Ciaran Ward

Leveraging Australia's Lessons: Finding the balance between functionality and commercial viability of the Customer and Product Data Bill

LLB (Honours) RESEARCH PAPER
LAWS 489

FACULTY OF LAW

VICTORIA UNIVERSITY OF WELLINGTON
TE HERENGA WAKA

2023

Contents

Abstract

The implementation of a Consumer Data Right (CDR) in Australia pioneered an economy-wide data portability framework, setting a precedent for others to follow. New Zealand is poised to adopt a similar model, and in June 2023, unveiled the New Zealand Customer and Product Data Exposure Draft Bill for public scrutiny. This paper offers an overview of the CDR and evaluates whether New Zealand's legal framework and implementation strategies can circumvent the hurdles that impeded the CDR's adoption in Australia. Ultimately, the author argues that without sufficient industry and consumer participation, the CDR's efficacy and long-term viability are at risk - concessions must be made to ensure the CDR attracts both customers and industry players. This paper considers action initiation, the decision to utilise existing Privacy Act IPPs, the exclusion of reciprocal data sharing and the considerations of Māori Data and Māori Data governance.

Subjects and Topics

"Customer and Product Data Bill" "Consumer Data Right" "Consumer Data" "Open Banking"

Word length

The text of this paper (excluding abstract, table of contents, footnotes, and bibliography) comprises approximately 7992 words.

I Introduction

The implementation of a consumer data right (CDR) in Australia established the beginnings of an economy-wide data portability framework, heralded as first-in-kind.[1] New Zealand intends to follow suit by establishing a regime based broadly on the Australian model.[2] June 2023 saw the much-anticipated New Zealand Customer and Product Data Bill (the draft law) released for public consultation.[3] New Zealand's legislature will have the benefit of learning from Australia's implementation, which, as with any novel legal or regulatory framework, has experienced growing pains.[4]

When crafting legislation, striking the correct balance between conflicting interests is a significant but important challenge. This is particularly critical in the context of a regulatory regime which seeks to enshrine in law the ability for consumers to control data held about them. As such, legislation must simultaneously enable key functionalities to address regulatory demands while garnering widespread acceptance from consumers and industry stakeholders. Without sufficient participants, a CDR will fail to be effective.[5] Australia has been unable to strike this balance, struggling to amass industry and consumer participation in its CDR.[6] This lack of participation is partly explained with reference to the legislative choices in its framework.

The initial implementation and performance of the CDR in New Zealand will greatly determine its long-term use and effectiveness.[7] Therefore, New Zealand must be practical in its implementation to ensure its success. Ultimately, there is little value in designing a theoretically perfect framework that fails to gain traction in real-world implementation.

---

[1] See Treasury Laws Amendment (Consumer Data Right) Act 2019 (Cth).

[2] Ministry of Business Innovation and Employment *Discussion document*: *unlocking value from our customer data* (June 2023) at [45].

[3] See Ministry of Business Innovation and Employment *Draft for Consultation: Customer and Product Data Bill (Exposure Draft Bill) (2023)*

[4] See, generally, Elizabeth Kelly *Statutory Review of the Consumer Data Right* (Australian Government Treasury, 2022).

[5] Scott Farrell *Banking on Data - Evaluating Open Banking and Data Rights in Banking Law (*Kluwer Law International B.V, The Netherlands, 2023) at 111.

[6] Elizabeth Kelly, above n 4, at 41 – 42.

[7] See Farrell Page, above n 5, at 113.

The draft law, designed by the Ministry of Business Innovation and Employment (MBIE), proposes to depart from the Australian model in numerous ways relating to consumer protection and the regime's functionality. Key departures include the approach to the application of privacy principles and the functionality of the regime stemming from the inclusion of write access and exclusion of reciprocity.[8] Furthermore, unique to New Zealand, emphasis is placed on Māori Data Sovereignty.[9]

This paper aims to provide an overview of the CDR. Then, it considers whether New Zealand's legal framework and implementation are well placed to avoid the issues that have inhibited private sector adoption of the CDR in Australia.[10] Ultimately, the paper argues that concessions must be made to ensure the CDR has sufficient appeal to customers and industry.

II What is the Consumer Data Right

The CDR is the legislative implementation of data portability – in this context, the ability to move data between a holder of data to a third party.[11] In New Zealand, this will include the requirement for data-holders to make product data available electronically,[12] and the ability for an individual to mandate a registered data holder to share their personal data with a third party, such as an accredited requestor (AR).[13] The requested data will be shared in a standardised machine-readable format so an AR can use it for the customer's benefit.[14] Differing from industry-specific data portability, such as Open Banking, a CDR provides for an expansive economy-wide right of data portability.[15]

---

[8] See Ministry of Business Innovation and Employment, above n 2, [87], [97].

[9] See Generally, *Iwi Data Needs* (Te Kahui Raraunga, 12 March 2021) and *Māori Data Governance Model* (Te Kahui Raraunga, 26 May 2023).

[10] A paper on the CDR has the potential to be multi-faceted. Complex issues exist around the design and considerations behind individual sectorial designations, the accreditation of parties, and many issues from a technical implementation standpoint. Discussing the CDR's technical implementation is largely beyond this paper's scope.

[11] See Ministry of Business Innovation and Employment, above n 2, at [13]. See also Elizabeth Kelly, above n 4, at 3.

[12] For example, this can include a company's product offerings and product eligibility requirements.

[13] Customer and Product Data Bill Exposure Draft Bill 2023, above n 3, s 15.

[14] Ministry of Business Innovation and Employment, above n 2, at [164].

[15] See Scott Farrell *Future directors for the consumer data right* (Australian Government Treasury, October 2020 at 1) and see also Ministry of Business Innovation and Employment, above n 2, at [46].

This can be contrasted against the current system, where such data is largely unavailable, or a customer must personally supply any third party with the relevant information.[16] Information can also be supplied through unsecure and rudimentary data-sharing methods such as screen scraping.[17]

The CDR is designed to be a competition and consumer protection regime, requiring data sharing to be at the customer's request. The CDR does not empower data holders to unilaterally share customer data with other parties for their own benefit.[18]

When conceptualising the CDR in New Zealand, it is helpful to distinguish its features from existing data rights established by the Privacy Act 2020. Under the Act, individuals can request personal information held about them from data holders. This process can take up to 20 days and can be at a cost.[19] Further, the information provided is not necessarily in a standardised form and is not available to any AR unless provided by the customer. The CDR builds on this limited right to data provided for in the Privacy Act.

A Key Instruments of the CDR Framework

The draft law is high-level legislation consisting of rules which create a framework for how the CDR will operate in each designated sector. Once enacted, this will be supplemented by secondary legislation - namely sector-specific standards containing technical specifications.[20] Each instrument is subject to its own concerns and debates, which are beyond this paper's scope; as such, the description of these concepts will be brief. Essential to the operation of a CDR are the concepts of designation and accreditation.

---

[16] Negotiating bespoke data-sharing agreements without any underpinning by a CDR is possible. These exist sparsely (but primarily in the open baking sphere). See Xero's arrangement with ANZ for example. Xero "ANZ NZ direct feeds" Xero Central <central.xero.com>

[17] Screen scraping typically involves a third-party logging into a customer's account and "scraping" the required information. These authorizations may not meet information privacy principles under the Privacy Act 2020, and consumers may not be aware of what data is being collected and how it is being used. See "What is Open Banking" WS02 <ob.docs.wso2.com>

[18] Note that the Privacy Act allows de-identified data to be shared without consent. See Privacy Act 2020, IPP 10. MBIE is considering whether consent should be requirement in the CDR. See Ministry of Business Innovation and Employment, above n 2, at [143]. Numerous submissions (primarily from incumbent data holders) to the exposure draft bill are disagree with the requirement for consent to use de-identified data.

[19] Privacy Act 2020, pt 4.

[20] Ministry of Business Innovation and Employment, above n 2, at [76].

