AN EXAMINATION OF THE CUSTOMER AND PRODUCT DATA BILL: LEVERAGING AUSTRALIA'S LESSONS

Ciaran Ward*

The implementation of a Consumer Data Right (CDR) in Australia has 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 May 2024 introduced the New Zealand Customer and Product Data Bill to its House of Representatives. This article offers an overview of the CDR and evaluates whether New Zealand's legal framework and implementation strategies can circumvent the hurdles that have 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 article considers action initiation, the decision to utilise existing Privacy Act 2020 Information Privacy Principles (IPPs), the exclusion of reciprocal data sharing and the considerations of Māori data and Māori data governance.

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 Exposure Draft Bill (Exposure Draft Bill) released for public consultation followed by the introduction of the Customer and Product Data Bill

* Barrister and Solicitor of the High Court of New Zealand. Submitted in partial fulfilment of the LLB (Honours) Degree, Faculty of Law, Victoria University of Wellington | Te Herenga Waka, 2023. The author wishes to thank his supervisor, Dr Marcin Betkier, for his support and guidance.

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.

(the Bill) to the House of Representatives in May 2024.[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 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 trust and acceptance from consumers and industry stakeholders. Australia's experience suggests that without sufficient participants, a CDR will not be effective.[5] By failing to strike this balance, Australia has struggled to amass industry and consumer participation in its CDR.[6] This lack of participation can be partly explained by the legislative choices made in crafting the framework.

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

The Bill proposes to depart from the Australian model in numerous ways. Key departures include the approach to the application of privacy principles, the inclusion of write access and the exclusion of reciprocity which, in sum, could markedly alter the functionality of the regime.[8] Furthermore, unique to New Zealand, emphasis has been placed on Māori data sovereignty which introduces a unique consideration for the implementation of a CDR.[9]

---

3 See Ministry of Business, Innovation and Employment *Draft for Consultation: Customer and Product Data Bill* (2023) [Exposure Draft Bill]; and Customer and Product Data Bill 2024 (44-1). The Exposure Draft Bill was prepared by the Parliamentary Counsel Office and released alongside a Discussion Document (Ministry of Business, Innovation and Employment, above n 2) which provided commentary on provisions and sought feedback on certain aspects of the Exposure Draft Bill. The Bill remained largely the same as the Exposure Draft Bill with some alterations (such as the inclusion of penalties) in response to feedback on the Exposure Draft. Since this article was written, the Bill has progressed from the Economic Development, Science and Innovation select committee through to the Committee of the Whole House.

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, The Netherlands, 2023) at 111.

6 Kelly, above n 4, at 41–42.

7 See Farrell, above n 5, at 113.

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

9 See generally Te Kāhui Raraunga *Iwi Data Needs* (12 March 2021); and Te Kāhui Raraunga *Māori Data Governance Model* (26 May 2023).

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

A Open Banking as an Example

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 is the first intended application for New Zealand's CDR.[12]

While open banking has no singular agreed-upon definition, the Canadian Federal Advisory Committee on Open Banking defines it as:[13]

> … 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.

In the open banking context, the CDR allows customers to request that their data, such as account balances, credit facility and spending details be shared.[14] For example, a FinTech[15] (as an accredited requestor) could 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

10 Any article 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 article's scope.

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

12 Ministry of Business, Innovation and Employment, above n 2, at 4.

13 Canadian Federal Advisory Committee *Final Report* (Department of Finance Canada, April 2021) at 29.

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

15 "FinTech" is an abbreviation of "Financial Technology." This is a term used to refer to financial service providers who integrate technology to enable their services. An accredited requestor is a requestor of data that has been accredited under sub-pt 3 of the pt 5 regime under the Bill. Accreditation means the requestor's request will be mandatory; this is explained in more detail in Part III(A).

customer.[16] With the customer's consent, a FinTech could then action the switch to a better account.[17] This can also allow the separation of previously bundled banking services.[18] The availability of this valuable data will empower new entrants in the market,[19] enabling the provision of new creative services.[20]

B The CDR at a Glance

The Bill requires data holders to make product data available electronically.[21] This allows third parties to interact with the data. For example, in the banking context, up-to-date comparisons of mortgage account interest rates could be provided; or, in the telecommunication context, the price of one gigabyte of data. Additionally, and perhaps more importantly, individuals will be able to mandate that a registered data holder share their personal data with a third party – an accredited requestor (AR).[22] The requested data will be shared in a standardised machine-readable format so an AR can use the information for the customer's benefit.[23] Differing from industry-specific data portability like open banking, a CDR can apply to other industries as they are designated by the Minister of Commerce and Consumer Affairs (the Minister). Currently, the telecommunications, energy and health sectors are being considered as the next designated sectors after open banking, providing for an expansive economy-wide right of data portability.[24]

---

16 There are existing online tools that compare products, but the CDR enables FinTechs to personalise these to the customer.

17 This will require the use of action initiation or "write access". See Part III for further discussion.

18 Basel Committee on Banking Supervision *Report on open banking and application programming interfaces* (19 November 2019) at 8.

19 Ariadne Plaitakis and Stefan Staschen *Open Banking: How to Design for Financial Inclusion* (Consultative Group to Assist the Poor, October 2020).

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

21 For example, this can include a company's product offerings and product eligibility requirements: Customer and Product Data Bill, cl 22. For clarity, data holders will be a defined class of persons in each sector: Customer and Product Data Bill, cl 6.

