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

Your name and organisation

Name	Scott Miller
Organisation	New Banking Ventures

Responses to discussion document questions

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?*

Inertia – we are used to duplicating our information

Individuals have got used to recreating and in effect duplicating their personal data to each of the platforms, sites or business relationships they have. Regulations like AML/CFT have necessitated this where the case for data sharing from an authoritative source ought to be overwhelming. Hence there is low expectation of sharing between platforms today when we can't share basic data like that used for KYC (although that may be more to do with lack of trusted identity framework). Furthermore, it may well be easier or faster to duplicate our personal data in new or competitive services than wait for a sharing feature between service providers. Some may prefer different profiles for different purposes even if the personal data behind each is the same.

Inertia – we are used to our consumer data being captive

Consumers are used to data being captive to the organisation it relates to and may not see the possibility of what could be achieved via sharing.

Lack of identity trust framework

Without reliable methods for validating digital identity and a trust framework, it is difficult to provide a ubiquitous data sharing ecosystem, rather many point solutions proliferate and instead of data sharing, there is data duplication. The CDR needs to go hand in hand with efforts to establish a Digital Identity Trust Framework.

Complexity added due to lack of unique ID to enable matching

Without a unique ID it isn't possible for entities to match existing consumer data with data being shared. Understanding which profiles represent a single or "common customer" is key. In jurisdictions with personal ID numbers this isn't the same challenge (e.g. most of the EU).

No mandated need for explicit consent

Data sharing is predicated on trust which starts with a robust and secure identity framework, and one which ensures "explicit consent" per purpose would need to be provided as a key safeguard (so authorisation would not be a default), and also the mechanism to rescind such consent and remove related sharing.

Inefficiency in sourcing of personal information

	One other challenge is the inefficiency of the sourcing and provision of personal information, often duplicating the process at every business relationship onboarding at a cost to the economy. A way for true "data sharing" of up-to-date personal information either from the individual or between agencies is absent. Indeed the Privacy Act 2020 appears to require the individual to provide the information and not to be able to source it from a third party thus restricting data sharing. Other Acts like AML/CFT may also add to this inefficiency for KYC and CDD.
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?*
	Yes
3	*Are there additional benefits, costs or risks that have not been explored in the above discussion on a consumer data right?*
	Costs – **necessitates standardisation** and an agreed governance model for multi-party data sharing via agreed common APIs and data formats, whether managed sector by sector (preferred) or universally Costs – **safeguards and accreditation** of agencies able to participate in data sharing esp in regulated sectors Costs – **strengthening Privacy Act 2020** to facilitate more safeguards and rights Risks – **lack of regulatory convergence** if a significantly different outcome compared to ACDR is put in place. Divergence from "stronger" regimes like the EU GDPR may be a risk for globally active NZ organisations which need to implement controls to a stronger regime than locally required in order to satisfy their overseas market requirements.
4	*What would the costs and benefits be of applying the consumer data right to businesses and other entities, in addition to individuals?*
	Cost in development and governance of the standards that include common data items subject to CDR, sector specific data subject to CDR and should allow for optional elements into the standards not subject to CDR – derived data. There will be a cost to maintaining the standards and their governance as an ongoing process, likely sector-funded where sector-designated. **Cost in implementing to the relevant standards** for an entity will depend on its sector designation, and within the sector, its business coverage and product offerings. To be able to partake in the ecosystem effectively certain minimum data (by product type) would be expected and that should be defined in the standard(s). If a consumer has that type of product then the standard for sharing the consumer data related to it is set. Likely as products innovate this level could be changed over time or be broader in certain sectors than others. The standards shouldn't just define the minimum level but be an extensible model and a business should be able to choose the extent to which it provides additional and/or optional APIs and for what data for read and/or write access, so that the costs/benefits and implementation timeline are able to be managed by the business entity.

Cost of compliance Businesses and other entities are inevitably going to absorb the costs of applying the CDR in their operations which will be factored into pricing and indirectly as a cost passed to consumers. This might be more burdensome in certain sectors than others and dependent on the degree of digitalisation and complexity of the consumer and product data footprint. The degree of motivation to take costs will in part relate to whether there will be penalties for not complying vs allowing market forces to determine the sufficiency of an entity's data sharing with third parties (both data under CDR and optional elements) and spur innovation, or result in consumers moving to a competitor if unsatisfied.

No direct cost to individuals, for data subject to CDR. However, there may be costs for other optional data services provided via data sharing standards and this may be through, e.g. cost of an app or subscription service, or services are freely offered to generate a competitive advantage and attract customers, e.g. many FinTech partnerships providing consumer addons to mobile banking platforms in the EU with the bank absorbing the cost. Conversely individuals and their business partners should not be prevented from monetising the sharing of their personal information.