Sector designation

Like Australia, the draft bill provides that the CDR will be implemented on an industry-by-industry basis.[21] Any industry/sector is to be designated by the Minister of Commerce and Consumer Affairs.[22] After a sector is designated, all "in-scope" data will be subject to data portability. For each sector, this legislative designation will specify the types/scope of data, parties eligible to be data-holders, the functionality enabled and the rules and standards governing data transfer.[23]

Accreditation

The draft law will create an accreditation regime for those who want to make binding requests for designated customer data.[24] Accreditation regulates the approval to enable parties to be accredited as ARs[25] and attempts to ensure that a provider will meet the trust under the Bill and future secondary legislation.[26] Overseas experience shows that it is vital for any data-sharing regime to have a high level of trust.[27] Importantly, entities that are not accredited can request data, but there is no obligation for data holders to respond.[28]

B How it will work

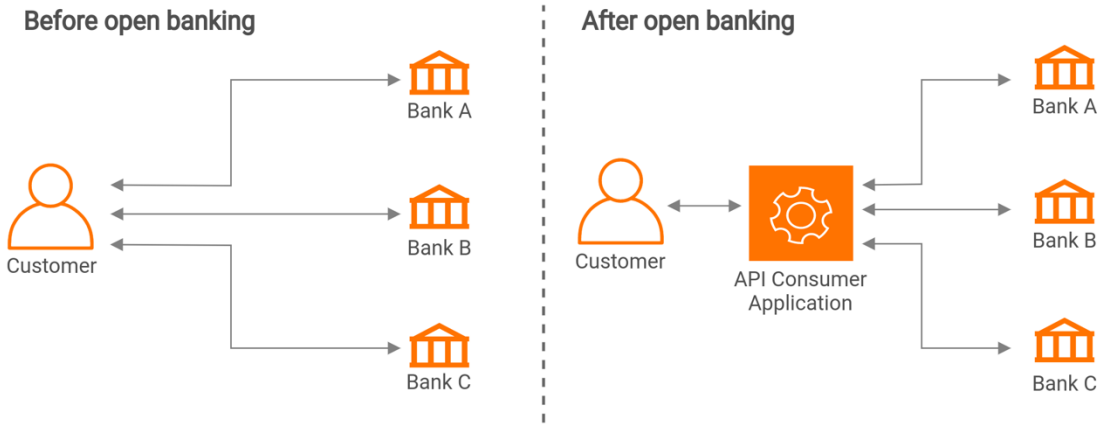
Broadly speaking, the CDR will be technically enabled by Application Programming Interfaces (APIs).[29] At its core, "an API is a documented set of connecting points that allow an application to interact with another system."[30] These APIs can autonomously process

[21] See Customer and Product Data Bill Exposure Draft Bill 2023, above n 3, pt 5.
[22] Clause 84.
[23] Part 5.
[24] Part 5, sub-part 2.
[25] Clause 64 – 73.
[26] See definition of accreditation. Ministry of Business Innovation and Employment, above n 2, 5.
[27] Note that the discussion document states it will be an offence for requestors to represent themselves as accredited falsely. See Ministry of Business Innovation and Employment, above n 2, at [87]. **Section C** of this paper discusses accreditation in the context of action initiation.
[28] Customer and Product Data Bill Exposure Draft Bill 2023, above n 3, cl 7.

[29] "What is Open Banking" TIBCO Software <tibco.com>.
[30] Laura Brodsky and Liz Oakes *Data sharing and open banking* (online ed, McKinsey&Company) at 5.

transaction information and communicate from one data-holder or AR to another.[31] The below diagram illustrates where APIs would sit in the banking system.

Diagram 1 – Visualisation of APIs in Open Banking [32]



An important factor to bear in mind is that APIs can be open or proprietary.[33] Without a CDR regime, the few existing data-sharing arrangements are enabled by bespoke agreements.[34] In each industry, large companies would likely issue a set of APIs accompanied by potentially unfavourable terms and conditions, which partners will be pressured to accept.[35] Introducing standardised APIs and terms and conditions is important, as parties with less bargaining power could be placed under the burden of negotiating separately with potential partners. Without set standards, each data holder, by adopting their own systems for providing data, would necessitate each data recipient to build,

[31] TIBCO Software, above n 29.
[32] WS02, above n 17.
[33] Open APIs are freely available to the public and typically not managed by an directly interested party. Closed or proprietary APIs are designed and maintained privately and can only be used if access is granted See Cameron McKenzie "Open API" TechTarget <techtarget.com. and Brodsky and Oakes, above n 30, at 5
[34] For example, the partnership struck by ANZ and Xero allowing small to medium businesses to streamline their accounting.
[35] Brodsky and Oakes, above n 30, at 5.

maintain and update customised systems for retrieving and processing data from multiple data holders.[36] This would add untenable cost and complexity to the system.[37]

While not dictated by the draft law, similar to the Australian Act, each designation will issue standardised data standards and APIs. These standards will build on the work the New Zealand API Centre has already undertaken.[38]

III Implementation of the CDR in Open Banking

At times, the CDR can appear to be an abstract concept. Therefore, it is helpful to conceptualise the CDR through practical application. The most prominent use of a CDR is its application in the banking sector - open banking. Open banking as the New Zealand CDR's first intended application.[39]

While Open Banking has no singular agreed-upon definition, the Australian Federal Advisory Committee defines it as:

> "a system that allows consumers to securely and efficiently transfer their financial data between financial institutions and accredited third-party service providers in order to access services that can help them improve their financial outcomes."[40]

The CDR allows customers to request that data, such as account balances, credit facility, and spending details, be shared.[41] For example, FinTechs [42] (as an AR) can utilise this data to compare a customer's existing financial products with other offerings, such as savings accounts or mortgage plans, to determine the best account for the customer. [43] With the

---

[36] At 6.

[37] Ministry of Business, Innovation and Employment *Regulatory Impact Statement: Establishing a consumer data right* (23 June 2021) at 62.

[38] Office of the Minister of Commerce and Consumer Affairs *Establishing a consumer data right* (Ministry of Business, Innovation & Employment, 9 July 2021) at 4.

[39] At 4.

[40] Canadian Federal Advisory Committee *Final Report on Open Banking* (Department of Finance Canada, April 2021) at 29.

[41] Note that this data must be designated as "in scope" for it to be available to share under the CDR.

[42] "Financial Technology." This is a term used to refer to financial service providers who integrate technology to enable their service.

[43] There are existing online tools that compare products, but the CDR enables FinTechs to personalize these to the customer.

customer's consent, a FinTech could then action the switch to a better account.[44] This also can allow the separation of previously bundled banking services. [45] The availability of this valuable data will empower new entrants in the market [46] enabling the provision of new creative services.[47]

Having introduced the CDR and provided an example of its implementation in Open Banking, the remainder of this paper will compare and contrast the draft law with its Australian counterpart and highlight the key issues that the New Zealand legislature should consider when refining the draft legislation.

IV "Read" and "write" functionality

A notable difference in New Zealand's CDR compared to the Australian model is the adoption of both read and write functionality. As a core tenant of a CDR, read access describes the ability for data to be shared with ARs in a machine-readable format. This allows ARs to utilise in-scope customer information stored by data-holders. Building on read access, action initiation will allow ARs to issue instructions to data holders when authorised by a customer. Write functionality is called "action requests" or "action initiation" in the draft law.[48] Write access enables (the "writing" of data, which is) functionality such as moving data, updating details, or opening and closing accounts.[49]

Including action initiation in New Zealand's CDR is consistent with the United Kingdom's Open Banking legislation but a significant departure from Australia's implementation,

---

[44] This will require the use of action initiation or "write access". See **Chapter IV** for further discussion.

[45] Basel Committee on Banking Supervision *Report on Open Banking and Application Programming Interfaces* (19 November 2019) at 8.

[46] Ariadne Plaitakis & Stefan Staschen, "Open Banking: How to Design for Financial Inclusion" (online, October 2020).

[47] Oscar Borgogno and Giuseppe Colangelo *Consumer Inertia and Competition-Sensitive Data Governance: The Case of Open Banking* (January 3, 2020) at 7, cited in Scott Farrell "Designing Data Rights for Canadian Open Banking: Lessons from Banking Law in Australia and the United Kingdom" (2022) 85 Sask L Rev 165.

[48] See Customer and Product Data Bill Exposure Draft Bill 2023, above n 3, at cl 81. And Ministry of Business Innovation and Employment, above n 2, at [132].

[49] Ministry of Business Innovation and Employment, above n 2, At [37]

which deliberately excluded write functionality until a later date.[50] By enabling action initiation from the outset, the CDR is poised to have more applications and functionality. In theory, this should increase the rate of adoption and avoid the limited customer uptake observed in Australia.

While Australia is currently legislating to allow action initiation, this will not be functional until the Australian CDR's fourth operational year.[51] Australian regulators were particularly mindful to ensure customers initially gained confidence in the CDR as a data-sharing framework. They were concerned that write access (particularly as it could be used to allow the transfer of funds) could create distrust in the new system, reducing participation.[52] Arguably, the exclusion of functionality enabled by write access actually had the opposite effect, with the exclusion hampering the CDR's utility, thus disincentivising consumers from using the system.

