



**Submission to the
Economic Development, Science and Innovation Committee
Select Committee**

on the

Customer and Product Data Bill

5 September 2024


***Prepared by the Policy and Regulatory sub committee of Digital Identity NZ's
Executive Council comprising volunteer member organisation representatives from a
mix of large and small businesses.***

Digital Identity New Zealand (DINZ) thanks the Select Committee for the opportunity to provide a submission on the Customer and Product Data Bill (CPD)

We continue to support the overall intention of the proposed legislation: to provide a framework to realise the value of certain data for the benefit of individuals and society; to promote competition and innovation for the long-term benefit of customers; and to facilitate secure and efficient data services.

Nonetheless there are areas where our members offer precautionary notes and specific concerns where the Bill is capable of improvement if it is to deliver on the intended outcomes that we all want to see evidenced.

As always, we are happy to provide any clarifications in writing, on a call, or in a physical meeting.

DocuSigned by:

F84DA1755B8C410...
Colin Wallis
Executive Director,
Digital Identity NZ
M +64 21 961955 Wellington



About Digital Identity NZ (DINZ)

DINZ is a not-for-profit, membership-funded association of approximately 100 organisations across the public and private sectors, representing a variety of industries as well as individuals. Recognised as the foremost industry voice for Digital Identity in NZ, it is part of the New Zealand Tech Group (NZTech), connecting the digital identity community and seeking to actively influence policy and solutions. DINZ members help facilitate digital identity and digitisation across the board in instances such as public-facing government services, open banking, account opening and customer & product data under consultation here, which are all underpinned by digital identity in concert with AI, biometrics and cloud computing. Some members deploy digital ID and verification software and related solutions both in NZ and other countries.

Relevance to DINZ

The CPD Bill establishes a new right for an approved business (with customer consent) to access products and consumer information held by other businesses. This right also creates mandatory obligations on businesses holding data to make the information available and to verify their customer has authorised the release. These rights and obligations must be balanced with responsibilities for data protection, privacy, and confidentiality. This is a complex scenario requiring careful regulation as well as standards for data and communications.

Traditional Identity and Access Management digital systems do not cater well for scenarios where identity and access permissions are determined by external parties. Without adequate mechanisms to claim, validate, verify, and express individual identity and consent, meeting obligations to provide consumer and product data will be challenging at scale. Digital Identity Services and a robust trust framework will be essential components.



Opening Statement

DINZ joined forces with FinTechNZ to host a 'town hall' styled dynamic submission webinar for MBIE on July 17 2023, in response to the initial consultation and on the Draft Exposure Bill. Alongside our overall support, matters raised there look to be reflected in the Bill, for which we are grateful. Introductory comments, precautionary notes and specific concerns follow, to further frame our support for the Bill proceeding.

Opening Comments

Scope and purpose of the Bill - going back to the original intent:

A clearly defined customer data right should be the focus of this Bill. There is no "new" data right created by this Bill for the customer. Earlier consultation documents on the proposed CPD released earlier outlined a vision of granting a customer a right to its customer-related data. With this right, the customer would then be empowered to authorise a third party to request that specific data on their behalf from a specific data holder. The Bill has changed this, and it effectively grants the data right directly to the requesting party, with a control requiring them to obtain authorisation from the consumer. This structure creates legal and practical complexities that could be avoided if the intent in the original paper was followed. Of course, it is acknowledged that the Bill does contain clauses that define a data right for the individual. However, this is a subset of the data rights created by the Privacy Act Information Privacy Principle (IPP) 6 in the Privacy Act. There is no "new" data right created by this Bill for the customer.

Banks and electricity retailers simply opening up their books for customers to be able to request information (or request a transaction be made on their behalf) is simply one side of the equation (although evidence on why these were the first designated sectors seemed absent from the consultation documents). A strong set of competitive third-party data requestors, where the customer has a choice between multiple providers to authorise data access and transactions is another side of this. But a bigger picture emerging is how customers are informed, empowered to act on this information and given options to choose from a range



of suppliers and at a minimal cost. (Many third party providers charge a subscription fee to the customer so access to data is not free or in some cases quite expensive).

