Submission on discussion document: *Unlocking value from our customer data*

Your name and organisation

Name	Josh Daniell
Organisation (if applicable)	Akahu
Contact details	Privacy of natural persons

[Double click on check boxes, then select 'checked' if you wish to select any of the following.]

☐ The Privacy Act 2020 applies to submissions. Please check the box if you do not wish your name or other personal information to be included in any information about submissions that MBIE may publish.

☐ MBIE intends to upload submissions received to MBIE's website at ***www.mbie.govt.nz***. If you do not want your submission to be placed on our website, please check the box and type an explanation below.

I do not want my submission placed on MBIE's website because… [Insert text]

Please check if your submission contains confidential information:

☐ I would like my submission (or identified parts of my submission) to be kept confidential, and **have stated below** my reasons and grounds under the Official Information Act that I believe apply, for consideration by MBIE.

I would like my submission (or identified parts of my submission) to be kept confidential because… [Insert text]

Responses to discussion document questions

How will the draft law interact with protections under the Privacy Act?

1 *Does the proposed approach for the interaction between the draft law and the Privacy Act achieve our objective of relying on Privacy Act protections where possible? Have we disapplied the right parts of the Privacy Act?*

General

We strongly support the approach of relying on the Privacy Act wherever possible. This approach simplifies participation in the CDR regime and will significantly help to drive adoption.

Extending the Privacy Act principles via the CDR regime

In our view, there are two ways in which the Privacy Act principles could be explicitly extended through the bill or regulations:

1. Apply the Privacy Act principles to all CDR data (except product data), instead of limiting their application to "personal information".
2. Apply the Privacy Act principles to all legal persons, instead of limiting their application to "individuals".

These two extensions would represent a significant extension to the Privacy Act boundaries. However in Akahu's experience, organisations that collect sensitive information tend to treat all such information in the same way, rather than siloing personal information and applying a higher standard to that data alone. We're unaware of any operational difficulties that organisations would face if they were required to comply with the suggested extensions.

Privacy Act and ethical standards

Extending the Privacy Act principles as suggested above would also address the issue of whether to apply ethical standards to participants in the CDR regime.

In our view, it's inappropriate to develop ethical standards in parallel with the constraints that are defined in the Privacy Act. The proposed extensions would provide appropriate protections for all relevant CDR data, and would enable a clear and consistent approach to data protection in New Zealand.

Section 35

If the Privacy Act is extended as suggested above, we think that section 35 would be unnecessary because the Privacy Act provides appropriate protection around the collection of data.

Consent settings: respecting and protecting customers' authority over their data

2 *Should there be a maximum duration for customer consent? What conditions should apply?*

Ongoing consent is important

Ongoing customer consent is critical for many use cases. To provide some data from Akahu's operations:

- Akahu has 44 accredited app customers. Of these 44 apps, 37 request ongoing consent from customers in order to deliver relevant functionality in their products.
- Akahu also has 621 customers with "personal apps". These are people or organisations that use Akahu to programmatically interact with their own bank accounts. All of these customers have granted ongoing access to themselves via Akahu API credentials.

Limited duration is sometimes appropriate when requesting consent

The duration of a customer consent should be tailored to the use case. If there is no purpose in collecting data for an extended period of time, then it would be appropriate for the accredited requestor to limit the duration of the consent request. The Privacy Act Principle 1 provides a guardrail on this point. Accredited requestors should be able to define a limited duration of an ongoing consent.

However we rarely see use cases where limited consent duration is apparent at the time of granting consent. The appropriate duration of consent is usually related to use of a product, and a customer usually won't know how long they'll use the product for at the time of granting an ongoing consent.

Using notifications for non-expiring consents

In the absence of a regulatory framework, Akahu developed our own rules around ongoing consents that we enforce with our app customers. These rules evolved over time, and during 2022 we landed on an approach that now gets high satisfaction from both customers and apps.

1. We initially imposed a 12 month maximum duration for ongoing consents. This led to a high dropoff when the consent expired, because a significant portion of customers did not quickly reconnect their accounts following expiry notifications. Customers and apps were both frustrated by this dropoff, and it was difficult for products like accounting software and household budgeting tools to synchronise seamlessly when data feeds were reconnected.
2. Based on customer and app feedback, we no longer impose a maximum duration for ongoing consents. This policy matches the concept of non-expiring consents in scenarios like direct debit and tax agent authorisations. To ensure that customers remain aware of the ongoing consents that they have granted, we send an annual notification to customers regarding their active ongoing consents. The annual notification provides customers with a 1-click option to login to my.akahu.nz, which is our tool to give customers visibility and control of their ongoing consents. We see a very small dropoff (less than 2%) in the month after an annual notification is sent to a customer, implying that the vast majority of customers want to keep their non-expiring consents active.