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')?*

Consumer Data – Provided and Observed data should certainly be subject to CDR. Derived data may actually be where the business value is to the consumer but this data should not be subject to CDR but may be part of the optional data that may also be included in the same data sharing standards so also able to be shared by making use of the same implementation for API standards, rules, third party accreditation, safeguards, standards and rules etc as for CDR.

Product Data – sufficient to make sense of the consumer – product relationship but more could also be provided via the optional part of the data sharing standard so not specifically part of the CDR but this is where the business case will be to enable the products and services to be enumerated so third parties can offer them. Market data is derived and could use the same data sharing standards but not be subject to CDR.

Determining relevance - within the data sharing standards, it will be key to determine what data, and what data actions are to be subject to the CDR for the entity as distinct from the wider set of derived data and actions that may be optional or not applicable depending on a given business context.

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

A CDR necessitates a secure and trusted accreditation framework for the third parties a consumer wishes to use with stricter hurdles for third parties intending to use write access APIs provided by an entity.

The regulatory burden in terms of liability needs to be placed fairly especially as the ecosystem blurs the lines between parties and their interchangeable roles (given the potential for ever more complex multi-directional information sharing there are an emerging risks that "no one" is in control of the individual's data or that the obligations are "circular" and unresolvable, e.g. how to resolve inaccuracies when A shares with B, B with C, C back with A).

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?*
	Outcome to include a form of "right to be forgotten" is relevant since if the outcome is for an ability to share data, then the reverse, the ability to rescind that sharing needs a mechanism. The extent could be the question – from reliance on the removal of consent, through to right to removal of data. The Privacy Act 2020 does not provide for a "right to be forgotten" principle, however there are provisions that would give rise to this although more weakly – when authorisation is rescinded and legitimate purpose removed, however the determination of removal of the latter is not in control of the individual concerned. **Outcome to include data portability for "switching"** Consumer-driven "portability" does extend beyond "data sharing" to also "switching" where the intent is the move of data from one provider to another and this is prevalent already in competition cases where ease of provider switching is mandated or common practice e.g. mobile phone nr portability between operators, or current account switching between banks as in the UK, or energy provider switching also as in the UK. This could be seen as an extreme form of "data sharing" that involves transferring to the new provider and removing it from the original. Although the mechanisms to transfer the necessary data may be the same as implemented for "data sharing" as provided for by a CDR there are often significant costs to provide this and more obligations on the parties involved for "switching" and the support for such needs to be motivated by more than the rights that the CDR provides alone, e.g. mandates in other legislation or industry guidance, however the "switching" use case should not be forgotten in the types of data portability being envisaged. **Outcome to allow sharing for KYC** Today KYC doesn't allow grandfathering of data between banks and results in duplication of processes and data from a consumer's perspective. An outcome should be to strengthen controls to enable data sharing to support concepts like an industry or sector KYC utilities to centralise this information to allow sharing with accredited sector participants to improve the quality and accuracy of consumers' personal identifying data and reduce cost in acquiring it at point of onboarding a new business relationship and in keeping it up-to-date.
8	*Do you have any comments on our proposed criteria for assessing options? Are there any additional factors that should be considered?*
9	*Do you have any comments on the discussion of Option one: Status quo?*
	No
10	*Do you have any comments on the discussion of Option two: A sectoral-designation process?*
	This is the option that allows a designation to mandate the framework sector by sector and may be closest in alignment with ACDR allowing more regulatory alignment with our closest market.

	Sectoral designation could keep the sectoral data set narrow enough and the number of APIs to a manageable number, allowing governance of the standards to be effective. Having a sectoral designation may create boundary issues for outside of sector participation, e.g. accreditation, obligations. As noted in Q15, it may not be sufficient on its own.
11	*Do you have any comments on the discussion of Option three: An economy-wide consumer data right?*
	If the mechanisms for sharing are to be universally standardised and codified via this option, then it could be too complex to implement. It is easy to foresee a proliferation of requirements for slightly different data sets and APIs for similar purposes giving rise to inability to agree standards resulting in governance and implementation bottlenecks. Cross-sector sharing between non-regulated and regulated sectors could also lead to governance issues as well. See Q13 as there are variants to this option that might be more feasible.
12	*Do you have any comments on the discussion of Option four: Sector-specific approach?*
	Option four may be faster than option two to put in place. Reference to option four having worked in the EU and UK with Open Banking is based on being underpinned by the foundational and economy-wide data portability rights enshrined in the EU GDPR, which is more akin to the EU having effected option three in terms of a generic foundational data portability right which is universally applied, and then implemented option four on top. The implication is that option 4 also needs some Privacy Act underpinning to work.
13	*This discussion document outlines four possible options to establish a consumer data right in New Zealand. Are there any other viable options?*
	As noted above in Q11, there is a variant to option three that is a minimal version - "**economy-wide – minimum data right**" option, to make a level playing field for all and be used to strengthen foundational aspects in the Privacy Act 2020 which would be sector independent, like the right to personal consumer data access in an electronic form and enable its correction (Privacy Act 2020 Information Privacy Principles 6 and 7), and crucially to also establish a new generic data portability principle which stops short of enshrining the extent of the right. This could be applied across the economy universally and could then be combined with option two to apply the right by sector designation. Without some minimum right across the economy there will be blind spots in sectors not designated.
14	*Do you have any comments on our initial analysis of the four options against our assessment criteria?*
	The options do not need to be mutually exclusive Aspects of option four could be a stepping-stone towards option two to enable trials and