As action initiation is intended to be included in New Zealand from the outset, the Australian concerns must be addressed. There must be robust protections in place to prevent misuse and, equally, to instil confidence and trust in the system. The proposed approach to require further accreditation to utilise action initiation paired with strong consent requirements may achieve this.[53]

C Accreditation for action initiation

The draft law indicates that there will be different tiers of accreditation for read and write access. These two classes will have differing requirements and obligations correlating to the perceived risk levels associated with read and write access - ensuring costs and protections are proportionate to the risk.

As suggested in the discussion document, action initiation accreditation should include a condition that requires a requestor's systems and policies to be used ethically, responsibly,

---

[50] See, Ross Buckley, Natalia Jevglevskaja and Scott Farrell "Australia's Data-Sharing Regime: Six Lessons for the World" (2021) UNSWLRS 67 45 – 47.

[51] Treasury Laws Amendment (Consumer Data Right) Bill 2022 (126-22) (Cth). See also, Valeska Bloch, Alex Ortner, Art Honeysett "CDR action initiation is coming – what does it mean and why does it matter?" (30 November 2022) Allens Linklaters <allens.com.au>

[52] Kelly, above n 4 at 17.

[53] Ministry of Business Innovation and Employment, above n 2, at [90] – [92], [138] – [142].

and fairly.[54] To strengthen this condition, MBIE should consider adding or clarifying an obligation that each action initiation is subject to these standards.[55] This could play a role both in creating a robust accreditation regime and assuring customers that use of action initiation is safe.

Currently, non-accredited parties will be able to make data requests, but data holders are not obligated to comply.[56] Action initiation should be reserved for specially accredited parties. If misused, the functionality enabled by action initiation has the potential to cause significant harm, such as the unauthorised movement of funds or unsecure handling of data. The result could be a negative impression on consumers' perception of the CDR, creating distrust in the system. For this reason, the functionality should require accreditation.

It may also be prudent for New Zealand to mirror the Australian amendment legislation.[57] This Bill proposes that each designated sector have a list of approved actions that can be requested. While this imposes some regulatory intervention and may slow or prevent certain use cases, it will likely comfort customers to know they can only request pre-approved actions.

D Consent

With the addition of action initiation, the required consent from customers will increase public trust in the system. The draft law focuses on consent by reference to "authorisation". Authorisation must be express, and the customer must be "reasonably informed about the matter to which the authorisation relates."[58] The effect is that consent must be meaningful.

Consent documents drafted in an overly legalistic manner do not, in substance, allow customers to make informed decisions. MBIE should consider including in the draft law a

[54] Ministry of Business Innovation and Employment, above n 2, at [141].
[55] Even if this in effect is already the case, the addition of a clarifying provision will increase consumer confidence in the system.
[56] At [166] and [89].
[57] The Bill is currently in its first reading before the house. See Treasury Laws Amendment (Consumer Data Right) Bill (Cth), above n 51.
[58] See Customer and Product Data Bill Exposure Draft Bill 2023, above n 3, cl 30 – 35. The requirements in the draft law are more stringent than the consent requirements in the Privacy Act. Additional discussion can be found in **Chapter V.**

requirement for standardised consent requests, which must make clear what authorisations are requested and how far authorisation will extend.

The discussion document seeks feedback on how long consent should last, dictating how often an AR needs to collect consent from the consumer for an authorised activity.[59] A balance must be struck between mitigating administrative burdens, compliance costs, and friction for the consumer and, on the other hand, providing sufficient consumer protection.

MBIE suggests mirroring the Australian approach, wherein the draft bill imposes a maximum consent period of 12 months; thereafter, consent must be renewed.[60] A 12-month maximum consent period would arguably provide required customer protection and a commercially workable time frame. This timeframe would potentially balance the "fatigue and frustration" caused by an overly short timeframe to renew consent, which could cause customers to forgo using data-enabled services.[61]

Further, if New Zealand requires that a meaningful informed consent process be followed when initial consent is first acquired, a "yes/no" renewal option could be implemented instead of requiring the re-collection of full consent after expiry. This could be accompanied by a summary of what the consent authorises. Including these options would strike a balance between allowing frictionless use of the service and assisting customers in keeping track of and reassessing consent given, which should increase trust in the framework.

E Conclusion on Read and Write Access

Action initiation in New Zealand's CDR is a welcome inclusion. By enabling this additional functionality, as opposed to read-only access, the system has increased utility for customers. Consumer perception of the framework is a risk that must be managed: for it to succeed, it must be perceived as safe and utile. The draft law proposes apt protections through its consent provisions. This must be communicated and understood by the public

[59] See Ministry of Business Innovation and Employment, above n 2, at [55] – [65]
[60] At [63].
[61] At [64]

- it is not enough that the system is, in fact, safe. Consumers must also know this fact and believe it to be true.

Consumer confidence is crucial. However, the acceptance by many consumers of the current use of a comparatively unsafe data-sharing method (screen scraping) indicates that consumers have an appetite for convenience and utility. They may not be as concerned with (or understand) the privacy and safety implications. In this context, increased functionality (so long as it is accompanied by appropriate protection) should encourage participation in the CDR.

V Privacy Act implementation comparison and considerations

The CDR enabled by the draft law centres on data transfer, which naturally raises privacy as a crucial element to be carefully addressed, including the ability to delete data. Ensuring the proper handling of data enables the system to function effectively and fosters public trust in its operations.

At their core, the privacy legislation in both New Zealand and Australia acknowledges individuals' right to access the data held by other parties.[62] Compared to the Australian equivalent, New Zealand's privacy legislation is better positioned to enable a CDR. As such, the draft law avoids regulatory overlap by relying on its present privacy law instead of legislating on top of it, as has been done in Australia.[63] This approach arguably does not yield an ideal outcome but prioritises functionality and practical considerations.

F Australia's Implementation of Privacy Protection

Comparing the two regimes requires context as to how the Australian CDR interacts with the Australian Privacy Act.[64]

Recognising that their existing Privacy Act was not fit to provide the necessary protections nor facilitate all the required functions, Australian regulators implemented additional privacy standards beyond what was offered by the Australian Privacy Act, known as the

[62] See Privacy Act 2020 IPP 6 and Privacy Act 1988 (Cth) APP 12.
[63] Competition and Consumer Act 2010 (Cth), pt IVD, division 5.
[64] Privacy Act 1988 (Cth).

"Privacy Safeguards". [65] The Privacy Safeguards are placed within Part IVD of the Competition and Consumer Act.[66] These Safeguards will apply when an AR requests data or a data holder collects data from a customer.[67] Broadly, these Privacy Safeguards (and the Australian Privacy Principles (APPs) in its Privacy Act) regulate how organisations can collect and handle personal information.[68]

The Australian Privacy Act applies only to personal information collected and handled by businesses with more than A$3 million annual turnover.[69] This puts many organisations beyond the scope of the APPs. As a result, commentators have argued that at various times, the applicability of each regime may be unclear, in effect leading to 'twin privacy regimes' and requiring parties to, in some circumstances, comply with both.[70] This imposes significant costs and creates complexity. In some cases, it has also dissuaded certain parties from entering the regime.[71]

G New Zealand's Approach

Until the draft law was released, it was uncertain what approach New Zealand would take.[72] It has become clear that instead of duplicating Australia's Privacy Safeguards, New Zealand has opted to rely on its existing Privacy Act.[73] The draft law's scope is extended from the Privacy Act's "identifiable individuals" to "identifiable customers," allowing trusts and companies to benefit from the draft law.[74]

---

[65] The Australian Government Treasury *Consumer Data Right Privacy Protections* (December 2018) at 4.
[66] Part IVD of the Competition and Consumer Act 2010 (Cth) was inserted through amendment by Treasury Laws Amendment (Consumer Data Right) Act 2019 (Cth).
[67] See Part IVD of the Competition and Consumer Act 2010 (Cth), s 56EA.
[68] Australian Government "Consumer Data Right - Privacy" <www.cdr.gov.au>
[69] Privacy Act 1988 (Cth), s 6D.
[70] Natalia Jevglevskaja and Ross Buckley "The Consumer Data Right: How to Realise This World-Leading Reform" (2022) 45(4) UNSWLJ 1325 at p 1616.
[71] See Kelly, above n 4.
[72] See MBIE's initial consultation documents on the CDR. Office of the Minister of Commerce and Consumer Affairs *Establishing a consumer data right* (Ministry of Business, Innovation & Employment, 9 July 2021).
[73] See Ministry of Business Innovation and Employment, above n 2, at [25] – [35].
[74] For clarity, the Privacy Act retains its original scope of "identifiable individuals". The draft law, diverging from the Act extends the types of data it applies to. See, Ministry of Business Innovation and Employment, above n 2, At 17.