Non-expiring consents are important for adoption of the CDR regime

We believe that enabling non-expiring consents is important to encourage uptake of the CDR regime. For example, if a merchant such as an energy retailer is comparing direct debits which don't expire, versus a CDR consent that will expire each year, it's hard to imagine that the energy retailer will choose to use the CDR regime for customer payments.

	We believe that the Privacy Act contains the necessary countermeasures to protect customers from over-collection of data via a non-expiring consent, especially if the Privacy Act principles are extended as we suggest in response number 1.
3	*What settings for managing ongoing consent best align with data governance tikanga?*
4	*Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?*
	Accredited requesters should be able to terminate an authorisation under clause 31. For example if a customer switches their tier of subscription with an accredited requester's product, and CDR data is no longer required, the accredited requester should be able to terminate the authorisation. This will allow the accredited requester to align with the Privacy Act Principle 1 around the purpose for collection of information.
5	*How well do the proposed requirements in the draft law and regulations align with data governance tikanga relating to control, consent and accountability?*
6	*What are your views on the proposed obligations on data holders and accredited requestors in relation to consent, control, and accountability? Should any of them be changed? Is there anything missing?*
	Intermediaries We provide comments in relation to intermediaries and consent in response number 11. **Modifying consent** When referring to modification of a consent in section 30(3)(d), we assume that the technical process would involve revoking an existing consent and creating a new consent. If deemed necessary to include consent modification requirements in lower level regulations, those requirements should be limited to: • Duration of an ongoing consent. • Choosing which accounts are connected to an ongoing consent. In our experience, many use cases require "all or nothing" consent. It would be difficult for many accredited requestors to deliver a product that caters to a range of consent scopes, other than varying limits to duration or changes to connected accounts. Similarly, we don't think it's feasible to enable a customer to modify an ongoing consent via a data holder's consent dashboard. It would be very difficult for a data holder to convey the impact of modifying a consent, as the data holder won't have context about the accredited requestor's product. We support the ability to view and revoke consents through a data holder's consent dashboard, but not the ability to modify them. **Communication methods** We think it's important to retain flexibility as to how consent obligations are delivered. For example, it may be beneficial for a data holder or accredited requestor to deliver consent-

	related information via both apps and email. This approach may help customers to avoid consent fatigue, retain more information, and more easily search for details such as consent management and dispute information. We do not see any related issues with the draft bill, so this comment regarding consent flexibility is intended for consideration with lower level regulations.
Care during exchange: standards	
7	*Do you think the procedural requirements for making standards are appropriate? What else should be considered?*
	We note the intent to consider delegating standards development to relevant entities such as industry bodies. We support the adoption of existing work where relevant. For example we support the adoption of the API Centre standards into the CDR regime. However we have concerns about delegating standards development to industry bodies due to potential conflicts. In our experience, industry bodies tend to be biased towards industry incumbents, which will often sit in tension with the customer-centric intent of the CDR regime. This bias is often covert rather than overt, naturally flowing from the weight of participation from incumbents with deep resources. It can show up in subtle ways, such as the level of ambition with standards, or the prioritisation of functionality, or the service levels. If standards development is delegated to industry bodies, we think it should be simple and quick for the regulator to step in and block, modify, or make its own decisions regarding standards. The regulator should also be able to set parameters around any entity with delegated authority, such as ownership, representation, and decision making processes. These controls will protect the ability to develop standards that align with the intent of the CDR regime.
8	*Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?*
9	*From the perspective of other data holding sectors: which elements of the Payments NZ API Centre Standards[1] are suitable for use in other sectors, and which could require significant modification?*
	We think that any other sector will require standards that are significantly different from the API Centre standards.
10	*What risks or issues should the government be aware of, when starting with banking for standard setting? For example, could the high security standards of banking API's create barriers to entry?*
	In the banking sector, most customers have login credentials to online accounts, and many customers have downloaded mobile apps that can be used by data holders to simplify authentication by a data holder.

