 of the DITF Cabinet Paper, digital identity is defined as "user-consented, digitally enabled sharing of personal and organisational information", with figure 1 showing examples of the 'Infrastructure Providers' that enable consumers to consent to the sharing of their information or directly share it with 'Relying Parties' themselves. Making this relationship clear is critical to enable businesses and consumers fully to realise the potential benefits of the CDR.

2. Future focussed framing and terminology.

The proposed CDR defines 'data holders' as '*an entity that holds consumer data*'. MATTR's view is that this definition (and role) must be drafted to explicitly anticipate that in the near future consumers could be that 'entity' themselves. This is necessary to enable consumers to hold and control their data themselves through self-sovereign identity style tools (and/or enlisting fiduciary style custodial services to hold it for them). The current terminology used in the CDR risks restricting this as a possibility.

Digital identity providers (such as MATTR) are developing and deploying software infrastructure (**"Infrastructure"**) that will provide consumers with a meaningful role in their data transactions. This includes enabling consumers to initiate and explicitly consent to authorize data transactions through tools like cryptographically secure digital wallets and ***personal data vaults***. The standards underpinning this Infrastructure is being developed collaboratively across the globe (through organisations such as W3C and DIF) to ensure full interoperability and portability across providers and sectors. The collaboration is helpful in de-risking the possibility of vendor lock-in (which is detrimental to both consumers and business at a market level).

The proposed terminology and framing in the CDR does appear to consider this developing infrastructure. Defining 'data holders' as '*an entity that holds consumer data*' restricts the direction the market could take in the future, including the consumers ability to utilise tools that give them more personal control over their data.

Our view is that the framing and terminology could be improved in a number of ways. One way would be to include two roles – one for the "**Information Provider"** (e.g. an entity, such as a bank) which asserts and issues consumer information (and may or may not hold the data), and one for "**Subject"** of the information (the consumer) that controls and shares their information (who also may or may not choose to hold their data) through software tools. This would enable the market to develop in a way that does not structurally exclude the consumer from their own data eco-system. Alternatively, without introducing new terminology, the implementing legislation could clarify that the "entity that holds consumer data" may be the consumer themself.

If the CDR is developed further, it is imperative that the framing and terminology aligns with the DITF for the many businesses that will need to understand and adhere with both frameworks.

The W3C standard *Verifiable Credentials Data Model 1.0* may be a useful reference on how terminology is developing in a way that is user centric and future focused.

B. Costs / Risks

We partially agree with the costs and risks as outlined in the paper but we think two factors would, if incorporated in the analysis, **materially reduce the risks and costs** outlined on page 10. Recognising these factors and trends in the CDR framework will provide a future focused approach to tackling what have been traditionally hard problems of security, portability and user centricity.

1. **The use of linked data, standards and shared data schemas to mitigate implementation costs and barriers to entry can materially reduce the risks and costs outlined on page 10**

There is global recognition of the growing importance that the three interrelated concepts of linked data, standards and data schemas play in promoting data portability and interoperability. In this context:

- ***Linked data*** is the concept of sharing data in a standardised way, providing the ability to connect that data to other sources of information that exist across the web.
- *Technical standards* such as those developed at the W3C and IETF allow different entities to operate on commonly shared data models.
- ***Data Schemas*** are a structure for organizing and classifying data in a database. Commonly agreed data schemas (like ***Schema.org***) make it possible for different entities to operate cross contextually with shared semantics.

The three concepts are interrelated. Linked data provides a flexible way to structure data and describe relationships between data on the web. Rather than mandating a specific implementation or approach, it is a general model for an interconnected web of data on the internet. Standards describe and specify how data is actually represented in such a system, in order to provide entities with an interoperable way of implementing linked data. In turn, data schemas provide the ability to describe data using commonly shared definitions to enable real-world applications and data portability across different contexts.

Schema.org is an open organisation that creates, maintains, and promotes vocabularies for linked and structured data on the Internet (also known as the 'Semantic Web'). This approach to linked data can be used with many different encodings or syntaxes, including RDFa, Microdata and ***JSON-LD***. Over 30% of the web have adopted (and are increasingly adopting) the Linked Data Schema approach, most notably because it is used to index and organize the web into consumable and accessible knowledge graphs. This approach, coupled with new verifiable data infrastructure, as outlined above in the context of the W3C standard, can substantially increase flexibility and reduce the costs associated with integration and interoperability.