Customers will need to be informed to choose (and have a strong ongoing consent mechanism) with third parties. How this ongoing consent mechanism works should also be carefully considered within the Digital Identity Services Trust Framework. These providers should also ideally have services that can enhance their offering across a customer's data footprint, according to the customer's desire for integration across transactions like taxes, bank accounts, budget services etc. To do that, others outside of the designated sector should be included within the CPD - something that the NZ Commerce Commission highlighted in its recent report: [A stronger Kiwibank and open banking could shake up NZ banking sector, 20 August 2024](#).

[Foster a competitive environment:](#)

For a good supply of third-party data requestors there needs to be not only sustainable business value for them but also the regulations that support this legislation will need to be internationally interoperable (i.e. use international standards for information sharing). Without this, New Zealand providers will develop solutions that cannot interoperate and be sold overseas. Furthermore, an international-standards and interoperable regulatory system will mean off-the-shelf solutions can be offered in the New Zealand market, supporting a more innovative and cost-effective ecosystem whereby New Zealand customers benefit from a competitive range of solutions.

[Learn from overseas regimes:](#)

We urge caution in rushing with the Bill, and risk pushing this on to the market before fully appreciating the current landscape and lessons learned from overseas. This Bill is following a path forged by the UK and Australia, with a view that increased data sharing would offer the potential for greater competition (particularly in concentrated markets), enable the development of alternative business models, and provide transparent and comparable information about



pricing and products in order to inform customers in their purchasing choices. A worthy pursuit but needs careful implementation and consideration.

Australia right now is undergoing a review of its CDR legislation and learning that the supporting regulations are just as important as the legislation itself to deliver on the intent. That there has been low (estimated at around 0.3%) uptake, speaks for itself. The Australian banks have spent an estimated \$1.5billion on implementing and operating the CDR regime.

The experience in Australia over the nearly four years is not encouraging. Implementation costs were substantially higher than predicted, as are operational costs. Uptake has been described as “extremely low”, with no evidence that any of the desired outcomes will be realised. The Assistant Treasurer Stephen Jones, Australian Government, describes their CDR experience as “It’s a good idea, poorly executed”. Much of the execution is prescribed in the Act, similar to the NZ Bill. We need to learn and not just copy, to achieve the success we all want to see.

[CDP’s relationship with other regulations and sectors:](#)

It’s clear that there has been some consideration of identity verification of all entities in the chain in advance of customer consent to authorise sharing, but the Bill’s intent is much less clear in pinpointing that it needs to be designed in and implemented from before the start of any data exchange. Enacting this Bill without the proper data exchange could attract fraudsters and scammers keen to take advantage of new systems that hold personal data, to be used for future nefarious purposes. Any breach of this ecosystem will erode trust immediately.

In the Discussion Paper - Open banking regulations and standards under the Customer and Product Data Bill published by MBIE in August 2024 we note that ‘Officials from the Department of Internal Affairs and the Ministry of Business, Innovation and Employment are working together to ensure alignment between the DISTF and the Bill to fully realise the benefits of both initiatives and minimise compliance costs for system participants’. While this is laudable and welcomed, it must be appreciated that the DISTF has only just come into force (1 July 2024) with the rules still being worked through by the Department of Internal Affairs.



While we all hope for the best outcome and the DISTF is widely adopted, it's too early to estimate adoption. There's no question that on the face of it, the principles can be aligned, but it's less clear that DISTF's full suite of standards can be adopted uniformly in every sector. The first designated sector is banking and it's easy to see how the CPD Bill augments open banking use cases in that sub sector of banking. However, the established international standards, protocols and code libraries for open banking that enable cross border interoperability in that sector are not identical to the standards suite underpinning the DISTF, even if the essential parts needed for conformance and interoperability were capable of being mapped. If it came to pass that PaymentsNZ's API suite used those open banking standards, protocols and code libraries for its identification, verification authorisation and consent, and in turn banks used those for their open banking deployments rather than the DISTF standards suite then the future take up of CDP in that sub-sector might be impacted.