[1] New Zealand API standards to initiate payments and access bank account information. They are based on the UK's Open Banking Implementation Entity standards but tailored for the New Zealand market. Market demand has driven development and led to the creation of bespoke functionality for New Zealand.

Data holders in other sectors that are considered for designation may not have the same ease of authenticating a customer. For example if DIA (passport-related data) or NZTA (driver licence-related data) or IRD (income, KiwiSaver, and tax-related data) became data holders in a designated sector, the draft bill would currently require those organisations to authenticate customers directly. That is a departure from the current methods of interacting with those organisations as third parties, where the third party obtains customer consent and the data holder trusts their accreditation of the third party instead of directly authenticating the customer.

We recommend modifying the wording in clause 37 so that lower level regulation can enable appropriate authentication requirements for a sector. For example, section 37(2) could be modified to "Before the data holder provides the service, the data holder must verify the identity of the accredited requestor, and must be satisfied that the customer's identity has been verified (either directly by the data holder, or by the accredited requestor)." Then the current wording of section 37(5) enables lower level regulation to contain further requirements for a designated sector.

Trust: accreditation of requestors

11 *Should there be a class of accreditation for intermediaries? If so, what conditions should apply?*

Intermediaries and outsourced providers

Intermediaries typically represent the majority of requests in an open banking ecosystem.

We strongly support the simple accreditation framework, which does not create a special tier for intermediaries. However this could lead to potential issues where an intermediary (as an accredited requestor) is required to carry out all obligations of an accredited requestor, even if certain obligations would be better delivered by a downstream service.

For example, an intermediary should not be required to provide a dashboard to enable customers to manage ongoing consent. If an intermediary could not pass on this obligation to a downstream service, it would have to collect and verify information about each customer so that it can authenticate the customer when granting access to the dashboard. It would also be more intuitive for the customer to manage the ongoing consent with the relevant downstream service where they have the primary relationship.

These potential issues would be resolved if an intermediary is able to satisfy CDR obligations through the existing outsourced provider provisions, which would enable an intermediary to delegate delivery but remain responsible for meeting an obligation. If the outsourced provider provisions already intend to capture these scenarios, then no further action is required.

Other issues relating to intermediaries

There are some technical issues that arise when an intermediary is acting as the accredited requestor for a downstream service. For example:

- An intermediary should be able to refer to a relevant downstream service, instead of the intermediary, when providing details of the consent request to a data holder. That would lead to a more intuitive authorisation screen with the data holder.
- A data holder should show the name of a relevant downstream service, instead of an intermediary, in the data holder's consent management dashboard. That would enable the customer to properly identify and manage each consent.

	These types of issues are best dealt with in lower level regulation, but it's important that there are no blocking provisions in the primary legislation.
12	*Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?*
	We think that the bill should enable insurance requirements to be set in lower level regulation. This will enable any requirement to evolve more rapidly to reflect commercial availability and developments in protectable risks. In our experience, cyber policies contain the most relevant protections against foreseeable risks for our business. We don't see meaningful protection from professional indemnity, theft, or other policies that we have reviewed, however the risks will be different for each accredited requestor.
13	*What accreditation criteria are most important to support the participation of Māori in the regime?*
14	*Do you have any other feedback on accreditation or other requirements on accredited requestors?*
	We strongly support the decision to not create a separate class for intermediaries. We strongly support the simple approach to accreditation tiers. There can be a temptation to create more tiers, but extra tiers only make sense to the extent that there are meaningful differences in the accreditation requirements for each tier. With one-off consent, we think that customers have a reasonable intuition about the trust they're placing in the accredited requestor, regardless of whether the consent relates to data or payments. For example, with one-off data consent for a loan application, or one-off payment consent for an online purchase, the customer can make a relatively straightforward assessment about whether they trust the accredited requestor to carry out the proposed actions. In our experience, there is a meaningful difference in risk between: • One-off consent and ongoing consent: It may be less intuitive for a customer to assess the risks associated with granting ongoing consent. Ongoing consent creates different risks that could be subject to different accreditation requirements. • One-off payment consent and ongoing payment consent: If an ongoing payment consent includes the flexibility to initiate a payment to any destination account, there is an increased risk that could be subject to increased accreditation requirements. As an example of additional controls, Akahu's app accreditation process distinguishes between **application authentication requirements** for enduring payment consents versus other types of consent.
Unlocking value for all	
15	*Please provide feedback on:* • *the potential relationships between the Bill safeguards and tikanga, and Te Tiriti/the Treaty*