2. **Innovations in "bridging" technologies can materially reduce the risks and costs outlined on page 10.**

Significant innovations are occurring both locally and globally to create new and cost effective solutions that can plug into existing enterprise and government infrastructure. These allow investments to be leveraged in new ways and reducing dependencies on expensive back-end legacy system changes. One such innovation is the use of the OpenID Connect protocol (which is standard in many organisations identity and access management solutions) to manage issuance of data in secure, portable, linked-data formats. New decentralised secure communication protocols expand on this model to further support management of on-going interactions across secure connections in a decentralised network allowing cheap, highly performant, secure ways to achieve auditable interactions.

If the CDR is developed, our view is that it must recognise these standards and trends. Doing so will provide a future focused approach to tackling what have been traditionally hard problems of implementation cost, security, portability and user centricity.

If these mitigating factors are embraced, we can reduce some of the more substantial costs and risks outlined and stimulate innovation at the same time. Creating an early policy directive on standards will allow private sector to innovate with the confidence that they are directionally aligned with future regulatory intervention.

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

As we discuss in our response to question 22, we see the proposed CDR policy as an opportunity for NZ to learn, lead, and take a progressive approach.

The standards landscape (and what is technically possible) is constantly maturing. Progressive regulation in this context means being able to continue to benefit from evolutions of the technology and standards that underpin it. In our view the governing bodies should double down on progressive technical standards which can promote economic stimulus, rather than prescription in regulation. Where the regulatory position fixes a model it undermines innovation by creating barriers that were never intended.

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

We support individuals having a general legal right to data portability (please see the "other comments" section at the end of this document. Whether to extend the CDR to entities (in addition to individual consumers), depends on the nature of the CDR and scope of data included.

In terms of costs for business, our view is that these can be reduced by adopting a common data definition and ***schema*** approach rather than focusing on APIs which bind entities into a single delivery model. Verifiable data Infrastructure further enables scaled transactions volumes to be handled cheaply and efficiently. In reality, we believe that the costs associated with mishandling consumer data incorrectly far outweigh the costs of implementing a well-designed data portability scheme that would properly address the rights of data subjects and reduce the liability taken on by existing data holders who often unwittingly manage and process massive amounts of redundantly stored consumer data.

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')?*

1. **Consumer data**

In general, we agree with the statements made in para. 18 and para. 19. Regarding para. 18, we believe the right should also extend to "a particular consumer that is the end user who purchases *or intends to purchase* a good or service from a supplier," as prospective consumers also tend to share substantial amounts of data in the lead up to an actual or contemplated transaction.

Regarding para. 19, while it could be useful to extend the CDR to businesses as well as individuals, it should be done in a way that discourages businesses from increasing their data sharing about consumers against the interests of consumers themselves. For example, if the CDR attaches to the business but the underlying data actually relates to the consumer, e.g. in the context of observed, derived, or even aggregated data, extending the CDR to businesses might actually exacerbate the surveillance capitalist dynamics of the existing digital ecosystem to the consumer's detriment.

2. Derived data

Whilst we agree with the rationale provided in para. 20, we anticipate that businesses may in the future choose to provide "derived data" to consumers as premium service, notwithstanding the valid concern identified in paragraph 20 relating to commercial sensitivity in other cases.

In this scenario, it would be beneficial for data portability if derived data was provided in the same standardised way as consumer data (using verifiable data infrastructure to ensure security, portability and maintain the semantic context). In addition, though derived data isn't equivalent to consumer data, it should be constrained by terms which are plainly and explicitly outlined in a consent-driven way to consumers. That said, we are aware of other challenges around derived data such as when it relates to multiple individuals at one time (meaning one individual might dictate consent terms for another).

3. Product data

We do not have a strong view on the statements made in para. 21. We can see potential challenges with this model where organisations innovate pricing around customers. We think that careful consideration would need to be given to the set of data schemas as part of that implementation. We also think that it is important not to limit a consumer's ability to negotiate by forcing standardised rate cards for all aspects of offers, although this may be better suited for consumer protection legislation.

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

In MATTR's view the inclusion of both read and write access is necessary to realise the benefits proposed in the table on page 10.

The CDR is based on the premise of giving consumers more rights over their data. It follows that the CDR should promote a consumer's right to choose whether they authorise read access, write access, or neither, and under which circumstances they authorise each of these activities. Data holders should not be able to deny consumers this ability to choose (provided that the option is technically and commercially feasible, and backed by a clear and robust liability scheme).

Safeguards would need to be built in which could govern the conduct of data entities granted write access and/or to protect vulnerable consumers, as noted in paragraph 25. We support the development of an accreditation scheme and robust liability framework.