The Privacy Act 2020 and its Information Privacy Principles (IPPs) govern the collection, use, disclosure, storage, retention and access to personal information.[75] Unlike its Australian counterpart, New Zealand's Privacy Act applies to any organisation regardless of annual turnover, better placing it to capture and regulate privacy requirements for a CDR.[76] Fundamentally, New Zealand's Privacy Act can be applied across the CDR without requiring many additional requirements within the draft law. [77]

By applying the existing Privacy Act in the draft law, New Zealand avoids legislative overlap. However, the Privacy Act must also be fit to enable a CDR. MBIE's discussion document does not provide a detailed consideration of the two approaches to privacy protection. The tables below compare New Zealand's existing IPPs against Australia's Privacy Safeguards.[78] The comparison highlights some gaps between the Safeguards and the IPPs. It concludes that with supplementation in the draft law, the IPPs are apt to support a CDR. A comparison of this nature is subject to some uncertainty as the IPPs and Privacy Standards do not align one to one.

Table 1- Comparison of Australian Privacy Safeguards APPs and New Zealand IPPs

New Zealand IPP [79]	**Australian Privacy Safeguard [80]**	**Comparison**
IPP 1 - Purpose of collection of personal information	PS 1 - Open and transparent management of CDR Consumer Data	IPP 1 sets out the general purpose of data collection. Information that is not necessary for its purpose should not be collected. PS 1 is tailor-made for a CDR, requiring a CDR data management policy.
IPP 2 - Source of personal information	PS 3 Soliciting CDR Consumer Data from CDR participants	IPP 2 allows for limited collection from other sources that are not necessarily consented. PS 3 requires express consent for the collection of data. The concept of data minimisation is included in PS 3.

[75] "Collection & Processing in New Zealand" (20 January 2023) DLA Piper Global Data Protection Laws of the World < dlapiperdataprotection.com>

[76] See Privacy Act 2020, s 4.

[77] From a consumer confidence perspective, optically, using the Privacy Act instead of overlaying new regulations baked into the Act as was in Australia may make New Zealand's protections appear "off the shelf" and not bespoke to this system. It will be essential to make it abundantly clear to the user base that it is safe.

[78] Or APPs when applicable.

[79] Privacy Act 2020, s 22

[80] Part IVD of the Competition and Consumer Act 2010 (Cth), division 5, subdivision B.

		IPP 3 is not directly compatible with a CDR's strict consent requirements – consent requirements in the draft law have supplemented this.
IPP 3 - Collection of personal information from subject	PS 3 Soliciting CDR Consumer Data from CDR participants	IPP 3 ensures data collectors are clear about why data is being collected, who will receive it and what will happen if data is not shared. It recognises that there may be good reasons for not letting someone know their data is being collected. PS 3 has strict requirements on consent requirements. Data may only be collected from another business with consent. As above, this has been supplemented by consent requirements in the draft law.
IPP 4 - Manner of collection of personal information	PS 4 - Dealing with unsolicited CDR Consumer Data from CDR Participants	IPP 4 allows collection of data in lawful, fair and not unreasonably intrusive ways. While not directly comparable, PS 4 imposes a strict requirement that any data collected without consent must be deleted.
IPP 5 - Storage and security of personal information	PS 12 - Security of CDR Consumer Data	IPP 5 and PS 12 are similar. They require appropriate data security requirements to protect data from misuse, interference, loss, modification, disclosure, or unauthorised access. PS 12 requires any unneeded data to be deleted or de-identified.
IPP 6 - Access to personal information	APP 12 (Not PS 12)	The Privacy Safeguards do not have an IPP 6 equivalent. Australian Privacy Principle (APP) 12 imposes this standard. In effect, IIP 6 and APP 12 provide the foundations of a CDR.
IPP 7 - Correction of personal information	PS 13 - Correction of CDR Consumer Data	IPP 7 and PS 13 impose similar obligations. A person may request for their data to be corrected. Even if the data holder disagrees, they must nevertheless attach a statement of correction to the data to show the person's view. [81]
IPP 8 - Accuracy of personal information to be checked before use.	PS 11 - Quality of CDR Consumer Data	IPP 8 and PS 11 require businesses to take reasonable steps to check that data is accurate, complete, relevant, up-to-date and not misleading. IPP 8 requires "reasonable steps" to check the accuracy of data, while PS 11 uses stronger language with the term "ensure". PS 11 requires the customer to be informed if incorrect data is disclosed. IPP 8 has no comparative requirement.
IPP 9 - Agency not to keep personal information for	PS 12 - Security of data and the handling of redundant data	IPP 9 requires that data not be kept longer than is necessary. PS 12 requires any unneeded data to be deleted or de-identified.

[81] Remains similar to PS 13.

longer than necessary.		
IPP 10 - Limits on use of personal information.	PS 6 - Use or disclosure of CDR Consumer Data by ADRs or designated gateways	IPP 10 and PS 6 are generally comparable. Both require data only to be used for consented purposes. IPP 10 includes an exception for directly related purposes. This has been interpreted to mean an uninterrupted, immediate relationship to the original lawful purpose".[82]
IPP 11 - Limits on disclosure of personal information.	PS 6 - Use or disclosure of CDR Consumer Data by ADRs or designated gateways	IPP 11 and PS 6 restrict the disclosure of data unless consented. IPP 11 also allows disclosure in an anonymous way when necessary to avoid endangering someone's health or safety or prejudice to the maintenance of the law.
IPP 12 - Disclosure of personal information outside New Zealand.	PS 8 - Overseas disclosure of CDR Consumer Data by ADRs	IPP 12 allows data to be transferred overseas if the data will be adequately protected. (Application of the Privacy Act or similar regime to the overseas recipient or consent by the customer.) PS 8 only allows data to be shared overseas if the recipient is accredited under the CDR.
IPP 13 Unique identifiers.	PS 9 - Adoption or disclosure of government-related identifiers by ADRs	IPP 13 permits restricted use of unique identifiers used by another organisation if the use of identifiers is used to communicate about a customer. PS 9 entirely prohibits the use of government-related identifiers. This is an important requirement to be added in the draft law – it prevents misuse.

Table 2 – Privacy Standards with no IPP equivalent.

PS with No IPP Equivalents	**Draft Law implementation**
PS 5 - Notifying the collection of CDR Consumer Data	PS 5 requires accredited businesses to notify customers through the consumer dashboard when data is collected.[83] It is unclear if this is included in the draft law, but it could be covered by s 38. The use of a consumer dashboard appears to be currently undecided.[84]
PS 7 - Use or disclosure of CDR Consumer Data for direct marketing by ADRs	There is no equivalent in the draft law or the IPPs. This is an important protection to be included in the draft law – it prohibits ARs from using data held about a customer to advertise to them.
PS 10 - Notifying of the disclosure of CDR Consumer Data	While the Privacy Act has no IPP equivalent, section 38 of the draft law requires notification after providing data.[85]

[82] Privacy Commissioner "When can I use the directly related purpose exception?" <Privacy.org.nz>

[83] See Competition and Consumer Act 2010 (Cth), Part IVD, s 56EH. See also, Office of the Information Commissioner "Chapter 5: APP 5 Notification of the collection of personal information" (22 July 2019) <oaic.gov.au>

[84] Ministry of Business Innovation and Employment, above n 2, at [75]

[85] Customer and Product Data Bill Exposure Draft Bill 2023, above n 3, cl 38.

PS 2 Anonymity and pseudonymity	PS 2 requires an AR to provide a consumer with the option of dealing anonymously or pseudonymously with the entity concerning that CDR data. There is no equivalent in the IPPs.

This comparison with Australia's Privacy Safeguards demonstrates that the IPPs are broadly fit for purpose, with most of the newly drafted Privacy Safeguard requirements already met by the IPPs. A key exception is found in IPP 3 and IPP 4, which regulate data collection and are purpose-based rather than consent-based - allowing data to be collected in some circumstances without customer consent. This diverges from Australia's Privacy Safeguards and is fundamentally incompatible with the stringent consent requirements of a CDR. The draft law includes consent provisions to remedy the deficiencies in these IPPs.[86]

The Privacy Act principles are not specifically designed for a CDR, whereas the Privacy Safeguards were designed for that very purpose. The draft law addresses many additional requirements not met by the Privacy Act. These include the requirement for informed consent, notification, and data storage obligations.[87] Nevertheless, several concerns arise from this implementation.