	• *the types of use-cases for customer data or action initiation which are of particular interest to iwi/Māori* • *any specific aspirations for use and handling of customer and product data within iwi/hapū/Māori organisations, Te Whata etc, which could benefit from the draft law.*
16	*What are specific use cases which should be designed for, or encouraged for, business (including small businesses)?*
	We strongly support the inclusion of businesses in the CDR regime. We don't consider that specific use cases need to be considered in the draft bill.
17	*What settings in the draft law or regulations should be included to support accessibility and inclusion?*
18	*In what ways could regulated entities and other data-driven product and service providers be supported to be accessible and inclusive?*
Ethical use of data and action initiation	
19	*What are your views on the proposed options for ethical requirements for accreditation? Do you agree about requirements to get express consent for de-identification of designated customer data?*
	As discussed in response number 1, we strongly support the approach to rely on the Privacy Act wherever possible. In our view, there are two ways in which the Privacy Act principles could be explicitly extended through the bill or regulations: 1. Apply the Privacy Act principles to all CDR data (except product data), instead of limiting the application to "personal information". 2. Apply the Privacy Act principles to all legal persons, instead of limiting the application to "individuals". With these extensions, CDR data would have appropriate protection. Separate ethical requirements would be unnecessary and undesirable.
20	*Are there other ways that ethical use of data and action initiation could be guided or required?*
Preliminary provisions	
21	*What is your feedback on the purpose statement?*
	We think that 1(a) should refer to "customer" instead of "individual" so that the scope of that purpose includes all legal persons.

22	*Do you agree with the territorial application? If not, what would you change and why?*
Regulated data services	
23	*Do you think it is appropriate that the draft law does not allow a data holder to decline a valid request?*
	It's appropriate for data holders to have the ability to exercise judgement and decline a valid request if they have reasonable grounds for doing so. For example if a data holder has reasonable grounds to suspect that a valid request is fraudulent, then the data holder should be able to reject that request. It's important that this flexibility is not abused by data holders. So there should be appropriate penalties to deter behaviour that does not align with the intent of the legislation.
24	*How do automated data services currently address considerations for refusing access to data, such as on grounds in sections 49 and 57(b) of the Privacy Act?*
	We support the ability for data holders to apply these considerations for refusing access to CDR requests.
Protections	
25	*Are the proposed record keeping requirements in the draft law well targeted to enabling monitoring and enforcement? Are there more efficient or effective record keeping requirements to this end?*
26	*What are your views on the potential data policy requirements? Is there anything you would add or remove?*
	We strongly encourage reliance on the Privacy Act. We think that customers will benefit from consistency in disclosure, rather than unusual data policy disclosure.
Regulatory and enforcement matters	
27	*Are there any additional information gathering powers that MBIE will require to investigate and prosecute a breach?*
Administrative matters	
28	*Are the matters listed in clause 60 of the draft law the right balance of matters for the Minister to consider before recommending designation?*

29	*What is your feedback on the proposed approach to meeting Te Tiriti o Waitangi/Treaty of Waitangi obligations in relation to decision-making by Ministers and officials?*
30	*What should the closed register for data holders and accredited requestors contain to be of most use to participants?*
31	*Which additional information in the closed register should be machine-readable?*
32	*Is a yearly reporting date of 31 October for the period ending 30 June suitable? What alternative annual reporting period could be more practical?*
33	*Should there be a requirement for data holders to provide real-time reporting on the performance of their CDR APIs? Why or why not?*
	We think that data holder compliance should be externally monitored and reported on. This will deliver better accuracy and accountability.
34	*What is your feedback on the proposal to cap customer redress which could be made available under the regulations, in case of breach?*
	We think that it's appropriate to include a cap.
Complaints and disputes	
35	*In cases where a data holder or requestor is not already required to be member of a dispute resolution scheme, do you agree that disputes between customers and data holders and/or accredited requestors should be dealt with through existing industry dispute resolution schemes, with the Disputes Tribunal as a backstop? Why or why not?*
	We agree that disputes between customers and data holder or accredited requestors should be dealt with as proposed. However a dispute between a data holder and an accredited requestor should be dealt with via MBIE or a relevant entity that is granted delegated authority under the CDR regime.

Other comments

36	**Product data** We question whether the inclusion of product data is: 1. Necessary: In a sector like banking, product data can often be scraped from public data holder websites without the need for customer consent.