Furthermore, it's particularly important that 'write access' be authorized both legally and technically by consumers using verifiable information processes (as described in the context of our response to questions 1 and 2) in order to establish trust and auditability in this process.

In our view the inclusion of write access is necessary to future proof the model. The concept of ***personal secure data vaults*** is progressing rapidly in global communities such as W3C and DIF and will be available to consumers in market in the coming years.

Supporting write access in the CDR does not mean it has to be immediately available or approved – but it must be included to ensure that it is not precluded - allowing innovations to come to market as they mature. In our view, a standard approach to delegations must be included in the accreditation scheme.

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

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?*

We agree that the broad outcomes set out in the table under paragraph 26 – consumer welfare and economic development – are appropriate. However we would add some elements to the more granular detail provided in paragraphs 27-28. Specifically, in order to achieve consumer welfare (benchmarked against the criteria of 'trust', 'reach', 'speed', 'cost' and 'flexibility'), we consider that clear goals should be included to:

- establish a clear relationship between the CDR and the Digital Identity Trust Framework,
- clarify the terminology used in the CDR, as noted in our earlier responses (e.g. in relation to 'data holder',
- the outcomes of verifiability of data, processes, and relationships should as part of the criteria of 'Trust', in line with the DITF, should be sought, and
- be flexible in the sense that it does not unwittingly preclude emerging technology and trust models.

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

First, we have strong concerns with the objectives of 'speed' and 'cost'. It must be explicit that the objectives of 'Speed' and 'cost' must not come at the cost of robust outcomes. To provide one example, the commercial imperatives of speed-to-market would otherwise incentivise Fintechs to adopt processes that achieve financial functionality, but come at the cost of or place less weight on trust by undermining consumer privacy and security.

Secondly, in our view the objective of trust (as described) is dramatically limited. Trust on the internet is much broader than privacy rights in legislation and security of data when used and shared. In addition to these two important factors, trust on the internet also depends on the verifiability, authenticity and auditability of the data, process and relationships that are established. To achieve Trust these factors must also be included in the objective.

In terms of "reach," the discussion document is only concerned with reach across sectors of the economy, whereas we are also concerned with reach across individuals and communities in the population (see also "inclusion" below). We also note that the 'reach' criteria should also take into account "cross-border reach".

We would also add "future focussed" or "sustainable," which would also help address concerns around "speed" and/or "cost" in the long term. It is vital that in the process of developing the CDR framework we think beyond existing models of trust. Developments in decentralised technologies, including emerging standards at the W3C, and new cryptographic techniques signal future scenarios where the subject has far more control, privacy and security over their data, from a technical perspective, than is possible with existing technologies today. This is likely to lead to the development of new innovations and business models. It is vital that the CDR framework developed in the present does not limit such innovations. Rather, new and emerging legislative and regulatory frameworks could support and supplement emerging technical standards.

We would also add "inclusion" or "inclusivity". It is important that in the process of developing the consumer data right, we do not lose sight of the consumer. Being able to understand and take advantage of benefits of a CDR requires that the right is *accessible*, and that consumers or businesses have sufficient digital literacy and capability to make use of it. This may require interventions during the implementation of the new approach to ensure that inclusion is achieved – but is also key during the policy design phase, to ensure that simplicity and user accessibility is 'baked in'. Moreover, the ability to exercise rights under the CDR or related schemes will depend on the practical mechanisms for their exercise, which could risk excluding