Notably, the IPPs are expressed as principles to be adhered to, while the draft law suggests secondary legislation will be drafted to implement prescriptive standards, which must be complied with. While this is not dissimilar to the Australian regime, it is certainly not the most harmonious solution. Privacy Principles undoubtedly allow for broader coverage and enable regulation that does not require all contingencies to be accounted for. However, applying prescriptive standards on top of principles to provide greater legal description may result in complexity and inconsistencies. A more extensive principle-based framework could remedy this. There is no easy and elegant solution to implement here. As recognised in Australia, any meaningful action would require a review of the privacy legislation, as these issues stem from the underlying privacy protections and framework. Any review of

[86] Part 3.

[87] These will be included in future iterations of the bill. See e Customer and Product Data Bill Exposure Draft Bill 2023, above n 3, pt 5.

this kind would need to be considered on its own merits – the CPD Act is not the appropriate vehicle to bring such change.[88]

H Deletion of data

Central to privacy and a key functionality missing from the draft law is the ability for customer-requested data deletion. The concept of deletion is provided for in both the IPPs and the draft law. However, it exists only in the context of the requirement to not hold data for longer than is required for the authorised purpose.[89] This section suggests that a standalone right to deletion should be established.[90]

The status of data as a non-rivalrous commodity exemplifies interest in the deletion of data. Non-rivalry is the concept that "one party's consumption of a good does not reduce its value available for others."[91] Essentially, data is not consumed upon use and remains within the system until deleted by service providers. The exclusion of a deletion function unnecessarily increases the risk of misuse of data.

The initial Australian CDR did not include a standalone right to data deletion on request. However, it has been subsequently included through amendment. A right to deletion fundamentally increases trust and confidence in the system by instilling confidence in consumers that they retain control over their data.

Additionally, the right to deletion may provide clarity in the case of insolvency or the merger of data holders. In these instances, the deletion of data will be an important consideration that legislation should regulate. While a request for data deletion may not be an optimal solution to the issue of insolvency and mergers, it provides consumers with the comfort of certainty and choice.

A right to data deletion will require careful consideration as there is no corresponding right in the Privacy Act. There will likely be existing considerations, such as data retention

---

[88] Mark Burdon and Tom Mackie "Australia's Consumer Data Right and the uncertain role of information privacy law" (2020) 10(3) International Data Privacy Law 222 at 235.

[89] Privacy Act 2020, IPP 9.

[90] For deletion of data see Ministry of Business Innovation and Employment, above n 2, at [132]. And more generally, "Chapter 8 - Preserving Value of Shared Customer Data" in Farrell, above n 5.

[91] "Non-Rivalrous Goods" (15 December 2022) Corporate Finance Institute <corporatefinanceinstitute.com>

obligations, that may be impacted.[92] The inclusion of a right to deletion will promote confidence in the system and, ideally, will have the effect of promoting consumer adoption of the system.[93] While this arguably adds complexity to the legislative process and burdens ARs, it is a feature worth implementing.

I The argument for an improved Privacy Act

The Privacy Foundation argues that the draft law does not create a comprehensive right to data portability but rather that it enables functionality through the draft law.[94] It is arguable that many functions and protections, such as consent, deletion, and notification, are valuable to consumers outside of the CDR context. Additionally, aligning the CDR and the Privacy Act will reduce the already minimal effect of twin regulation.

There is existing commentary that New Zealand should first reform its privacy legislation before implementing, or alongside, the CDR.[95] The Minister for Commerce and Consumer Affairs has stated that (similar to the approach taken in Australia) he will not recommend the establishment of additional data rights to underpin the CPD regime.[96] He argues that this reduces compliance costs across the economy, given that the existing framework can be utilised. At face value, this is a compelling reason to retain the current privacy law. However, the draft law introduces a strong case for an updated Privacy Act with protections akin to those existing in the European Union as enacted in its General Data Protection Regulation (GDPR).[97] Such protections could include updating consent requirements and strengthened notification in the Privacy Act to align with the draft law's more onerous and consumer protection-focused equivalents.

Reform of the Privacy Act could provide consistency and clarity between the Act and the CDR, benefitting businesses and consumers with a unified set of rules. This has the flow-

---

[92] An analysis of the implementation of deletion is not in the scope of this paper.

[93] See Australian Community Attitudes to Privacy Survey 2023 (Office of the Information Commissioner, 8 August 2023).

[94] See Marcin Betkier *Submission on Draft Customer and Product Data Bill and Discussion Document* (Privacy Foundation NZ, 24 July 2023).

[95] Commerce Commission *options for establishing a consumer data right in New Zealand*: a submission (Ministry of Business, Innovation and Employment, 19 October 2020) at 6.

[96] Office of the Minister of Commerce and Consumer Affairs, above n 38, at 5.

[97] See Chapter 3 of Regulation 2016/679 on the General Data Protection Regulation [2016] OKJ L 119/1.

on effect of streamlining compliance. Many businesses will operate both in and out of the CDR framework – if the Act and framework are uniform, the approach to compliance will overlap, potentially reducing costs. It may also be possible for regulators to more efficiently oversee compliance of all data collecting and sharing parties in and out of the CDR.

Additionally, there is scope to argue that a strengthened Privacy Act will better align with international best practices. This may facilitate cross-border data sharing, which could be important for future developments of the CDR.

J Conclusion on Privacy

Overall, using existing privacy law is less of a stop-gap approach than the baked-in privacy safeguards included in Australia's legislation. While the IPPs are not a perfect answer to the CDR's regulatory requirements, most required protections are met with the supplementation in the draft law. Using the existing privacy framework reduces compliance costs for businesses and should avoid businesses intentionally opting out of the system for this reason. While data deletion would impose additional compliance costs on businesses, the draft law would benefit from adopting such a right. The customer benefit and a resultant increase in participants likely justify the cost to business.

Chapter V argued for an overhaul of the Privacy Act. Ideally, this reform would be executed in tandem with the draft law. However, the implementation of the CDR should not be shelved, waiting for the development of a hypothetical privacy framework that is more suitable.

VI Reciprocity

The concept of reciprocity is not included in the draft law. It refers to the requirement for ARs to respond to customers' requests to share data with other data recipients. These recipients could be other ARs or data holders such as banks.[98] The Australian CDR

[98] Ministry of Business Innovation and Employment, above n 2, at [97].

includes reciprocity as a principle extending the possible obligation of data sharing beyond data holders.

The benefits of reciprocity are twofold. First, it creates a dynamic ecosystem by increasing the flow of data compared to one in which ARs "are solely receivers of data, and data holders are largely only transmitters of data."[99] Second, it increases competition by allowing data holders and other ARs to benefit from the data generated. Having data move circularly prevents perceived disadvantages to incumbent data holders who view "big tech" companies as a threat.[100]

Conversely, it has been argued that reciprocity discourages ARs from participating, either because of the increased costs to participate or the costs of sharing valuable customer data.[101]

Submissions to MBIE from interested parties in response to the draft law oppose the exclusion of a reciprocity principle – these are mainly from banks or their representative groups.

The author argues that the exclusion of reciprocity in the initial iteration of the CPD Act is preferable to its inclusion. Reciprocity imposes costs and regulatory complexity on developing FinTechs.[102] Additional requirements in Australia have limited the number of ARs who have opted into the system, resulting in less incentive and benefits provided to customers. This creates a catch-22, where customers want to utilise the system, but third-party providers do not exist, and conversely, new service providers that are established will lack a consumer base. Partly due to this issue, Australia's original principle of reciprocity has been watered down significantly - the principle now only applies to ARs after a year

[99] Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2018 (Cth) cited in Scott Farrell, above n 5.
[100] See for example Financial Services Council *Submission: Customer and Product Data Bill Exposure Draft* (Ministry of Business, Innovation and Employment, 24 July 2023) (forthcoming) at 6.
[101] Farrell, above n 5, at 139.
[102] Financial technology companies.

of operation.[103] Initial concerns raised by data holders (especially large banks) that big-tech would "creep" into the sector were ill-founded. The fact that the big four banks in New Zealand have already experienced the implementation of a CDR in Australia likely explains why they are not vehemently protesting the exclusion of reciprocity.[104]

MBIE could opt to apply reciprocity to large companies from the outset. This would likely cause unneeded complexity. Reciprocity is a principle that should eventually be included in the CDR, and it is possible to implement it later through amendment.

K Derived Data

The lack of reciprocity should pause derived / value-added data from being included in the draft laws' scope.