22 Customer and Product Data Bill, cl 15.

23 Customer and Product Data Bill 2024 (44-1) (explanatory note) [Explanatory Note]; Ministry of Business, Innovation and Employment, above n 2, at [164].

24 See Scott Farrell *Future directions for the Consumer Data Right* (Australian Government Treasury, October 2020) at 1. See also Ministry of Business, Innovation and Employment, above n 2, at [46].

This can be contrasted with the current system, where such data is largely unavailable, or where a customer must personally supply any third party with the relevant information.[25] Information can also be supplied through unsecure and rudimentary data-sharing methods such as screen scraping.[26]

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.

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 that Act, individuals can request personal information held about them from data holders. This process can take up to 20 days and may incur financial costs.[27] Further, the information provided is not necessarily in a standardised form and is not available to any third party unless provided by the customer. The CDR builds on this limited right to data provided for in the Privacy Act.[28]

C Instruments of the CDR Framework

The Bill 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 specific rules and technical specifications.[29] Each instrument is subject to its own concerns and debates, which are beyond this article'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.

1 Sector designation

Like Australia, the Bill provides that the CDR will be implemented on an industry-by-industry basis.[30] Any industry or sector is to be designated by the Minister.[31] For each sector, this legislative

25 Negotiating bespoke data-sharing agreements without any underpinning by a CDR is possible. These exist sparsely (but primarily in the open banking sphere). For example, see Xero's arrangement with ANZ: Xero Central "ANZ NZ direct feeds" <www.central.xero.com>.

26 Screen scraping typically involves a third party logging into a customer's account and extracting the required information. These authorisations 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 WSO2 "Open Banking Accelerator Documentation" <www.ob.docs.wso2.com> (under "What is Open Banking?").

27 Privacy Act 2020, pt 4.

28 The Bill clarifies that requests for personal information under the Privacy Act (IPP 6) are not prevented: Customer and Product Data Bill, cl 17.

29 Explanatory Note, above n 23; and Ministry of Business, Innovation and Employment, above n 2, at [76].

30 See Customer and Product Data Bill, pt 5.

31 Clause 97.

designation will specify the types or scope of data, parties eligible to be data holders, the functionality enabled and the rules governing data transfer.[32]

2 Accreditation

The Bill creates an accreditation regime for those who want to make binding requests for designated customer data. Accreditation regulates the approval to enable parties to be accredited as ARs as an attempt to ensure that a provider will meet the trust required under the Bill and future secondary legislation.[33] Overseas experience shows that it is vital for any data-sharing regime to have a high level of trust.[34] Differing from what was suggested in the Exposure Draft Bill, entities that are not accredited cannot request customer data or initiate actions.[35]

D How it Will Work

Broadly speaking, the CDR will be technically enabled by Application Programming Interfaces (APIs).[36] At its core, "an API is a documented set of connecting points that allow an application to interact with another system".[37] APIs can autonomously process transaction information and communicate from one data holder or AR to another.[38] Figure 1 illustrates where APIs would sit in the banking system.

---

32 Clause 100.

33 Part 5, sub-pt 3.

34 Clause 64 of the Customer and Product Data Bill prohibits any person from holding themselves or another person out as an accredited requestor. A contravention of this clause can result in civil liability and a pecuniary penalty being ordered under cls 72, 73 and 75. Part II(C)(2) of this article discusses accreditation in the context of action initiation.

35 Explanatory Note, above n 23. Compare Exposure Draft Bill, above n 3, cl 7.

36 Spotfire "What is open banking?" <www.spotfire.com>.

37 Laura Brodsky and Liz Oakes *Data sharing and open banking* (McKinsey&Company, July 2017) at 5.

38 Spotfire, above n 36.

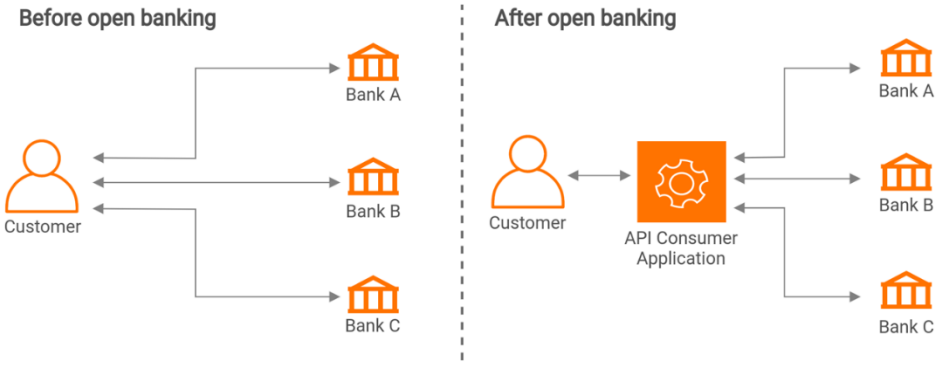

Figure 1: Visualisation of APIs in open banking[39]

An important factor to bear in mind is that APIs can be open or proprietary.[40] Without a CDR regime, the few existing data-sharing arrangements are enabled by bespoke agreements.[41] In each industry, large companies would likely issue a set of APIs accompanied by potentially unfavourable terms and conditions, which partners would be pressured to accept.[42] Introducing standardised APIs and terms and conditions is important, as parties with less bargaining power could otherwise 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, maintain and update customised systems for retrieving and processing data from multiple data holders.[43] This would add untenable cost and complexity to the system.[44]

---

39 WSO2, above n 26 (under "A sample open banking use case"), used under CC BY 4.0 license without changes.

40 Open APIs are freely available to the public and are typically not managed by a directly interested party. Closed or proprietary APIs are designed and maintained privately and can only be used if access is granted. See Cameron McKenzie "What is an open API (public API)?" TechTarget <www.techtarget.com>; and Brodsky and Oakes, above n 37, at 5.

