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

Your name and organisation

Name	Lynne Carroll
Organisation (if applicable)	Perpetual Guardian
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?*
	Yes.
Consent settings: respecting and protecting customers' authority over their data	
2	*Should there be a maximum duration for customer consent? What conditions should apply?*
	Yes, a maximum of 12 months, or earlier if specified by the customer or if the customer closes an account with the data holder.
3	*What settings for managing ongoing consent best align with data governance tikanga?*
	Similar to the United Kingdom's Open Banking system, requiring customers confirm their consent at regular periods.
4	*Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?*
	Yes.
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?*
	The proposed obligations are reasonable.
Care during exchange: standards	
7	*Do you think the procedural requirements for making standards are appropriate? What else should be considered?*
	Our only concern is that it's not explicitly outlined that we would be considered a group that is substantially affected – therefor would we be consulted. I'd like it to say something like affected data holders to make that irrefutable.
8	*Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?*
	Yes

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?*
	Account information standard should be broadly translatable. Payment initiation wouldn't work at all in our view.
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?*
	From our perspective – high security standards in banking APIs are good. ***Our biggest concern is cost to entry will be much higher then in the banking sector. There's limited platform standardisation in the sectors – this will potentially have excessive costs to implement APIs based on usage/demand. Potentially a threshold should be established before market participants are required to implement APIs, with alternative methods for providing data if the volume threshold is not met/forecasted.***
Trust: accreditation of requestors	
11	*Should there be a class of accreditation for intermediaries? If so, what conditions should apply?*
	As long as the customer consent process to allow an accredited requester to share information with an intermediary is clear, then we do not think that intermediaries need to be accredited*.*
12	*Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?*
	Yes. Cover should include adequate Professional Indemnity and Statutory Liability insurance; Cyber protection cover. ***The proposal to publish guidance on appropriate insurance would be helpful but guidance doesn't need to be followed and it would also be dependent on insurance companies' willingness to provide cover for this type of event.***
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?*
	There is significant risk in the ability of Requestors to be able to change data. For an informed decision, when a customer's consent is sought each individual use i.e. to access, hold, view, change and use data should be stipulated rather than a blanket consent for all access.

[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.

	Of the suggested criteria for accreditation the demonstration of adequate information protection and security measures is the only preventative/detective control but is also dependent on having quality systems and support that can be adequately demonstrated and on an on-going basis. This may not be the case for SMEs.
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)?*
	Verifying a customer's bank account number i.e. name and number match (anti-fraud measure) ***Potential for customers to share identity and address verification documents with another entity (AML/CFT Act).***
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?*
	The proposed options for ethical requirements appear reasonable to ensure accredited requesters act ethically, transparently and in good faith. ***We agree with the requirements to obtain express consent for de-identification. This will ensure transparency and clarity on how personal information may be used.*** ***Yes - necessary to stop uncontrolled and unnecessary access and breach of privacy. We prefer client consent (assuming we can reach the client).***

20	*Are there other ways that ethical use of data and action initiation could be guided or required?*
	A prescribed checklist of elements that must be met.
Preliminary provisions	
21	*What is your feedback on the purpose statement?*
22	*Do you agree with the territorial application? If not, what would you change and why?*
	We have no comment on the proposed territorial application as it seems appropriate and in line with the Privacy Act 2020, however we note that some legal firms have commented on the use of the 'carrying on business in New Zealand' threshold being problematic, with the Courts having given that phrase different interpretations under different legislation.
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?*
	No; there may be other reasons such as personally sensitive or commercially sensitive where it is not appropriate to disclose this or where the requestor does not have good intentions or will use it for purposes other than which it was collected. Is the dissemination of the requested information safeguarded against wider and unacceptable use e.g. social media, on-selling for marketing or other purposes? ***There are current protections in the Privacy Act that allow an agency to deny providing information to an individual which should be considered i.e. how old should a person be before they can provide express and informed consent?. Also if a data holder has information on file that their customer has lost mental capacity; then ipso facto that customer cannot provide valid consent and a data holder should be able to deny a request.***
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?*
	If sensitive - particularly to other parties in the matter (redaction) or commercially sensitive or the requestor is seeking to use the information in an inappropriate manner e.g. against other parties e.g. disputed estates.
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?*
	Five years is in line with other legislation but the retention will require storage of this data which will incur further compliance costs. One option is for businesses to log the requests and information with a regulator such as PC but this would be another layer of bureaucracy,

	cost and external dissemination of information and security concerns.
26	*What are your views on the potential data policy requirements? Is there anything you would add or remove?*
	Agree - customers should be informed on any further use of their information in addition to existing Privacy rights.
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?*
	Whether there any restrictions to the types or access of information.
31	*Which additional information in the closed register should be machine-readable?*
	Only thing we can think of would be what aspects of data response is available – i.e. similar to how Open Banking APIs are in various states of availability, this would allow programmatically to know what can be queried for.
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?*
	Yes but as other legislation requires this reporting period this would be a busy time for compliance reporting.
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?*
	Where the threshold is met, yes – real time reporting should be in place for internal metrics anyway… still come back to there needing to be a threshold however for businesses to need to meet the standard. ***Not a requirement but an option if this is easier than an annual collation of data.***

34	*What is your feedback on the proposal to cap customer redress which could be made available under the regulations, in case of breach?*
	This provides jurisdictional parameters.
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?*
	Yes

Other comments