2. Desirable: If "compare and switch" services become popular, prescribed product disclosures through the CDR regime could have unintended negative consequences by encouraging product manufacturers to focus solely on the prescribed features instead of innovating holistically.

We think it's useful to retain the ability to include product data in a sector designation, but we think that power should be used carefully.

37

Derived data

The discussion document states an intention to include "derived data, and data derived from derived data".

We think that data a customer has "provided" or "generated' should be in scope, but derived data can be problematic. For example:

- Derived data is more likely to include valuable intellectual property of the data holder. If that data is required to be shared upon customer request, it may lessen the incentive for data holders to generate derived data for customers.
- Derived data is less likely to be consistent across data holders. For example if the result of an loan affordability analysis was included in the scope of CDR data, that output could vary significantly across data holders.

We think it's useful to retain the ability to include derived data in a sector designation, but we think that power should be used carefully.

38

Non-functional requirements

Non-functional requirements, such as API availability, response times, data caching/recency, and throttling, are important for adoption of the CDR regime. These factors have a material impact on the value of the CDR regime for accredited requestors and customers.

If non-functional requirements are not set appropriately and enforced, there is less incentive for participants to migrate from alternative access methods that may offer better performance.

This risk is heightened if standards development is delegated to industry bodies, where there may be an incentive to simplify implementation for data holders to the detriment of accredited requestors and customers. For example the API Centre standards do not contain mandatory requirements regarding caching and throttling. This enables banks to serve old data while still being considered compliant with the standards.

We recommend that non-functional requirements are given careful consideration in lower level regulation.

39

Direct access

We expect that intermediaries will adequately address demand from customers that want direct access. For example Akahu provides "personal apps" free of charge to customers that want programmatic access to their own accounts. We expect to continue providing customers with this type of direct access (provided that the costs of doing so via the CDR regime are not prohibitive).

We think it's useful to retain the ability to include direct access in a sector designation, but we think that power should be used carefully to avoid delaying the rollout of higher priority functionality.

40

Current connectivity methods

There are a number of existing methods for third party services to interface with bank systems in New Zealand, with the most common being screen scraping, reverse engineered integrations, and SFTP file sharing.

The most common applications of these methods are:

- One-off payments: Some merchants enable customers to pay by initiating a bank payment via a third party service. This payment option avoids expensive card fees, and is more inclusive for people who do not have a Visa, Mastercard, or Amex card. Around 2,000 merchants use these services each month including The Warehouse, Spark, Bunnings, Air New Zealand, Auckland Council, and Waka Kotahi.
- Loan applications: All retail banks use some form of bank account connectivity to gather financial information for loan applications. Some banks like Heartland Bank and The Co-operative Bank use these methods directly to enable loan applicants to connect their financial accounts during the application process. Other retail banks use brokers to gather this information on their behalf via intermediaries like Illion, Credit Sense, Equifax, and Akahu.
- Personal finance tools: Companies like AMP, Booster, and PocketSmith have personal finance products that help people to better understand and manage their financial lives. These services use connected financial accounts via intermediaries like Yodlee and Akahu.
- Accounting solutions: Companies like Xero, MYOB, and Solo enable businesses to connect their bank accounts to simplify bookkeeping and accounting. These services use direct bank integrations or intermediaries like Akahu.

We estimate that around two million New Zealand customers have connected a bank account to a third party service over the last two years.

Statement of support for existing connectivity methods

Many organisations in New Zealand are interested in building enhanced functionality that relies on customers connecting their bank accounts.

However some of this innovation is currently being stymied due to lack of clarity as to whether existing connectivity methods, particularly screen scraping and reverse engineered integrations, will be discouraged by regulators.

In Australia, during the development of their CDR regulations, ACCC and ASIC were questioned on this topic during a Senate hearing. **They responded** that they had not seen evidence of consumer harm from the existing methods of screen scraping and reverse engineering, and they did not plan to block or discourage them. That statement gave participants in Australia more confidence to continue innovating while the Australian CDR regime was being developed and phased in.

There are comments to this effect in the discussion document on pages 4 and 23. We think that further public statements reinforcing this position would encourage competition and innovation in New Zealand while our own CDR regime is being developed, resulting in better outcomes for customers. We think that it's reasonable to consider discouragement of existing connectivity methods at a point in time when the CDR regime has demonstrated a viable alternative system.