41 For example, the partnership struck by ANZ and Xero which allows small to medium businesses to streamline their accounting.

42 Brodsky and Oakes, above n 37, at 5.

43 At 6.

44 Ministry of Business, Innovation and Employment *Regulatory Impact Statement: Establishing a Consumer Data Right* (23 June 2021) at 62.

While not dictated by the Bill, each designation will issue standardised data standards and APIs, similar to the Australian Act. These standards will build on the open APIs being developed by the New Zealand API Centre.[45]

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

III "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 tenet of a CDR, "read access" describes the ability for data to be shared with ARs in a machine-readable format. In the open banking context, this could include bank balances. This allows ARs to utilise in-scope customer information stored by data-holders. Building on "read access", "write access" will allow ARs to issue instructions to data holders when authorised by a customer. Write functionality was referred to as an "action request" or "action initiation" in the Exposure Draft Bill, while it is referred to as an "action" or "designated action" under the Bill.[46] Write access enables the "writing" of data, providing functionality such as moving data and updating details. In the open banking context, this includes opening and closing accounts or moving funds.[47]

Including action initiation in New Zealand's CDR is consistent with the United Kingdom's open banking legislation but significantly departs from Australia's approach, which deliberately excluded write functionality until a later date.[48] 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 that has been observed in Australia.

While Australia is currently legislating to allow action initiation, this will not be functional at least until the Australian CDR's fourth operational year.[49] Australian regulators were particularly mindful to ensure customers initially gained confidence in the CDR as a data-sharing framework. They were

---

45 Office of the Minister of Commerce and Consumer Affairs *Establishing a Consumer Data Right* (Ministry of Business, Innovation and Employment, 9 July 2021) at 4.

46 See Exposure Draft Bill, above n 3, cl 81; Ministry of Business, Innovation and Employment, above n 2, at [132]; and Customer and Product Data Bill, cl 18.

47 Ministry of Business, Innovation and Employment, above n 2, at [132].

48 See The Payment Services Regulations 2017 (UK). See also Ross P Buckley, Natalia Jevglevskaja and Scott Farrell "Australia's Data-Sharing Regime: Six Lessons for Europe" (2022) 33 KLJ 61 at 88–90.

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

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.[50] Arguably, the exclusion of functionality enabled by write access had the opposite effect of hampering the CDR's utility, which disincentivised consumers from using the system.[51]

As action initiation is intended to be included in New Zealand from the outset, the Australian concerns regarding its inclusion 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.[52]

A Accreditation for Action Initiation

The explanatory documents accompanying the Exposure Draft Bill indicated that there would be different tiers of accreditation for read and write access. These two classes were described as having differing requirements and obligations correlating to the perceived risk levels associated with read access and write access – ensuring costs and protections are proportionate to the risk.

The Bill incorporates these tiers of accreditation through reference to "classes of accreditation". These classes will be included in designations – which are secondary legislation – meaning that the Bill itself does not impose any classes of accreditation, such that requestors who seek either read access or write access would not be required to apply for a separate class.[53] Instead these classes are left to be created as each sector is designated.[54] The Bill allows types of designated actions (write access) to be considered when designing these classes. It is likely the intention that each sector designation will impose differing classes of accreditation for read and write access.

It may also be prudent for New Zealand to mirror the Australian amendment legislation.[55] The Australian 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. While not

50 Kelly, above n 4, at 17.

51 Farrell, above n 24.

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

53 Customer and Product Data Bill, cl 100.

54 These designations will be made by the Governor-General on the recommendation of the Minister: see cl 97.

55 The Bill passed its final reading in the Senate on 15 August 2024. The Bill seeks to incorporate recommendations from the Statutory Review of the Consumer Data Right, above n 4.

provided for in the Exposure Draft Bill, it appears that under the current wording of the Bill, such considerations are available to the Minister when designating a sector.[56]

There was no clear restriction in the Exposure Draft Bill on non-accredited parties making data requests or action initiation requests.[57] An initial draft of this paper which preceded the Bill argued action initiation should be reserved for accredited parties.[58] 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. The Bill has subsequently confirmed that only ARs will be able to initiate actions and request customer information under the regime.[59]

As suggested in the discussion document, accreditation for action initiation should include a condition that requires a requestor's systems and policies to be used ethically, responsibly and fairly.[60] This wording has been omitted from the Bill. However, its inclusion could play a role both in creating a robust accreditation regime and assuring customers that the use of action initiation is safe.[61]

B Authorisation

The addition of action initiation increases the already vital requirement for public trust in the system. The Bill achieves this by requiring customer consent as a central component of all data sharing, focusing on consent by reference to "authorisation". Under the Bill, authorisation must be "express", and the customer must be "reasonably informed about the matter to which the authorisation relates".[62] The effect of this is that consent must be meaningful.