Derived data refers to a class of information subject to processing by the party that holds that data (typically data holders). It is, therefore, distinct from customer data, which is usually unprocessed. [105] There have been objections by incumbent data holders to incorporating derived data within a (CDR) framework.[106] Incorporating derived data might pose challenges to protecting the intellectual property rights of data holders as data processed in a proprietary method would be in the ambit of shareable data.[107] It could also discourage investment in data and associated technologies since any competitive edge gained from these investments would be readily accessible to rivals. It also raises questions of accountability in cases where derived data is prepared negligently.[108]

These issues are amplified when the principle of reciprocity is excluded - there is no recourse for data holders to access customer data held by ARs, let alone derived data. This

---

[103] Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2023 (Cth). See also Peter Mulligan and Kirk Boladeras "Preparing for changes to the CDR: What you need to know" (April 2023) Norton Rose Fulbright <nortonrosefulbright.com>

[104] Note there are objections to the exclusion of reciprocal data sharing obligations (FSC submission cited above).

[105] Office of the Information Comissioner "What is the Consumer Data Right" <OIAC.govt.au>

[106] See, for example, Financial Services Council, above n 100. AIA *Submission: Customer and Product Data Bill Exposure Draft* (Ministry of Business, Innovation and Employment) (forthcoming). ASB ASB *response - Consumer Data Right discussion document* (Ministry of Business, Innovation and Employment) (forthcoming).

[107] See Farrell, above n 5, at 83 – 84.

[108] At 83 – 84.

creates an inherently one-sided arrangement, which severely disadvantages data holders. Derived data should be "out of scope" and revisited when or if reciprocal obligations are included in the CDR.

VI Māori Data

A challenge unique to New Zealand is managing the interests of Māori and Māori Data,[109] which is a taonga. The draft law requires consideration of the Treaty of Waitangi and tikanga principles when designating a sector/industry and while drafting secondary legislation.

Much discourse in this field centres on the concepts of Māori data governance (MDGov) and Māori data sovereignty (MDSov). Te Ngira defines MDGov as the "[M]echanisms, legal instruments and policies through which Māori exercise control over Māori Data" and defines MDSov as "The inherent rights and interests that Māori have in relation to the collection, ownership and application of Māori data."[110]

Māori have numerous interests in their data. Firstly, as a taonga, data has deep cultural significance.[111] Secondly, stemming from the data's taonga status, Māori also have kaitiaki obligations over their data.[112] Thirdly, there is both an individual and collective interest in data, given that it can potentially unlock significant value.[113] Collective Māori data is particularly important to Iwi leaders, organisations, and groups for utilisation in advancing

[109] Which can include information or knowledge from or about Māori, such as population, place, culture and environment. It can include data generated by the Government and private sector.
[110] The University of Waikato's Institute for Population Research. See Te Ngira Institute for Population Research *Māori Data Sovereignty and Privacy* (University of Waikato, March 2023).
[111] See *Māori Data Governance Model*, above n 9, at 3.
[112] A kaitiaki relationship refers to a relationship a kin to guardianship. See Joe Williams "Lex Aotearoa: A Heroic Attempt to Map the Māori Dimension in Modern New Zealand Law" (2013) 21 Waikato Law Review 1 at 3.
[113] See *Māori Data Governance Model*, above n 9, at 4.

common purposes.[114] One such purpose is data's use in governance, as it allows Iwi leaders to lead and develop "[their] people, places and interests toward their aspirational goals."[115]

In the context of the CDR, MBIE clarifies that

> "a te ao Māori lens emphasises the whakapapa of data associated with a person, and therefore data may need culturally appropriate infrastructure and safeguards to reduce any risk of it being mishandled." [116]

The concept of MDSov applies to both the collection/privacy implications of data and the use/access by Māori of this data. Currently, there are initiatives outside of the CDR to increase iwi access to Māori data. One of these is Stats NZ's integrated data infrastructure (IDI).[117] The IDI gives iwi leaders access to limited data sets, but these only include data collected by the Government. The CDR could grant iwi leaders access to other significant data sets should individuals consent, going far beyond what is currently available to and from the Government.[118] The CDR will not replace data-sharing arrangements already in place with the Crown, but rather will increase access to data and may alleviate concerns expressed by iwi around access to up-to-date data beyond Census data which is only collected every five years.[119]

There is no singular, homogenous understanding of Māori data and its application, and the area of law is constantly evolving.[120] This section discusses relevant issues but does not offer conclusive suggestions. Any conclusions would require discussion

---

[114] The CDR has traditionally been seen as providing a right to individuals. However, CDR in New Zealand applies to businesses and trusts. This allows perhaps the CDR not only to apply to individuals but also to the collective. There does not appear to be much literature on this concept, with much of the understanding currently being written through a Western lens of data use and ownership.

[115] *Iwi data needs*, above n 9, at 5.

[116] Office of the Minister of Commerce and Consumer, above n 38, at 12. The term whakapapa refers to a line of descent from one's ancestors; genealogy.

[117] See Statistics New Zealand "Integrated Data Infrastructure" (23 August 2023) <Stats.govt.nz>

[118] For example, the CDR may allow access to individual banking, telecommunications, power, and health data. See Ministry of Business Innovation and Employment, above n 2, at 4.

[119] See Statistics New Zealand "About the Census" <Ccnsus.govt.nz>

[120] See generally, Natalie Coates "Resurgence of Māori Law: the Constitutional Transformation Movement in Aotearoa New Zealand" (2015) NZ Law Journal 1.

beyond the scope of this paper, and extensive consultation with and decision-making of Māori interest groups.

L Māori Health Data Example

By way of a brief example, the Te Pou Matakana judicial review cases demonstrate how the CDR can strengthen MDS. The case revolved around Whānau Ora,[121] commissioned by Te Puni Kokiri to provide underserved communities with COVID-19 vaccinations.[122]

Through its information systems provider, Whānau Ora requested to enter data-sharing arrangements with the Ministry of Health for relevant details of unvaccinated Māori, including their vaccination status and personal and contact details. This data was to be used to increase the Māori vaccination rate by targeting services where most required. The Ministry shared with Whānau Ora anonymised "street-level mapping representations that show areas with unvaccinated communities."[123] Whānau Ora asserted that this information was not specific enough to enable them to carry out their function.[124]

While slightly speculatory, as a health sector designation is yet to be designed, theoretically, if the health sector was designated under the CDR, Whānau Ora could register as an AR and, with the consent of individuals, have efficient access to the information they require.[125] This fundamentally increases Māori control over their data and directly allows for MDGov, which increases MDSov.

M Storage of Data

A substantial body of literature discusses concerns related to the offshoring of Māori Data. It is important to note that the draft law does not alter existing data storage obligations and will not impose new ones.[126] Current discourse on the storage of Māori data focuses on data held by the Government. Many cloud-based storage providers are based overseas. Services offered by these companies go beyond storage alone and include the processing

[121] A government-funded, Māori-delivered agency which supports whānau wellbeing and development.
[122] Te Pou Matakana Limited V Attorney-General [2021] NZHC 2942 at [11].
[123] At [16].
[124] At [22].
[125] There should be consideration here of the reality that unvaccinated people may not consent to sharing their data.
[126] Ministry of Business Innovation and Employment, above n 2, at [48].

of data. Consequently, the Government and private sector have increasingly offshored many of their data storage requirements.

With the increasing amount of data transmission within the CDR, the amount of data stored overseas will necessarily increase, which is concerning in the context of Māori data rights. First, Treaty obligations do not apply outside New Zealand's jurisdiction.[127] Second, companies may be compelled to surrender data to foreign governments upon request.[128] Māori data might be included in these requests without Māori being aware or providing consent. Offshore storage, therefore, circumvents the authority and control exercised by Māori.[129]

Concerns around implementing data storage obligations focus on the lack of availability of onshore storage options and the high cost of mandating onshore storage. Such increased costs risk stifling innovation and participation in the CDR by pricing providers out of the market. Although current data storage discourse is focused on the Government, the requirement for the private sector to store Māori data onshore must be looked at in a broader legal context. The CDR is not an appropriate vehicle for the implementation of data storage laws. This issue must be revisited as general practice develops.

N Cultural Capability

The draft law currently excludes cultural capability considerations from the accreditation regime. As Māori data is a taonga, there is room to argue that ARs should be required to demonstrate cultural competency before being authorised to handle this data. Tikanga principles of manaakitanga[130] and kaitiakitanga[131] emphasise the importance of responsible and respectful stewardship of valuable resources. Cultural competency requirements would establish a baseline understanding and foundation for handling Māori data – an important step to acknowledging the unique cultural and data sovereignty rights of Māori.

---

[127] Note that Treaty obligations bind the Crown and not the private sector. However, the essence of this point is that the Crown has minimal powers in protecting Māori interests overseas.

[128] For example, the US asserts jurisdiction over data stored international by US headquartered companies. See for example, United States, Petitioner V. Microsoft Corporation US 17-2 (2018).