	certain individuals or populations if not carefully designed. Addressing inclusion or inclusivity will also further enhance the reach of any of the options pursued.
9	*Do you have any comments on the discussion of Option one: Status quo?*
	We do not support Option one. The status quo option delays the inevitable and runs the risk that New Zealand fall behind other trading partners and jurisdictions, decreasing the nation's economic competitiveness in the long run.
10	*Do you have any comments on the discussion of Option two: A sectoral-designation process?*
	As with our other responses, our comments below are subject to our views expressed in the **"other comments"** section below where we suggest an alternative approach. Of the four options proposed, we understand the temptation of the sectoral designation approach as the quickest and most practical option. However, our view is that the medium to long term impact of this option requires further consideration. The concept of option three is most likely to achieve the policy goal of data portability, however (as discussed in the "other comments" section) a separate CDR is not the most appropriate vehicle for it. We have summarised our concerns with option two below. We agree with the statement in the table on page 15 that "there may be some difficulty easily defining sectors as businesses offer products across different sectors or markets". Consumers are sector agnostic and are often participants in more than one sector simultaneously, including in respect of the same data. An effective CDR ultimately needs to provide the consumer with control, transparency, utility and visibility of their data, as well as an ability to manage data differently in different contexts, regardless of which sector their service provider is in. For example, much of the innovation around financial inclusion has come from allowing consumers to leverage utility consumption, telecommunications or spending data, or other non-financial data to obtain loans or other financial services. The phased approach 'by sector' in option two could dramatically limit the utility of the consumer data rights in this respect, and restrict the potential for innovation that would otherwise be possible if the CDR was deployed in a broader manner. Whilst some of this could be addressed through terminology (such as the definition of 'data holder' and the types of data) a more sustainable and globally interoperable approach would be to take a broader approach (as suggested in our "other comments" section). Equally, businesses are increasingly operating across domains or sectors, offering digital services that consumers provide from a wide variety of different domains. In fact, drawing on a broad range of data is often what makes these businesses so innovative, and able to provide so much utility to consumers. The phased sectoral approach in option two may limit business' ability to leverage the CDR in such a business model, potentially disincentivising and restricting the very innovation it seeks to enable. Subject to our response in the "other comments" section and our response to question 13, we see option three as being more sustainable and effective than option two.
11	*Do you have any comments on the discussion of Option three: An economy-wide consumer data right?*
	With some reservations outlined below, we broadly support the option of an economy wide consumer data right as the end goal. Whilst we understand the business costs associated with a wide implementation of a consumer data right, we note that there are ways to mitigate these. For example, through adoption of

standards based verifiable data infrastructure which enables scaled transactions volumes to be handled cheaply and efficiently. Moreover, because consumers are sector-agnostic and businesses increasingly provide services across sectors, implementation costs may actually be reduced by taking an economy-wide approach.

We also believe the net benefit of implementing a broad consumer data right manner will greatly reduce the existing costs for today's businesses having to manage consumer data on their own - which is susceptible to fraud, spam, and abuse. If the CDR is developed further, this approach seems most aligned the DITF and most likely to be rolled-out and deployed in a complementary manner.

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

We do not support option four.

As outlined in our response to question two, consumers are sector-agnostic and the boundaries between sectors are increasingly blurred in an increasingly data-driven economy. As with Option two, Option four is not a sustainable approach in the long-term.

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

In our view, a more viable option would be to enhance individual rights under the Privacy Act 2020 or data protection legislation in combination with a robust TDIF.

We have set out this option in the "other comments" section below.

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

We comment below only on the two options which appear to be viable - options two and three. Please also refer to our response to question 8 on the criteria and in particular the "other comments" section below.

<u>Option Two: Sectoral Designation</u>

Trust: We agree that the establishment of an accreditation regime, shared standards and privacy safeguards will foster consumer and business trust. We note, however, that as the CDR is expanded to encompass a range of different sectors, the sensitivity of some data may require more sophisticated authentication systems, and a preference from consumers to see consistent levels of assurance being used. This only goes to underscore the need for a robust, user-centric, decentralised digital identity eco-system grounded in the DITF.

Reach: Please refer to our response to question 10. In our view this option (as opposed to option three) limits reach.

Speed: This option will only see the development of data portability sooner in *a dramatically limited sense.* Further, while we agree it will develop faster under the status quo – this will not be because *"the detail is designed for specific sectors"* - it is because this option (unlike the status quo to which it is compared) involves government intervention. Any option with considered government intervention in this space is more likely to see the robust data portability implemented in practice. We would like to understand the criteria against which the 'need' in other sectors be determined, and how soon other sectors are intended to be designated.

Cost: We have reservation that much of the cost can be offset in part by the efficiencies gained at a sector and economy-wide level because this option is a limited version of data portability. In our view the cost of a broader implementation would be worthwhile and necessary for NZ to be a digitally advanced nation. We support the concept of a centralised accreditation body as opposed to the use of bi-lateral arrangements. In our view there would need to be alignment of the standards, roles and terminology of any CDR with those proposed in the Digital Identity Trust Framework. Any material conflicts between the two frameworks is likely to generate costs and uncertainty for businesses and consumers alike.

Flexibility: We agree with the comment that a sector by sector approach may create uncertainty in sectors which may or may not be subject to designation, which stifles innovation. Clear communication and timelines will be necessary to mitigate this risk.

Option Three: Economy Wide

Trust: We disagree with the analysis provided on this criteria. The discussion document states *"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".*

In reality, an "economy-wide CDR" is not a CDR anymore if it becomes an individual right to data portability (as is the logical outcome of this option). If all entities that hold data are subject to the consumer right to data portability, then there is no need to "accredit" specific entities. Rather, the legislation will have to outline the specific obligations and requirements for data protection, data security, etc. on behalf of all 'data holders.' As discussed in the "other comments section" below, this right is most appropriately placed in the Privacy Act. Whilst a broad right to portability is likely a heavier lift in the short-term, it is more sustainable and will reap more rewards in the long-term.