Consent documents which are drafted in an overly legalistic manner do not, in substance, allow customers to make informed decisions. Legislators should consider including in the Bill a requirement for standardised consent requests, which must make clear what authorisations are requested and how far authorisation will extend. The Bill allows for the "manner" of consent to be prescribed in each designated sector but does not impose this in any mandatory form.[63]

---

56 Customer and Product Data Bill, cl 100.

57 Ministry of Business, Innovation and Employment, above n 2, at [89] and [166].

58 Customer and Product Data Bill, cl 100.

59 Explanatory Note, above n 35.

60 Ministry of Business, Innovation and Employment, above n 2, at [141].

61 Even if this is already the case in effect, the addition of a clarifying provision will increase consumer confidence in the system.

62 See Customer and Product Data Bill, cls 36–38. The requirements in the Bill are more stringent than the consent requirements in the Privacy Act 2020. Additional discussion can be found in Part IV.

63 Clause 36.

The discussion document also sought feedback on how long consent should last, which dictates how often an AR needs to collect consent from the consumer for an authorised activity.[64] The Bill only requires authorisation to be collected and confirmed once for all services within the scope of authorisation (until expiry) instead of requiring consent for every action. Length of authorisation is a decision left to be made on a sector-by-sector basis, with the Bill prescribing no general rule.[65]

When deciding on the length of authorisation, 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. Departing from the currently proposed approach, which imposes no maximum period that consent can last,[66] it is arguable that a standardised maximum consent period of 12 months, after which consent must be renewed, would be preferable.[67] A 12-month maximum consent period would arguably provide both the required customer protection and a commercially workable timeframe. 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,[68] but would still ensure that customers are actively deciding to allow their data to be shared.

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.

C 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 the CDR to succeed, it must be perceived as safe and useful. While the Bill cements consent as a key requirement of the CDR, it leaves much of the substance to be decided at a sector level through secondary legislation. In promoting public uptake of the CDR, it is not enough that the system is, in fact, safe – consumers must also know this fact and believe it to be true. To achieve this, more protection should be

64 See Ministry of Business, Innovation and Employment, above n 2, at [55]–[65].

65 Customer and Product Data Bill, cl 36.

66 It also leaves the decision to be made on a sector-by-sector basis.

67 This approach was considered in MBIE's discussion documents in the exposure draft stage: see Ministry of Business, Innovation and Employment, above n 2, at [63].

68 At [64].

standardised by the legislation, applying to all sectors. Currently, the effectiveness of the consent will depend on how the regulations are designed and could differ substantially on a sector-by-sector basis.

While consumer confidence is crucial, 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.

IV PRIVACY ACT IMPLEMENTATION COMPARISON AND CONSIDERATIONS

The CDR centres on data transfer, which naturally raises privacy as a crucial element to be carefully addressed. Ensuring the proper handling of data enables the system to function effectively and fosters public trust in its operation.

At its core, the privacy legislation in both New Zealand and Australia acknowledges an individual's right to access the data held by other parties.[69] Compared to the Australian equivalent, New Zealand's privacy legislation is better positioned to enable a CDR. As such, the Bill avoids regulatory overlap by relying on its present privacy law instead of legislating on top of it, as has been done in Australia.[70] This approach arguably does not yield an ideal outcome, instead prioritising functionality and practical considerations.

A Australia's Implementation of Privacy Protection

Comparing the two regimes requires context as to how the Australian CDR interacts with the Australian Privacy Act 1988.

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 "Privacy Safeguards".[71] The Privacy Safeguards are placed within pt IVD of the Competition and Consumer Act.[72] These safeguards will apply when an AR requests data or a data holder collects data from a customer.[73]

---

69 See Privacy Act 2020, s 22 IPP 6; and Privacy Act 1988 (Cth), sch 1 APP 12.

70 Competition and Consumer Act 2010 (Cth), pt IVD, division 5.

71 Australian Government Treasury *Consumer Data Right Privacy Protections* (December 2018) at 4. Further discussion of the Privacy Safeguards can be found in Table 1 of this article.

72 Part IVD of the Competition and Consumer Act 2010 (Cth) was inserted through amendment by the Treasury Laws Amendment (Consumer Data Right) Act 2019 (Cth).

73 See Competition and Consumer Act 2010 (Cth), pt IVD, s 56EA.

Broadly, these Privacy Safeguards (and the Australian Privacy Principles (APPs) in its Privacy Act) regulate how organisations can collect and handle personal information.[74]

The Australian Privacy Act applies only to personal information collected and handled by businesses with more than AUD 3 million annual turnover.[75] 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.[76] This imposes significant costs and creates complexity. In some cases, it has also dissuaded certain parties from entering the regime.[77]

B New Zealand's Approach

Instead of duplicating Australia's Privacy Safeguards, New Zealand has opted to rely on its existing Privacy Act, with additional protection provided by the Bill.[78] The Bill has an extended scope applying to "identifiable customers" compared to the Privacy Act's more limited "identifiable individuals", allowing trusts and companies to benefit from the Bill.[79]

The Privacy Act 2020 and its Information Privacy Principles (IPPs) govern the collection, use, disclosure, storage, retention and access to personal information.[80] 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.[81] Fundamentally, New Zealand's Privacy Act can be applied across the CDR without needing many additional requirements within the Bill.[82]

---

74 Australian Government *Your privacy rights* (November 2020).

75 Privacy Act 1988 (Cth), s 6D.

76 Natalia Jevglevskaja and Ross Buckley "The Consumer Data Right: How to Realise This World-Leading Reform" (2022) 45 UNSWLJ 1589 at 1616.