For a good supply of third-party data requestors, the regulations that support this legislation (and DISTF) will need to be internationally interoperable (i.e. use international standards for information sharing). Without this, New Zealand providers will develop solutions that cannot interoperate and be sold overseas. This legislation potentially drives IT related spending, so it could be good for those DINZ members who develop software and services in the digital identity ecosystem to serve this demand. Furthermore, an international-standards and interoperable regulatory system will mean off-the-shelf solutions can be offered in the New Zealand market, supporting a more innovative and cost-effective ecosystem whereby New Zealand customers benefit from a competitive range of solutions. This was another lesson learned from the Australia's CDR.



Precautionary Notes:

- The few references to identity that there are, imply a traditional mindset to the data sharing and exchange. As drafted the Bill does not seem to envisage nor accommodate technical advances such as decentralised Identity, verifiable credentials, or alternative trust frameworks, nor the 'state of the art' of sector-based data sharing and exchange. These can potentially help dramatically reduce costs and avoid many of the issues encountered in Australia.
- There are existing data sharing initiatives (examples can be found in Appendix B) that address the concerns raised. There are innovations and novel business models being pursued today that may not be compatible with the prescriptive structure this Bill requires. What happens to these?
- Is this doubling up on activity already underway that other regulators are overseeing? For highly regulated markets like banking, initiatives such as open banking have overlapping goals as already mentioned earlier making the compliance and accreditation burden simply too high for entities' risk vs return decisions.
- Also as mentioned earlier, there are existing Trust Frameworks that have data sharing components in them, such as (but not exclusively) the Digital Identity Services Trust Framework Act 2023 and more to come such as the expected regime around open banking – and this is before considering international organisations operating in New Zealand that may have been accredited under another regime offshore. That only the Privacy Act 2020 is referred to in the Bill is concerning. Acknowledging the burden on those entities attempting to comply with multiple Trust Frameworks here and overseas and taking meaningful steps to align, map, conform, interoperate and mutually recognise to the extent possible is vital. Make the regulatory burden too high and entities simply won't engage and it will fail, just as we have seen in Australia.



- We note that clause 98 of the Bill gives the Minister considerable power to designate new sectors to be a part of the CDR, however it is unclear what justification or threshold is needed to be met to become designated. We recommend this be expanded to take into account a broader range of factors so that the Minister can make a considered and fully-informed decision on designation regulations. And on that theme, we wish to ask if the Select Committee has reviewed data that validates what exactly the general New Zealand customer is seeking in order to inform their purchase decisions in the sectors considered for designation, and the quantification of the potential market? Also, has there been a review on what this will cost participants, how it will be recovered and leveraged? In its absence, each participant will have to undertake this analysis itself, adding cost.
- The Regulatory Impact Statement (RIS) states: “The Panel notes that the detailed costs and benefits of a consumer data right are difficult to assess at this point, however this will be considered further in a second RIS to be produced at a later stage on detailed and second-order design questions.” This cost benefit analysis did not appear in the second RIS. There is a body of research on the Australian costs and benefits available to assist with this. See Appendix C for the links.
- When the UK introduced this, a comprehensive data protection and privacy regime was already in place to provide the guardrails. Australia and NZ are not as well prepared. This has been acknowledged by Australia with hindsight (see Appendix C). The Privacy Act 2020 IPPs offer some broad guardrails and the Bill indicates where compliance will require a departure from them with relevant guidance, but the significant burden expected with managing notice and consent does not appear to be acknowledged. This should be noted and necessitate proceeding with appropriate caution.