	sandboxing while the necessary secondary/tertiary legislation is run through for option two.
15	*Do you agree or disagree with our assessment that Option two is most likely to achieve the best outcome using the assessment criteria?*
	Option two is not likely to achieve the best outcome on its own A combination of… An alternative option three "economy-wide – minimum data right" – to make a level playing field for all and to be used to strengthen foundational aspects in the Privacy Act 2020 which would be sector independent, like the right to personal consumer data access in an electronic form and enable its correction (Privacy Act 2020 IPP 6 and 7), and crucially to also establish a new generic data portability principle which stops short of enshrining the extent of the right (which would be left to option two to implement via secondary/tertiary legislation). Plus option two "sectoral-designation" with implementation consideration for aspects of option four as a stepping-stone if this is faster to get going towards option two while the necessary secondary/tertiary legislation is run through.
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?*
	The high-level framework could add a minimum data right principle to be applied to all across the economy – to make a level playing field for all and be used to strengthen foundational aspects in the Privacy Act 2020 which would be sector independent, like the right to personal consumer data access in an electronic form and enable its correction (Privacy Act 2020 IPP 6 and 7), and crucially to also establish a new generic data portability principle which stops short of enshrining the extent of the right (which would be left to option two to implement via secondary/tertiary legislation). And then a sectoral-designation following option two layered on. Otherwise agree.
17	*Do you have any feedback on our discussion of any of these key elements?*
	No
18	*Are there any areas where you think that more detail should be included in primary legislation?*
	Yes, the opportunity is to strengthen the minimum data rights and how they are applied to all across the economy – both to make a level playing field for all and to strengthen some foundational aspects in the Privacy Act 2020 which would be sector independent, like the right to personal consumer data access in an electronic form and enable its correction (Privacy Act 2020 IPP 6 and 7), and crucially to establish a new generic data portability principle which stops short of enshrining the extent of the right and can be left to

	secondary/tertiary legislation.
19	*How could a consumer data right be designed to protect the interests of vulnerable consumers?*
	It may be possible to design provisions in the accreditation framework for mechanisms to support vulnerable consumer protection and possibly use a "best interests" test, however, it does raise the question of whether such rules should be independent of the source of the consumer data – whether shared to or from a third party or directly sourced – to avoid less protection for those not sharing their data than for those sharing it. Also it raises the question of how to identify vulnerability and what protections are on this kind of data and will consumers consent to sharing of their vulnerability status, as well as where the obligation lies – on the entity sharing or on the entity using the shared data.
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?*
	No
21	*How could a consumer data right be designed to ensure that the needs of disabled people or those with accessibility issues are met?*
	Accessibility considerations should be seen as independent of the source of the consumer data – whether shared to or from a third party or directly sourced. Accessibility considerations are rather more related to the channel and the relevant usability requirements of that and not related to the source of the data displayed, therefore should not be an implementational consideration of the CDR itself.
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?*
	Regulatory convergence is key to a future where data sharing may become regional or global. The advent of the EU GDPR is an example of regulatory convergence away from prior country specific Data Privacy Acts in each of the member states, benefiting cross-border innovation and protection of consumers across the union independent of where the data is held. A data portability principle broadly in convergence with EU GDPR would certainly set an upper bar, and likely it makes sense to at least consider compatibility regionally with what the ACDR provides for.
23	*Do you have any comments on where a consumer data right would best sit in legislation?*
	The Privacy Act 2020 could be the basis in primary legislation. One need is to define data portability and the CDR as a new generic Information Privacy Principle (IPP) to be applied universally in such a way as to allow for the extent of the right to be applied via a sectoral designation following option two.

24	*Do you have any comments on the arrangements for establishing any new bodies to oversee parts of a consumer data right?*
	No
25	*What are the pros or cons of having multiple regulators, or a single regulator, involved in a consumer data right?*
	Sectoral regulators, where present, should own the sectoral designation, standards, accreditation etc. The Privacy Commission should own the over-arching framework.
26	*If government decides to establish a consumer data right, do you have any suggestions of how its effectiveness could be measured?*
	No

Other comments