77 See Kelly, above n 4.

78 See Explanatory Note, above n 35; and Ministry of Business, Innovation and Employment, above n 2, at [25]–[35].

79 For clarity, the Privacy Act 2020 retains its original scope of "identifiable individuals". The Bill, diverging from the Act, extends the types of data it applies to. See Ministry of Business, Innovation and Employment, above n 2, at [17].

80 DLA Piper Data Protection Laws of the World "Collection & Processing: New Zealand" (18 January 2024) <www.dlapiperdataprotection.com>.

81 See Privacy Act 2020, s 4.

82 From a consumer confidence perspective, using the Privacy Act 2020 instead of overlaying new regulations baked into the Act (as was done 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 indeed safe.

By applying the existing Privacy Act to the Bill (unless in contravention of a clause in the Bill), New Zealand avoids legislative overlap. However, the Privacy Act must also be fit to enable a CDR. Neither the Bill's explanatory note nor the Ministry of Business, Innovation and Employment's (MBIE's) discussion documents provide a detailed consideration of the two countries' approaches to privacy protection. The tables below compare New Zealand's existing IPPs against Australia's Privacy Safeguards.[83] The comparison highlights some gaps between the Safeguards and the IPPs. It concludes that with supplementation in the Bill, 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.

New Zealand IPP[84]	**Australian Privacy Safeguard**[85]	**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. IPP 2 is not directly compatible with a CDR's strict consent requirements – consent requirements in the Bill 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 Bill.
IPP 4 – Manner of collection of	PS 4 – Dealing with unsolicited CDR	IPP 4 allows collection of data in lawful, fair and not unreasonably intrusive ways. While not directly comparable, PS 4 imposes a strict

83 Or APPs, when applicable.

84 Privacy Act 2020, s 22.

85 Competition and Consumer Act 2010 (Cth), pt IVD, division 5, subdivision B.

personal information	consumer data from CDR participants	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 – Access to personal information	The Privacy Safeguards do not have an IPP 6 equivalent. Australian Privacy Principle (APP) 12 imposes this standard. The Bill states that the basis of data sharing under the CDR is not founded on IPP 6.[86]
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.[87]
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 longer than necessary	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.
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

86 Customer and Product Data Bill, cl 52.

87 This remains similar to PS 13.

		the original lawful purpose.[88] The IPP 10 ability to utilise data beyond the consented purpose is not compatible with a CDR. This incompatibility has been overridden by the strict authorisation requirements within the Bill.[89]
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. 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 Bill – it prevents misuse.

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

88 Privacy Commissioner "When can I use the directly related purpose exception?" <www.privacy.org.nz>.

89 Customer and Product Data Bill, pt 3.

PS with no IPP equivalents	Draft law implementation
PS 5 – Notifying of the collection of CDR consumer data	PS 5 requires accredited businesses to notify customers through the consumer dashboard when data is collected.[90] It is unclear if this is included in the Bill. The use of a consumer dashboard appears to be currently undecided.[91]
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	The Privacy Act 2020 has no IPP equivalent.
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.

Table 2: Privacy Standards with no IPP equivalent

This comparison with Australia's Privacy Safeguards demonstrates that the IPPs are broadly fit to protect customer data under a CDR, with most of the newly drafted Privacy Safeguard requirements already met by the IPPs. There are key deficiencies 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 Bill remedies these deficiencies by clarifying that the IPPs do not apply when in contradiction with the Bill. Strict authorisation provisions included in pt 3 require express and reasonably informed consent to be provided, which prevents the types of collection permitted under IPPs 2, 3 and 4.

Similarly to the Australian system, the consent provisions imposed by the Bill may result in some instances of overlapping regulation depending on whether a data holder is acting within or outside of the CDR.

The IPPs are not specifically designed for a CDR, whereas the Privacy Safeguards were designed for that very purpose. Several concerns arise from this implementation of privacy protections.

---

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

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

Notably, the IPPs are expressed as principles to be adhered to, while the Bill suggests secondary legislation will be drafted to implement prescriptive standards which must be complied with.[92] It is still unclear what these might include. While this is not dissimilar to the Australian regime, it is certainly not the most harmonious solution. The IPPs 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 this kind would need to be considered on its own merits. The Customer and Product Data Act is not the appropriate vehicle to bring such change.[93]

C Deletion of Data

Central to privacy and a key functionality missing from the Bill is the ability for customers to request/demand their data be deleted. The concept of deletion is provided for in both the IPPs and the Bill. However, it exists only in the context of the requirement to not hold data for longer than is required for the authorised purpose.[94] This section suggests that a standalone right to deletion should be established.[95]

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.[96] 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 allowing consumers to 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, there will be inherent uncertainty around which party has access to what data, and whether authorisation continues. The deletion of data will be an important

---

92 Customer and Product Data Bill, cls 126 and 132.

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

94 Privacy Act 2020, s 22, IPP 9.

95 For deletion of data, see Ministry of Business, Innovation and Employment, above n 2, at [132]. See generally Farrell, above n 5, ch 8 "Preserving Value of Shared Customer Data".