Specific Concerns:

- The requirements in Clause 27 places an unnecessary requirement for data holders to build electronic systems to share data with customers or accredited requestors. In some instances, data holders may already have a sufficient electronic system to manage these requests. Furthermore, this assumes that a separate electronic system is required in the first place. This seems directly in contravention to the government policy which continues to offer services through non-digital channels (there are exceptions such as INZ at the border which has legislative underpinning). The clauses relating to electronic systems should be deleted as it is an overreach of the intent of the Bill. Data holders should be able to use their discretion to create their own processes that comply with their obligations under the Bill.
- Clause 33 and Clause 34 relate to derived data that we do not recall being included in the previous Exposure Draft. What is the rationale for their inclusion now? Again, on the face of it, it seems to be an overreach of the legislation that once an accredited requestor has received a customer's permission to access their data from a data holder, that the Act will still apply to customers who want to on-send their now derived data. Surely this is the purview of the Privacy Act 2020? Our understanding is that this was a major issue that impacted successful uptake and acceptable cost for businesses in Australia and offers a case in point in our submission that NZ is not learning Australia's lessons. This and any related references, should be deleted.
- Clause 53 is not necessary because the Privacy Act 2020 covers the requirement and the consequences of breach to any personal information. It's an unhelpful addition that further complicates compliance unnecessarily. It should be deleted.
- There are many reasons to be both concerned and optimistic about the impact of this Bill. This Bill should be robustly debated in the house, given



the industry disruption it will likely cause – even as opt in and not mandatory as in Australia. Without perspectives that point out the obstacles to overcome, NZ is likely to find itself on the same painful “happy path” as Australia has. This is highly consequential legislation that has not seemingly had the level of cost/benefit/risk analysis normally required when assessing regulatory impact. This should be directly addressed.



Appendix A: Supporting Notes

Australian CDR research key points:

- Implementation costs between \$1m to \$100m for data holders. Annual operating costs levelling off at ~\$3000 per customer.
- Data Schemas do not vary greatly from existing access to data customer exported queries and downloadable statements.
- Fintech startups find the prescriptive system constraining.
- Low uptake with high churn and early deceleration. Slowing down rollout to other industries while viable use cases are developed.

Note: References to “Increased Data Sharing” or similar constructs presumes data is an asset that is held by the data holder for the data subject. That is technically inaccurate. Businesses collect and store information about their business activity, which is a data asset that they create, own, and maintain. It contains information about the data subject (customer), but they are not providing a “data holding” service. Consequently, data is shared with customers and 3rd parties when there is value in doing so. The competitive market determines when data sharing is worthwhile. There is substantial data sharing with consumers by data holders. Within legal guardrails and where there is an economically viable use case, data is shared between industry players and competitors.

Appendix B: Examples of data holders sharing their data with consumers or other industry players.

- Financial: Customer Online Services (queries, exports, statements), data feeds to personal accounting services such as Xero, MYOB, and others. Identity and Access Management Permissions for Accountants to access client accounts and information, and more. Open Banking will expand this further. Broking Accounts provide access to raw data as well as data analysis.



- Power: Customers have access to their data through the online portals, this includes usage, billing payments history, etc. Comparison sites for informed choices exist such as PowerSwitch and SwitchMe, Power Compare, Consumer NZ papers, etc.
- Telcos: TM Forum's eTom and SIDs enable global integration of service provision to the individual.
- Health: Konnect provides real time insurance approval of medical expenses, Health 360 provides sharing of prescription, tests, medical history between health providers. Health monitoring devices such as smart bands enable the download of data collected by the user.
- Nearly all providers of products and services offer online registration, account & profile management, and access to customer information directly with the customer. CRM's (Customer Relationship Management) are integrated with e-commerce.

Appendix C: References

Australian CDR Cost review:

<https://treasury.gov.au/sites/default/files/2024-08/p2024-512569-report.pdf>

Accenture research for Australia Banking Association:

https://www.ausbanking.org.au/wp-content/uploads/2024/07/CDR-Strategic-Review_July-2024.pdf