Reach: Again, the medium to long term reach of a broad data portability right is much greater than option two.

Speed: We agree that the economy-wide roll out would lead to a CDR being available sooner than under the status quo (where there is no government intervention and no action on behalf of entities to promote it).

Cost: Our view is that the upfront implementation costs would be relatively low compared to the medium to long term benefits. Further, this option is more likely to reduce costs associated with fraud, spam, and abuse as well as open more opportunities for innovation which may set off costs.

Flexibility: An economy-wide scheme is, in many respects, the most flexible option because it allows consumers and businesses alike to determine the relevance of the same data in different contexts. It allows for innovative uses of data across traditional sectors and can promote inclusion by supplementing an individual's profile across contexts. An economy-wide scheme is also more likely to be interoperable with future cross-border and international frameworks, providing for extended flexibility across jurisdictions.

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

Whilst Option Two may intuitively feel more attainable in the short-term, we anticipate NZ will be back to the drawing board within several years of implementation. For the reasons discussed in our submission, it will not be a sustainable approach. In the long-term, this makes it less attractive across all criteria.

How could a consumer data right be designed?

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?*

In relation to option two, we broadly agree with the following key elements outlined:

- rules and data standards
- accreditation regime
- privacy safeguards
- liability, enforcement and redress.

In addition, we recommend that the following are considered:

- Privacy impact assessment of the option selected against other options considered, including the status quo
- Data security standards and requirements for entities holding and sharing/transferring consumer data
- Audit scheme or equivalent governance mechanisms to monitor and audit the compliance of data holders with privacy and security standards and rules set out under the CDR scheme
- Audit function of other mechanism by which to assess fairness, discrimination, and inclusion/exclusion of consumers and other impacts of the scheme
- Per para 41.f, relevant consumer redress mechanisms should include redress for erroneous or unauthorized data sharing/transfers and any violations of privacy or consumer-related rights

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

Whilst we recognise that the Discussion document is intended to be conceptual and not definitive, we note that it repeatedly takes for granted that the CDR would "improve consumer privacy" without explaining how. Providing consumers a right to data portability is part of an array of data protection-style rights that exist under other frameworks, such as the GDPR, but that does not inherently (in any way) promote privacy. On the contrary, data portability alone, without countervailing rights or measures, increases privacy and security risks by making the data ecosystem more open and by making transfers of data easier to achieve. The CDR has to be accompanied by specific privacy and data security requirements to mitigate those risks, whether in the primary CDR-enabling legislation or else in cross-referenced legislation from other domains (e.g. privacy, consumer protection, competition). In our view, the consumer right to portability should be established in the Privacy Act. We discuss this in the “other comments” section below.

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

We not that the nature of the primary vs. second/tertiary legislation would be very different depending on which option is selected.

If an economy-wide approach is taken (Option 3) the primary legislation may be more involved. The legislation would likely require a significant reconciliation with existing legislation across other legislation such as privacy, consumer protection, and competition. However, as noted above, we think that this is an inevitable and more sustainable option than option two in the long term.

With Option 2, we understand that the primary legislation could establish the nature and scope of the CDR at a high-level and the process for designating sectors. If this option is chosen, it will be critical (particularly) as additional sectors are designated) for coordination across relevant

agencies to mitigate risks of divergent or burdensome approaches, particularly for the businesses and entities that operate across multiple sectors, and where certain sectors have bodies with existing consumer protection or privacy remits.

If the Privacy Act was updated to include an individual right to data portability, this could obviate the need for a CDR entirely, or at least for an economy-wide scheme like Option 3. Introducing both a sector-specific CDR and a general right to data portability (which may be inevitable) brings its own challenges, for example the ***ongoing tension*** between the GDPR and PSD2 in Europe. We discuss this in more detail in the "other comments" section below.