96 Corporate Finance Institute "Non-Rivalrous Goods" (29 May 2024) <www.corporatefinanceinstitute.com>.

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 obligations, that may be impacted. It may also create unexplained inconsistencies between the two regimes. Nevertheless, 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.[97] While this arguably adds complexity to the legislative process and burdens ARs, it is a feature worth implementing.

D The Argument for an Improved Privacy Act

The Privacy Foundation argued that the Exposure Draft Bill did not create a comprehensive right to data portability, but rather that it enabled functionality through the draft law.[98] This reasoning is applicable also to the Bill. 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, or alongside, the implementation of the CDR.[99] The then-Minister, David Clark, stated that (similar to the approach taken in Australia) he would not recommend the establishment of additional data rights to underpin the CPD regime.[100] He argued 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 legislation 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).[101] Such protections could include updating consent requirements to require express consent for use or collection of personal data, and strengthened notification in the Privacy Act to align with the draft legislation's more onerous and consumer protection-focused equivalents.

---

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

98 See Marcin Betkier *Submission on discussion document: 'Unlocking value from our customer data' and on the Customer and Product Data Bill* (Privacy Foundation NZ, 24 July 2023).

99 Commerce Commission *Options for establishing a consumer data right in New Zealand: Submitted to Ministry of Business, Innovation and Employment* (19 October 2020) at 6.

100 Office of the Minister of Commerce and Consumer Affairs, above n 45, at 5.

101 See Chapter 3 of Regulation 2016/679 on the General Data Protection Regulation [2016] OJ L119/1.

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 would have the flow-on effect of streamlining compliance. Many businesses will operate both in and out of the CDR framework, so 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 parties who collect and share data in and out of the CDR.

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

E Conclusion on Privacy

Overall, New Zealand's use of existing privacy law will be 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 will be met with the supplementation in the Bill. 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 Bill would benefit from adopting such a right. The customer benefit and a resultant increase in participants likely justify the cost to business.

Part IV argued for an overhaul of the Privacy Act 2020. Ideally, this reform would be executed in tandem with the Bill. However, the implementation of the CDR should not be shelved, waiting for the development of a hypothetical privacy framework that is more suitable.

V RECIPROCITY

Reciprocity 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.[102] Without reciprocity, ARs are not captured as parties (just by holding customer information) who are required to share data under the Bill. This obligation only applies to data holders, who are a class of persons who will be defined in sector designations.

The benefits of reciprocity are twofold. First, it creates a dynamic ecosystem by increasing the flow of data compared to a system in which ARs "are solely receivers of data, and data holders are largely only transmitters of data".[103] Secondly, it increases competition by allowing data holders and other ARs to benefit from the data which is generated. Having data move circularly prevents perceived disadvantages to incumbent data holders who view "big tech" companies (who are likely to be ARs)

---

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

103 Treasury Laws Amendment (Consumer Data Right) Bill 2018 (Cth) (explanatory memorandum) at [1.124], cited in Farrell, above n 5.

as a threat.[104] 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.[105]

The Australian CDR includes reciprocity as a principle, extending the possible obligation of data sharing beyond data holders. However, the concept of reciprocity is not included in the Bill. Submissions to MBIE from interested parties in response to the Exposure Draft Bill opposed the exclusion of a reciprocity principle. These are mainly from banks or their representative groups.

The exclusion of reciprocity in the Bill is preferable to its inclusion. Reciprocity imposes costs and regulatory complexity on developing FinTechs. 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 customer base. Partly in response to this issue, Australia's original principle of reciprocity has been watered down significantly – the principle now only applies to ARs after a year of operation.[106] 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.[107]

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

A Derived Data

Derived data refers to a class of information which has been subject to processing by the party that holds that data (typically data holders). It is, therefore, distinct from customer data, which is usually unprocessed.[108] The lack of reciprocity may delay derived or value-added data from being included as "in-scope data".

---

104 See for example Financial Services Council NZ *Submission to the Ministry of Business, Innovation and Employment on the Customer and Product Data Bill Exposure Draft* (24 July 2023) at 6.

105 Farrell, above n 5, at 139.

106 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" (5 April 2023) Norton Rose Fulbright <www.nortonrosefulbright.com>.

107 There are in fact some objections to the exclusion of reciprocal data-sharing obligations: see for example Financial Services Council, above n 104.

108 Office of the Australian Information Commissioner "What is the Consumer Data Right?" (23 August 2024) <www.oiac.govt.au>.

There have been objections by incumbent data holders to incorporating derived data within a CDR framework.[109] 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.[110] 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.[111]

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 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.

While the Bill provides the option for derived data to be included as "in scope", it must first be incorporated into a sector-specific regulation to be requestable. Therefore, the inclusion of derived data in the Bill does not necessarily mean it would be included as "in scope" from the outset. To avoid the complexities and one-sided arrangements that were experienced in the Australian CDR, derived data should only be included once a designated sector matures.

VI MĀORI DATA

A challenge unique to New Zealand is managing the interests of Māori and Māori data, which is a taonga. This 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 the private sector. As such, the Bill should consider the Treaty of Waitangi and tikanga principles when designating a sector or industry, and while drafting secondary legislation.