[129] *Māori data sovereignty and offshoring Māori data* (Te Kahui Raraunga, 27 July 2022) at 16.

[130] The tikanga concept of nurturing relationships.

[131] The tikanga concept of guardianship or protection, the obligation to care for one's own.

Another reason for including cultural capability is that historically, Māori have been underserved by industries.[132] This may, in part, be due to these institutions and services being designed from a Western perspective. Cultural competency requirements may be an effective way to address this historical inequity. Including cultural competency requirements can make the CDR more inviting and accessible for Māori, respecting the principles of kotahitanga[133] and whakawhanaungatanga.[134] These requirements acknowledge the importance of embracing diverse perspectives within New Zealand's society, and upholding Treaty obligations.

On the other hand, it is important to consider potential drawbacks. A central issue discussed in this paper is that a CDR will fail if it is not broadly accepted and utilised. Consumer adoption and the entrance of service providers (ARs) are vital. Imposing an additional requirement of cultural competency on new businesses may discourage them from interacting with the CDR. This effect may be amplified for international participants looking to enter the New Zealand market.[135] Should the service providers not join the system, the CDR would not benefit anyone, including Māori, resulting in a net-negative outcome. Again, a balance must be achieved.

MBIE suggests that cultural competency should be left to market forces. Māori will gravitate towards providers who offer the best service for their needs. Instead of mandating cultural competency, a key aim of the CDR's debut should focus on providing ample resourcing for awareness messaging and education surrounding the protections offered by the CDR. Māori should be empowered to exercise their autonomy and make informed decisions.

---

[132] See, for example in the banking context *Improving Māori Access to Capital* (Reserve Bank of New Zealand, issues paper, 09 August 2022).

[133] The tikanga concept of unity.

[134] The tikanga concept of building positive and collaborative relations – the construction of aspirations and goals.

[135] It is worth noting that international entrance to the market will likely have less understanding of Māori data and Tikanga principles.

O Considering the MDG

The report by Te Kahui Raraunga outlines a Māori Data Governance Model (MDGM) designed by the Iwi Leaders Group and Māori data experts.[136] The report is primarily designed for the public sector but provides valuable insights for legislative design. The report recognises eight pou (pillars) MDGov that, when viewed holistically, promote, and enable "iwi, hapū and Māori to pursue their own goals for cultural, social, economic and environmental wellbeing."[137]

While regulations such as data storage obligations and cultural capability expressly legislated would currently harm the efficacy of the CDR, other protections can still be considered. MBIE has indicated that it will consider the MDGM.[138] This section will briefly consider pou 3 – 6.

Pou 3 offers guidance and ideal outcomes for the collection of Maori data.[139] While this was drafted in the context of government data collection, it offers helpful principles for the CDR. Pou 3 considers how any data collection will benefit Māori and any potential risks or harms. It suggests this is done through consultation with Māori data subjects, iwi, and communities. This process will be important to consider at the sectorial designation and data scope stage of the design. MBIE indicates that this will be central to the process. To best uphold this pou, it is important that this process occurs at the start of the design process and not nearing the end.

Pou 4 relates to privacy and consent. Consent requirements are a foundational control in the draft law - aligning with the importance placed on consent in the MDGM.[140] However, the draft law has not dealt with the concept of collective rights and collective consent. This requires consent and privacy principles to be viewed outside its arguably Western lens.

---

[136] *Māori Data Governance Model*, above n 9, at 3.
[137] At 3.
[138] Ministry of Business Innovation and Employment, above n 2, at [43].
[139] *Māori Data Governance Model*, above n 9, at 30 -32.
[140] At 33 - 37.

For Māori, a collective interest exists where data sharing has the potential to harm the collective rights, which cannot be reduced to individual privacies.[141] This is an important consideration for the CDR as the Privacy Act does not include specific Māori privacy considerations.

This is especially evident in the health context with data relating to DNA. While individual autonomy is important, significant consideration must be given to the whakapapa in the data. The MDGM suggests that "individual consent to share such data is inadequate, given the collective interests and risks involved in the ways in which personal data is aggregated."[142]

The idea of collective interests may be necessary to consider in the design of sectoral designations in terms of the scope of data and consent requirements.

The CDR is faciliatory for the "Access as a process" principle in **Pou 5**.[143] The access should be viewed as a relational and ongoing process. Fundamentally, the CDR allows Māori to access information held about them on an ongoing basis.

Pou 6 considers the secondary use of data, including data linkage, sharing or aggregation. The pou stresses that all data uses must be explained and explicitly agreed to.[144] This would include when data is used for statistics or anonymised for other purposes in a CDR.

There is an overlap here with the collective interest in data from Pou 4. A collection of individual consent may have implications for the larger collective—their interests in both a general and Māori data context on the de-identification of consumer data. While de-identified data has some substantial benefits, MBIE should consider requiring express and unbundled consent requirements for this use.

---

[141] At 33.
[142] At 35.
[143] At 38 – 42.
[144] At 43 – 45.

P Conclusion on Māori Data

Māori data concepts are an evolving issue, particularly in the concept of data-sharing. The CDR should increase MDSov by enabling access and control of data held by third parties. However, inherent tensions exist between the current predominantly Western, and Māori use and understanding of data. These tensions highlight some practical challenges in data storage and the provision of services. These concepts should be revisited as the CDR landscape continues to evolve.

The CDR still offers significant advantages to MDSov. While tikanga principles must be upheld, they should be approached pragmatically, considering the feasibility of market forces and the need for a functional system that benefits all, including Māori.

While New Zealand may not be trailblazing in the development of a CDR, it is the first jurisdiction to consider indigenous rights in this context meaningfully. Many other nations will be watching New Zealand's approach with interest.

VII Conclusion

The CDR is a comprehensive right aimed at unlocking value from consumer data. The draft law aims to improve competition in the market, laying the groundwork for new products and services. Vitally, the successful operation of the CDR hinges on the willing interaction of consumers with the system and the willing participation of ARs.[145] Therefore, the CDR must prioritise design choice that safely and conscientiously promotes this objective.

This paper explores key considerations in chapters IV through VII, emphasising the need for pragmatism in addressing challenges. Chapter IV argues that "write access" in the draft law is a welcome addition. While it has the potential to weaken customer confidence in the CDR, as long as these risks are mitigated, the additional functionality enabled will attract customers to the system. Chapter V concludes that New Zealand's approach of utilising the existing Privacy Act and its IPPs is mostly sound. Importantly, it avoids regulatory overlap caused by legislating on top of the existing Act, which would impose significant

[145] See Anton Didenko "Australia's Consumer Data Right and Its Implications for Consumer Trust" (50(1) Monash University Law Review) (Forthcoming).

cost and possibly dissuade service providers from entering the market. Chapter VI argues that despite opposition from industry, the exclusion of reciprocity is sound. It will enable market entrants to establish themselves without significant additional burdens. Finally, chapter VII considers the complexities of Māori Data and how tikanga principles best fit into the CDR. It concludes that more consideration must be given to the framework's design, which must be done pragmatically.

While the CDR may initially impose increased compliance costs, particularly on data holders, it has the potential to strengthen and promote innovation and market competition. To promote the CDR's long-term success, New Zealand's legislative choices must prioritise functionality for consumers while providing adequate protections without overburdening entrants (ARs) into the market with a burdensome over-regulated approach. Many important legislative choices remain as New Zealand's CDR is still in the exposure draft bill process. MBIE can continue to prioritise useful functionality to attract customers and, where prudent, in order to strike the correct balance, minimise regulatory burdens.

Appendix 1: List of abbreviations

List of abbreviations	
CDR	Consumer Data Right
The draft law	New Zealand Customer and Product Data Bill
MBIE	Ministry of Business, Innovation and Employment
AR	Accredited Requestor
API	Application Programming Interface
Fintech	Financial Technology
APPs	Australian Privacy Principles
IPPs	Information Privacy Principles
GDPR	General Data Protection Regulation
CPD	Customer and Product Data
MDGov	Māori Data Governance
MDSov	Māori Data Sovereignty
MDGM	Māori Data Governance Model

BIBLIOGRAPHY

Legislation

New Zealand

Privacy Act 2020

Australia

Competition and Consumer Act 2010

Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2023 (Cth).

Treasury Laws Amendment (Consumer Data Right) Act 2019 (Cth)

Privacy Act 1988 (Cth)

Treasury Laws Amendment (Consumer Data Right) Bill 2022 (126-22) (Cth)

European Union

Regulation 2016/679 on the General Data Protection Regulation [2016] OKJ L 119/1.

Cases

New Zealand

Te Pou Matakana Limited V Attorney-General [2021] NZHC 2942

United States

United States, Petitioner V. Microsoft Corporation US 17-2 (2018).