19	*How could a consumer data right be designed to protect the interests of vulnerable consumers?*
	We support the adoption of measures to protect the interests of vulnerable consumers. For example (as discussed in our response to question 16), include mandating a privacy impact assessment prior to introducing a CDR; auditing for fairness, discrimination, inclusion/exclusion of a given scheme; mandating heightened data security standards for entities holding/transferring consumer data; shifting as much of the burden off the individual as possible. Other design elements we have observed include things like introducing constraints around data transfers along the lines of financial services, e.g. it's easier to transfer $1000 than $100,000; limits on the number of transfers within a time period, etc. We also believe that a standard approach to delegation and custodianship is required.
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?*
	We fully support Te Tiriti o Waitangi and the meeting of the Treaty Partner's responsibilities, but we are in a not in a position to comment on this question.
21	*How could a consumer data right be designed to ensure that the needs of disabled people or those with accessibility issues are met?*
	Amongst other design factors and accessibility principles, a delegation and guardianship framework would support this.
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?*
	If development of a consumer data right framework is developed in NZ, it should take account of global developments to the extent it enables us to learn and lead. NZ is in a unique position in this regard. We have the benefit of being able to avoid the mistakes other jurisdictions have made that have led to negative economic and societal outcomes. From observing other regimes, we have identified several learnings that NZ could implement in order to avoid the challenges faced in other jurisdictions: • Effective consumer data portability rights are ineffective without a trusted digital identity eco-system. • The data sharing mechanism needs to be at the centre of the governance framework. This should fall under the ambit of the DITF. • In order to achieve data portability at scale, the authoritative agency should develop a decentralised but verified registry of accredited third parties. Without it the regime will struggle to scale or achieve operational cost control. The ***Verifiable Organisation***

Network in Canada is an example of registry that can be used for this purpose (amongst many others).

- Promote a common data definition and ***schema governance approach -*** rather than focusing on APIs which bind you into the delivery model. Avoid promoting consent / interaction models that unwittingly binds a customer more tightly to their initial service provider/data holder.

- Ensure the data sharing and interaction mechanisms support C2B as well as B2B models - Where a customer has the information, they should be able to share it (the verifiable credential standard coupled with a DID is an effective model).

- Avoid developing regimes in siloes. GDPR and PSD2 are related yet were developed separately. This led to the creation of multiple standards across the EU economy, and unresolved tensions between the two. Moreover, because the general data subject right to data portability in the GDPR was not designed in tandem with Europe's approach to digital identity or eID, there has already been significant ***fraud and abuse*** (as described in ***this link****)* of the data portability and other data subject access rights under the regulation.

Finally, compatibility should be considered from a trade perspective. Global efforts to regulate the digital economy are growing at pace, including among some of our key trading partners, in both the Asia-Pacific and Europe/the United Kingdom. Both data and data portability are key underpinnings of digital trade and digitally-enhanced trade today. Artificial intelligence and big data analytics (often made possible through IoT) are increasing the importance of how data is governed and used. NZ must take account of international developments to leverage the greatest benefits from the global digital economy but also to safeguard our own interests in it.

This may in fact be an area where we can lead in global policymaking, including, for example, as part of our current negotiations for a free trade agreements with the UK and European Union respectively, and in our host year for APEC in 2021, where there is a significant workstream on policymaking in the digital economy, likely including the topic of data governance issues.

23	*Do you have any comments on where a consumer data right would best sit in legislation?*
	Please refer to the "other comments" section at the end of this document. If option two or three is pursued, a high level framework in primary legislation, with details in secondary/tertiary legislation is likely most practical. We strongly recommend that if the CDR is pursued, then the CDR and DITF sit under one common agency. As detailed in the "other comments" section, the optimal position would be for elements of the CDR to be incorporated within the DITF.
24	*Do you have any comments on the arrangements for establishing any new bodies to oversee parts of a consumer data right?*
	As above, if the CDR is developed we would like to see common bodies established under CDR and DITF, housed within one agency. For example, it would also make sense for the two regimes to share a common accreditation scheme. However, as discussed in the "other comments" section, the optimal outcome is that elements of the CDR are incorporated within the DITF.
25	*What are the pros or cons of having multiple regulators, or a single regulator, involved in a consumer data right?*
	The cons of a multi-regulator approach include greater risks around decision making (timing, clarity of decision making and decision making power) both of which can lead to uncertainty.

	For these reasons we support a single regulator approach, but one that is obliged to coordinate closely across Ministries/Regulators of relevant sectors to ensure that approaches are consistent and fit for purpose.
26	*If government decides to establish a consumer data right, do you have any suggestions of how its effectiveness could be measured?*
	Some metrics include: – Value generated/costs saved. – Number and categories (demographics) of individuals requesting sharing/transfers of data per the CDR. – Frequency of use by individuals & categories of individuals (demographics) – Time to complete tasks, e.g. the switch phone companies or energy providers – Number of user generated transactions – Volume of data shared – Number of entities seeking accreditation – Number of entities accredited

Other comments

Introduction

MATTR welcomes the opportunity to comment on the New Zealand Consumer Data Right Consultation. Below we discuss an alternative and in our view more viable approach to the proposed CDR.