Much discourse in this field centres on the concepts of Māori data governance and Māori data sovereignty. Te Ngira defines Māori data governance as the "mechanisms, legal instruments and policies through which Māori exercise control over Māori Data" and defines Māori data sovereignty as "[t]he inherent rights and interests that Māori have in relation to the collection, ownership and application of Māori Data".[112]

---

109 See for example Financial Services Council, above n 104; AIA *Submission to the Ministry of Business, Innovation and Employment on the Customer and Product Data Bill Exposure Draft and Consultation Paper* (24 July 2023); and ASB *ASB response - Consumer Data Right discussion document* (24 July 2023).

110 See Farrell, above n 5, at 83–84.

111 At 83–84.

112 Te Ngira Institute for Population Research *Māori Data Sovereignty and Privacy* (University of Waikato, March 2023) at 3.

Māori have numerous interests in their data. First, as a taonga, data has deep cultural significance.[113] Secondly, stemming from the data's taonga status, Māori also have kaitiaki obligations over their data.[114] Thirdly, there is both an individual and collective interest in data, given that it can potentially unlock significant cultural and economic value.[115]

Collective Māori data is particularly important to iwi leaders, organisations and groups for utilisation in advancing common purposes.[116] One such purpose is the use of data in governance, as it allows iwi leaders to lead and develop "[their] people, places and interests toward their aspirational goals".[117]

In the context of the CDR, MBIE clarifies that:[118]

> … 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.

The concept of Māori data sovereignty applies to both the collection and privacy implications of data, and the use and 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).[119] 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.[120] 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.[121]

---

113 See Te Kāhui Raraunga *Māori Data Governance Model*, above n 9, at 3.

114 A kaitiaki relationship refers to a relationship akin to guardianship: see Joe Williams "Lex Aotearoa: An Heroic Attempt to Map the Māori Dimension in Modern New Zealand Law" (2013) 21 Wai L Rev 1 at 3.

115 See Te Kāhui Raraunga *Māori Data Governance Model*, above n 9, at 4.

116 The CDR has traditionally been seen as providing a right to individuals. However, the CDR in New Zealand also applies to businesses and trusts. This perhaps allows 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.

117 Te Kāhui Raraunga *Iwi Data Needs*, above n 9, at 5.

118 Office of the Minister of Commerce and Consumer, above n 45, at 12. The term "whakapapa" refers to a line of descent from one's ancestors; genealogy.

119 See Stats NZ "Integrated Data Infrastructure" (23 August 2022) <www.stats.govt.nz>.

120 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.

121 See Stats NZ "Census" <www.census.govt.nz>.

There is no singular, homogenous understanding of Māori data and its application, and the area of law is constantly evolving.[122] This section discusses relevant issues but does not offer conclusive suggestions. Any conclusions would require discussion beyond the scope of this article, and extensive consultation with, and decision-making, of Māori interest groups. Given the importance of protecting and promoting Māori data sovereignty, further work in this area will become increasingly critical.

A Māori Health Data Example

The Te Pou Matakana judicial review case demonstrated how the CDR can strengthen Māori data sovereignty. The case revolved around Whānau Ora,[123] which was commissioned by Te Puni Kokiri to provide underserved communities with COVID-19 vaccinations.[124]

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 they were most required. The Ministry shared with Whānau Ora "anonymised … [street level] mapping representations that show areas with unvaccinated communities".[125] Whānau Ora asserted that this information was not specific enough to enable them to carry out their function.[126]

While slightly speculatory given that 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.[127] This would fundamentally increase Māori control over their data and directly allow for Māori data governance, which increases Māori data sovereignty.

B Storage of Data

A substantial body of literature discusses the concerns related to the offshoring of Māori data.[128] It is important to note that the Bill does not alter existing data storage obligations and will not impose

---

122 See generally Natalie Coates "The Recognition of Tikanga in the Common Law of New Zealand" [2015] NZ L Rev 1 at 20–21.

123 A government-funded, Māori-delivered agency which supports whānau wellbeing and development.

124 *Te Pou Matakana Ltd v Attorney-General* [2021] NZHC 2942, [2022] 2 NZLR 148 at [11].

125 At [16(a)].

126 At [22].

127 There should be consideration here of the possibility that unvaccinated people may not consent to sharing their data.

128 See for example Bell Gully *Offshoring New Zealand Government Data: A report prepared for Statistics New Zealand* (21 June 2021).

new ones.[129] 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 of data. Consequently, the government and private sector have increasingly offshored many of their data storage requirements.

As the CDR will facilitate an increased amount of data transmission, the amount of data stored overseas will necessarily increase. This is especially concerning in the context of Māori data rights. First, Treaty obligations do not apply outside New Zealand's jurisdiction.[130] Secondly, companies may be compelled to surrender data to foreign governments upon request.[131] 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 over their data.[132]

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.

C Cultural Capability

The Bill 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[133] and kaitiakitanga[134] 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 status and data sovereignty rights of Māori.

---

129 Ministry of Business, Innovation and Employment, above n 2, at [48].

130 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.

131 For example, the United States asserts jurisdiction over data stored internationally by United States-headquartered companies. See for example *United States v Microsoft Corp* 584 US (2018).