Reports

AIA *Submission: Customer and Product Data Bill Exposure Draft* (Ministry of Business, Innovation and Employment) (forthcoming)

ASB *response - Consumer Data Right discussion document* (Ministry of Business, Innovation and Employment) (forthcoming).

Australian Community Attitudes to Privacy Survey 2023 (Office of the Information Commissioner, 8 August 2023).

Australian Government Treasury *Consumer Data Right Overview* (September 2019).

Australian House of Representatives *Explanatory Memorandum: Treasury Laws Amendment (Consumer Data Right) Bill 2019*

Australian Government Treasury *Statutory Review of the Consumer Data Right* (29 September 2022).

ANZ Bank New Zealand *Submission: Options for establishing a Consumer Data Right in New Zealand* (Ministry of Business, Innovation and Employment, 14 October 2020).

Basel Committee on Banking Supervision *Report on Open Banking and Application Programming Interfaces* (19 November 2019)

Bell Gully *Offshoring New Zealand Government Data* (Statistics New Zealand, 21 June 2021).

Canadian Federal Advisory Committee *Final Report on Open Banking* (Department of Finance Canada, April 2021)

Commerce Commission *options for establishing a consumer data right in New Zealand*: a submission (Ministry of Business, Innovation and Employment, 19 October 2020)

Elizabeth Kelly *Statutory Review of the Consumer Data Right* (Australian Government Treasury, 2022).

Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2018 (Cth)

Faith Reynolds *Open Banking A Consumer Perspective* (Barclays January 2017).

Financial Services Council *Submission: Customer and Product Data Bill Exposure Draft* (Ministry of Business, Innovation and Employment, 24 July 2023) (forthcoming)

Financial Data and Technology Association North America *Opportunities in Open Banking* (2019)

Improving Māori Access to Capital (Reserve Bank of New Zealand, issues paper, 09 August 2022).

Iwi Data Needs (Te Kahui Raraunga, 12 March 2021)

Māori Data Governance Model (Te Kahui Raraunga, 26 May 2023).

Māori Data Sovereignty and Offshoring Māori Data (Te Kahui Raraunga, 27 July 2022)

Marcin Betkier Submission on Draft Customer and Product Data Bill and Discussion Document (Privacy Foundation NZ, 24 July 2023).

Ministry of Business, Innovation and Employment *Regulatory Impact Statement: Establishing a consumer data right* (23 June 2021) Office of the Minister of Commerce

and Consumer Affairs *Establishing a consumer data right* (Ministry of Business, Innovation & Employment, 9 July 2021)

Ministry of Business Innovation and Employment *Discussion document: unlocking value from our customer data* (June 2023)

Ministry of Business Innovation and Employment *Draft for Consultation: Customer and Product Data Bill (Exposure Draft Bill) (2023)*

Marketing Means *Open Banking - TPP Customer Survey 2021 - Report on survey results collected by post, telephone and online* (November 2021)

PaymentsNZ *Customer experience guidelines* (API Centre, August 2020)

Oscar Borgogno and Giuseppe Colangelo *Consumer Inertia and Competition-Sensitive Data Governance: The Case of Open Banking* (January 3, 2020)

Secretariat of the Organisation for Economic Co-operation and Development *Consumer Data Rights and Competition - Background note* (AF/COMP(2020)1, 12 June 2020)

Scott Farrell *Future directors for the consumer data right* (Australian Government Treasury, October 2020 at 1)

Te Ngira Institute for Population Research Māori Data Sovereignty and Privacy (University of Waikato, March 2023).

United Kingdom Competition & Markets Authority *Retail Banking Market Investigation: The Retail Banking Market Investigation Order 2017* (2 February 2017)

United Kingdom Competition & Markets Authority "UK reaches 7 million Open Banking users milestone" (press release, 20 February 2023).

Journals

Anton Didenko "Australia's Consumer Data Right and Its Implications for Consumer Trust" (50(1) Monash University Law Review) (Forthcoming).

Ariadne Plaitakis & Stefan Staschen, "Open Banking: How to Design for Financial Inclusion" (online, October 2020).

Bruno Zeller and Andrew Dahdal "Open Banking and Open Data in Australia: Global Context, Innovation and Consumer Protection" **(**Qatar University College of Law, Working Paper No. 2021/001, 2021)**.**

Clare Sullivan "The new Australian Consumer Data Right: An exemplary model for Open Banking" (2022) 4 WIREs Forensic sci 1458.

Emma Leong and Jodi Gardner "Open Banking in the UK and Singapore: Open Possbilities for Enhancing Financial Inclusion" (University of Cambridge legal studies research paper series, 4/2023, 2023)

Joe Williams "Lex Aotearoa: A Heroic Attempt to Map the Māori Dimension in Modern New Zealand Law" (2013) 21 Waikato Law Review 1 at 3.

Laura Brodsky and Liz Oakes "Data sharing and open banking" (online ed, McKinsey&Company)

Mark Burdon and Tom Mackie "Australia's Consumer Data Right and the uncertain role of information privacy law" (2020) 10(3) International Data Privacy Law 222 at 235.

Natalia Jevglevskaja and Ross Buckley "The Consumer Data Right: How to Realise This World-Leading Reform" (2022) 45(4) UNSWLJ 1325

Natalie Coates "Resurgence of Māori Law: the Constitutional Transformation Movement in Aotearoa New Zealand" (2015) NZ Law Journal 1.

Phil Laplante and Nir Kshetri "Open Banking: Definition and Description" (2021) 10.1109 IEEE

Rebecca Chan, Indrit Troshani, Sally Rao Hill and Arvid Hoffmann "Towards an understanding of consumers FinTech adoption: the case of Open Banking" (18 March 2022) 40 IJBM 886

Ross Buckley, Natalia Jevglevskaja and Scott Farrell "Australia's Data-Sharing Regime: Six Lessons for the World" (2021) UNSWLRS 67

Scott Farrell "Designing Data Rights for Canadian Open Banking: Lessons from Banking Law in Australia and the United Kingdom" (2022) 85 Sask L Rev 165.

Books

Scott Farrell *Banking on Data - Evaluating Open Banking and Data Rights in Banking Law (*Kluwer Law International B.V, The Netherlands, 2023)

Websites

Australian Government “Consumer Data Right - Privacy” <www.cdr.gov.au>

“Collection & Processing in New Zealand” (20 January 2023) DLA Piper Global Data Protection Laws of the World < dlapiperdataprotection.com>

Consumer NZ “Trust in banks diving sharply amid soaring profit announcements” (12 May 2023) <Consumer.org.nz>

Dan Beck “Libraries are the beating hearts of communities” (12 May 2023) National Library <natlib.govt.nz>

“Fighting for Māori data rights” (1 November 2019) The University of Waikato <waikato.ac.nz>

Liz Blythe, Louise Taylor and Vaash Singh “Consumer Data Right Update – proposed penalties, supervisory authorities, in-scope sectors and approach to accreditation and fees” (16 January 2023) Russell McVeagh <www.russellmcveagh.com>

Nikki-Lee Birdsey ”Bank satisfaction survey 2022” (22 April 2022) Consumer NZ <Consumer.org.nz>

“Non-Rivalrous Goods” (15 December 2022) Corporate Finance Institute <corporatefinanceinstitute.com>

Office of the Information Commissioner “Chapter 5: APP 5 Notification of the collection of personal information” (22 July 2019) <oaic.gov.au>

Office of the Information Comissioner “What is the Consumer Data Right” <OIAC.govt.au>

“Our Data, Our Soverignty, Our Future” Te Mana Raraunga – Maori Data Soverinty Network <www.temanararaunga.maori.nz>

Passive Income NZ “You don’t have to be loyal to your bank” (May 2018) <passiveincomenz.com>

Peter Mulligan and Kirk Boladeras “Preparing for changes to the CDR: What you need to know” (April 2023) Norton Rose Fulbright <nortonrosefulbright.com>

Privacy Commissioner “When can I use the directly related purpose exception?” <Privacy.org.nz>

See Statistics New Zealand “About the Census” <Census.govt.nz>

Statistics New Zealand “Integrated Data Infrastructure” (23 August 2023) <Stats.govt.nz>

“What is Open Banking” WS02 <ob.docs.wso2.com>

“What is Open Banking” TIBCO Software <tibco.com>

Valeska Bloch, Alex Ortner, Art Honeysett “CDR action initiation is coming – what does it mean and why does it matter?” (30 November 2022) Allens Linklaters <allens.com.au>

Xero “ANZ NZ direct feeds” Xero Central <central.xero.com>