MATTR supports the policy goal of consumer data portability, and the creation of a legislative environment to achieve it in full. However, in consideration of existing policy efforts and the building blocks necessary to create the enabling environment for consumer data portability, we view the creation of a stand-alone Consumer Data Right framework to be regretful. We discuss the reasons below.

As our reliance on the digital economy grows, data portability in the context of government and private sector services, and interoperability between them is critical. A right to data portability will give consumers greater access to services, and help New Zealand **("NZ")** entities to keep pace with innovation in other jurisdictions.

In our view, there are two key building blocks that are required to enable data portability across the economy. These are best placed to be developed by Government and grounded in a regulatory environment. First, **consumers** need a general, legislative right to data portability. Second, **entities** need a legal framework of common standards (both technical and non-technical) to operate within to enable the data portability and interoperability that is sought.

Existing Efforts to Enhance Data Portability

In the past three years we have observed **three** relevant but different attempts to increase data portability in NZ. Each effort has been initiated by a **different** government agency. Whilst we recognise the varying historical origins, we note that each effort seeks the common outcome of enhanced consumer data portability. The efforts are as follows:

1. Office of the Privacy Commissioner's recommendation for Privacy Act Reform (2017)

a. In its ***Report*** to the Minister of Justice in 2017, the Commissioner's first recommendation was to introduce a right to data portability in the proposed modernisation of the Privacy Act.
b. If included in the Privacy Act 2020, **this would equate to the first of the two key building blocks referred to above.**
c. If this recommendation was followed, the 'consumer data right' (for individual data) as proposed in the CDR Discussion Document **would not be necessary**. We view the Privacy Act as the appropriate place for an individual right to data portability, with our reasoning included below.
d. We note this recommendation has not ***as yet*** been adopted in the Privacy Act 2020.

2. The Digital Identity Trust Framework (2018-ongoing)
    a. In July 2020 ***Cabinet agreed*** to develop a Trust Framework for NZ.
    b. The Cabinet Paper confirms the creation of a Trust Framework to accelerate and govern the development and uptake of "user-initiated, digitally-enabled sharing of personal and organisational information" *(data portability).*
    c. The legislation proposed includes the components proposed in the CDR Discussion Document.
    d. **The Trust Framework equates to the second of the two building blocks referred to above.**

3. The Consumer Data Right consultation (2020)
    a. The present ***consultation***.
    b. The discussion document proposes an Act to govern user initiated data sharing (*data portability*) in either a *limited* (option two), *economy wide* (option three) or *sector specific* (option four) manner.
    c. For the reasons discussed below, option two and four will detract from (1) and (2) above. Option three is not required once (1) and (2) are implemented.
    d. For these reasons, we view the proposed CDR as regrettable.

Additional regimes (such as CDR) will lead to uncertainty, complexity and rework.

With due respect, and after careful consideration, we are of the view that the policy goal of data portability should (and can) be achieved through the Trust Framework and Privacy Act.

The Privacy Act is the most appropriate legislative regime within which to establish an individual right to data portability (*building block one*). This is primarily because data portability is regarded as a logical continuation of an individual's existing right to access their personal information (Principle 6, Privacy Act). As set out in the Report, without portability, an individual's ability to meaningfully exercise the right contained in Principle 6 may be rendered illusory (at page 5). Including a general data portability right in primary privacy legislation is also more aligned with best practices at the international level and more likely to promote cross-border compliance and legal interoperability.

The Trust Framework is the most appropriate place to provide entities with a framework of common standards (both technical and non-technical) to operate within to enable the data portability and interoperability that is sought (*building block two*). This is because Trust Framework is scoped to govern the user-consented, digitally-enabled sharing of personal and organisational information.

The CDR proposes three options for legislative intervention. Option two attempts to introduce both building blocks (a right for individuals, and governance of entities) potentially in a single Act, but in a segmented and limited manner. **If CDR option two is pursued, it will create a separate but limited regime to govern certain aspects of data portability in a way that will create tension and complexity with broader efforts such as the Trust Framework**. Innovation will decrease as entities attempt to navigate an incoherent legislative environment. In our view this will require significant rework in the near term to function effectively and align with global efforts.