132 Te Kāhui Raraunga *Māori data sovereignty and offshoring Māori data* (27 July 2022) at 16.

133 The tikanga concept of nurturing relationships.

134 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.[135] Cultural competency requirements may be an effective way to address these inequities. Including cultural competency requirements can make the CDR more inviting and accessible for Māori, respecting the principles of kotahitanga[136] and whakawhanaungatanga.[137] These requirements acknowledge the importance of embracing diverse perspectives within New Zealand's society, and upholding Treaty of Waitangi obligations.

On the other hand, it is important to consider potential drawbacks. A central issue discussed in this article 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 businesses may discourage them from interacting with the CDR. This effect may be amplified for international participants looking to enter the New Zealand market.[138] 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.

When designing the Exposure Draft Bill, MBIE suggested 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 be to provide 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.

D Considering the MDG

A report by Te Kāhui Raraunga outlines a Māori Data Governance Model (MDGM) designed by the Iwi Leaders Group and Māori data experts.[139] The report is primarily designed for the public sector but provides valuable insights for broader legislative design. The report recognises eight pou (pillars) of Māori data governance that, when viewed holistically, promote and enable "iwi, hapū and Māori organisations, businesses and communities to pursue their own goals for cultural, social, economic and environmental wellbeing".[140]

---

135 See for example in the banking context Reserve Bank of New Zealand *Improving Māori Access to Capital: Issues Paper* (9 August 2022).

136 The tikanga concept of unity.

137 The tikanga concept of building positive and collaborative relations; the construction of aspirations and goals.

138 It is worth noting that international entrants to the market will likely have less understanding of Māori data and tikanga principles.

139 Te Kāhui Raraunga *Māori Data Governance Model*, above n 9, at 3.

140 At 16.

Although regulations such as data storage obligations and cultural capability would currently harm the efficacy of the CDR if expressly legislated, other protections can still be considered. This section will briefly consider pou 3–6.

1 *Pou 3*

Pou 3 offers guidance and ideal outcomes for the collection of Māori data.[141] 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 be 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. In the exposure draft process, MBIE indicated that the MDGM would be central to the process.[142] However, the Bill has weakened the language which required consultation with iwi, hapū and Māori organisations to now only requiring consultation with "*1 or more people* who have expert knowledge of te ao Māori approaches to data".[143]

2 *Pou 4*

Pou 4 relates to privacy and consent. Consent requirements are a foundational control in the Bill – aligning with the importance placed on consent in the MDGM.[144] However, the Bill 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.

For Māori, a collective interest exists where data sharing has the potential to harm collective rights, which cannot be reduced to individual privacies.[145] This is an important consideration for the CDR as the Privacy Act does not include Māori-specific privacy considerations.

This is especially evident in the health context with data relating to DNA. Although individual autonomy is important, significant consideration must also be given to the whakapapa in the data. The MDGM suggests that "[i]ndividual consent to share such data is inadequate given the collective interests and risks involved" in how personal data is aggregated.[146] 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.

---

141 At 30–32.

142 Ministry of Business, Innovation and Employment, above n 2, at [43].

143 Customer and Product Data Bill, cl 134(1)(c) (emphasis added).

144 At 33–37.

145 Te Kāhui Raraunga *Māori Data Governance Model*, above n 9, at 33.

146 At 35.

3 Pou 5

The CDR facilitates the "[a]ccess as a process" principle in Pou 5.[147] This 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.

4 Pou 6

Pou 6 considers the secondary use of data, including data linkage, sharing or aggregation. This pou stresses that all data uses must be explained and explicitly agreed to.[148] This would include when data is used for statistics or anonymised for other uses.

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, the legislature should consider requiring express and unbundled consent requirements for this use.

E Conclusion on Māori Data

Māori data concepts are an evolving issue, particularly in the concept of data-sharing. The CDR should increase Māori data sovereignty by enabling access and control of data held by third parties. However, inherent tensions exist between the current predominantly Western use and understanding of data, 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 Māori data sovereignty. 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 has the opportunity to lead in the meaningful consideration of indigenous rights in this context. Many other nations will be watching New Zealand's approach with interest.

VII CONCLUSION

The Consumer Data Right is a comprehensive right aimed at unlocking value from consumer data. The Bill 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

147 At 38–42.

148 At 43–45.

with the system and the willing participation of accredited requestors.[149] Therefore, the CDR must prioritise design choices that safely and conscientiously promote this objective.

This article explored key considerations in Parts III through VI, emphasising the need for pragmatism in addressing challenges. Part III argued that write access in the Bill 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 it enables will attract customers to the system. Part IV concluded that New Zealand's approach of utilising the existing Privacy Act 2020 and its Information Privacy Principles is mostly sound. Importantly, it avoids regulatory overlap caused by legislating on top of the existing Act, which would impose significant costs and possibly dissuade service providers from entering the market. Part V argued that despite opposition from industry, the exclusion of reciprocity is sound. It will enable market entrants to establish themselves without significant additional burdens. Finally, Part VI considered the complexities of Māori data and how tikanga principles best fit into the CDR. Without making any concrete conclusions, it suggested 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 into the market with an over-regulated approach. Many important choices remain as New Zealand's CDR is still in the early stages of legislative development. Parliament should continue to prioritise useful functionality to attract customers and, where prudent, minimise regulatory burdens in order to strike the correct balance.

149 See Anton Didenko "Australia's Consumer Data Right and Its Implications for Consumer Trust" (2024) 50 Mon LR 61.