Option three is an attempt to implement an economy wide consumer data right, potentially in a single Act. Whilst option three is broader, and therefore more future focussed and aligned with global efforts, it will **not be required if the Privacy Act is updated and Trust Framework implemented.**

We note that the CDR Discussion Document repeatedly states (and in our view, takes for granted) that the CDR will increase productivity and efficiency. The introduction of the proposed CDR will create a disjointed legislative environment that will decrease productivity and efficiency. The best way to enhance data portability in NZ is to continue to develop and advance the two existing regimes – the Privacy Act and the Trust Framework, rather than creating another (potentially conflicting) one. Additional regimes, particularly option two as proposed, will lead to uncertainty, complexity and rework. Viewed alongside the Privacy Act and Trust Framework, the proposed CDR regime is found wanting.

The components proposed in the CDR discussion document are already covered by the Trust Framework.

Section Four of the CDR Discussion Document (titled "Design of a Consumer Data Right" on page 19) identifies a number of areas that the legislation would seek to cover. We note that these areas overlap (or as with (1), conflicts) with the components *already* proposed under the Trust Framework. We discuss these below.

1. **Establishing a CDR that can be designated to specific sectors through secondary or tertiary legislation**
    a. This conflicts with the two aforementioned efforts that (in our view, correctly) seek to establish an individual right to data portability in a sector agnostic manner.
2. **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**
    a. The Trust Framework sets out the potential eco-system roles *(**page 3**).* These roles encompass data holders. Types of data could be developed as a subpart of the rules in the Trust Framework (see below).
3. **Providing for detailed rules for accessing and transferring data to be set during the designation process**
    a. Trust Framework will include rules for the user-consented, digitally-enabled sharing of personal and organisational information in an interoperable manner.
    b. The Cabinet paper states on ***Page 6*** that Trust Framework will "*create an enabling regulatory environment that will support better information sharing and management practices, by establishing commonly adhered to best practice rules and standards in New Zealand".*
4. **Establishment of an accreditation regime for third parties**
    a. Cabinet has agreed (***page 13 Impact Statement***) that the Trust Framework will develop and establish an accreditation regime.
    b. Providers will be accredited against the rules once the statutory Trust Framework is in place in 2022.
    c. The Providers that will need to seek under the Trust Framework overlap with those that would be considered to be "third parties" under the CDR.
    d. In order to avoid creating unnecessary costs for small to medium enterprises and agencies, it is critical that there is *one cohesive accreditation regime for these entities, governed by a single agency.* It is our view the accreditation regime should continue to be developed under the Trust Framework.
5. **Strengthening privacy safeguards**
    a. Privacy is considered in the Trust Framework Cabinet paper.
    b. As stated on ***page 5***, the Trust Framework will set out "rules that accredited participants must follow, with a focus on identification, *privacy* and security requirements that are based on laws and standards that are either existing or in development.
    c. The Trust Framework will also be subject to primary privacy legislation itself.

d. Comment from the Office of the Privacy Commissioner is included on ***page 9***.

6. **Establishing an enforcement regime and methods for consumer redress**
    a. The Trust Framework will be grounded in legislation providing a clear mechanism for legal enforceability upon system participants, and a method for consumer redress.
    b. As stated by the DIA in the Cabinet paper (***page 28 Impact Statement)*** *"Evidence gathered through the Department's engagement process indicated stakeholders generally wanted a government-led intervention, that combined rules, compliance testing and legal enforceability, and could be established in a timely manner"*.
    c. The enforcement regime is anticipated in phase two of Trust Framework development.

Consumer Consent

As discussed in our response to the questions, the CDR does not directly engage with consumer consent, or indicate how the tools mechanisms for consumer consent would be governed. A consent framework is a critical component of any data portability regime. We note that the Trust Framework addressed this by proposing to accredit Infrastructure Providers which "enable people to disclose their information and consent to share it" (***page 5 Impact Statement***) and by placing the consumer at the centre of the model (as shown in ***Figure 1***).

Coherent governance led by one entity

We strongly recommend that the framework of common standards for entities to operate within *(the second building block)* be developed and governed by one lead agency. Data portability is a complex and technical area. This requires strong consistent governance. The cost of entities having to deal with multiple agencies outweigh the benefits. Further, **by housing the policy effort in one agency, NZ will be in a better position to avoid the *tensions* that still exist in other jurisdictions which created different but intersecting regimes under different agencies**. PSD2 and GDPR in Europe is a clear example of this, and the issues that arise when a sector specific CDR is implemented alongside a general right to portability. The broader economic implications of failing to use the Trust Framework (and associated accreditation regime) are significant, as many entities across New Zealand have invested considerable time and effort not only in the consultation, but in preparing for the policy direction it has announced.

Conclusion

We hope that from our submission it is clear that we fully support the government's policy goal of enhanced data portability, and the creation of a legislative environment to achieve it. We hope our submission helps to guide the development of a coherent and enabling legislative environment for data portability in NZ.