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

Your name and organisation

Name	Richard Atkinson
Organisation (if applicable)	Illion
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?*
	Illion supports that oversight is fully owned by a single regulatory body - as distribution of responsibilities can cause a number of difficulties and potentially inconsistencies. It is useful to have clear provisions that set out how the Bill is intended to operate alongside other legislation such as the Privacy Act and its related Codes. *We consider that strong and clear specifics be included in the Regulations intended to supplement the Bill, to ensure that the benefits of CDR are achieved through investment in systems with a level of certainty that does not rely on variable policy positions that might change over time in relation to the Privacy Act and its Codes. An example of this is clarity between transaction based affordability assessment tools and information which may be developed through use of CDR, and traditional 'credit information' under the Credit Reporting Privacy Code, to enable certainty for innovation in product offerings.*
Consent settings: respecting and protecting customers' authority over their data	
2	*Should there be a maximum duration for customer consent? What conditions should apply?*
	Where a data recipient has an ongoing relationship with a person, it should be assumed that data sharing permissions continue to apply. *How you determine that a relationship has ended can be complex, and although Australia places onus on the Data Requestor to remind consumers of ongoing access, this invokes a need for the Data Requestor to also provide a management dashboard where consent may be revoked, independent of the termination of the ongoing service being provided by the data recipient to the consumer.* *We recommend that consumer control should centre around the consumer's relationship with their Data Holder, which offers the appropriate environment to manage data disclosure arrangements. Periodic reminders issued by the Data Holder may also be appropriate.* *If a service provided by a data recipient is cancelled then it should be a given that there will be no ongoing data capture by that service.*
3	*What settings for managing ongoing consent best align with data governance tikanga?*
	Data requestors adherence to their duty of care may be best enforced through obligations to follow ethical principles such as Manaakitunga. As mentioned above, there should be a clear need for data retrieval, justified by an ongoing provision of services to a person who gave original consent.
4	*Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?*
	We suggest that when a customer closes an account with an accredited requestor, associated consents would also be terminated automatically. *In the case where the end recipient of the customers data is not an accredited recipient, the accredited recipient operating as an intermediary would have no justifiable need for ongoing*

	retrieval of the customers data. Reminders of formal consent termination may also be issued by the data holder.
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?*
	We are pleased to see that overly prescriptive obligations have been avoided. Flexibility will be a key driver of take-up, but adequate logging around the provision of consent and the collection and use of data will be necessary to ensure proper accountability.
Care during exchange: standards	
7	*Do you think the procedural requirements for making standards are appropriate? What else should be considered?*
	In addition to the parties referenced in paragraph 80, we feel it would be appropriate to consult with accredited requestors, as the Data Standards Body does in Australia through issuance of Decision Proposals.
8	*Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?*
	illion are in agreement that the CDR legislation should look to leverage existing Privacy legislation rather than replace it, or create an additional layer of legislation specifically for CDR. *However, we note that existing privacy legislation may not fully consider the rules around use of CDR data in conjunction with other data sets that are legislated under the Privacy Act (for example Consumer Bureau data under the Credit Reporting Privacy Code). Where there is an absence of clarity in existing Privacy legislation around the storage and use of CDR data we would ask that specific clarification is provided.*
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?*
	Having been built with a payments focus, existing API's do not provide placeholders for product related information. However, we note that sectoral expansion in Australia required changes to account for the nature of the industry's unique data which would facilitate meaningful insight and support product decisioning. In all cases thus far, additional schemas / components have been required to support rollouts. It may be worthwhile to consolidate certain consumer information into 'common' API's as was attempted in Australia, but we do not feel it prudent to try and pre-empt the needs of future expansion at this time.

[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.

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 illion's experience implementing banking API's, we found that API integration was by no means one of the larger friction points nor was it overly onerous. Investment in infrastructure which ensures robust and secure API's is a necessity and does not need to be particularly complicated to achieve the intended outcomes. *Concerns have been raised around barriers to entry which might stifle innovation. We feel these ill-considered, given the open access provisioned for by allowing unaccredited parties to work with other accredited requestors.*
Trust: accreditation of requestors	
11	*Should there be a class of accreditation for intermediaries? If so, what conditions should apply?*
	We see no need for additional accreditation models for intermediaries. *In Australia, the obligations associated with inter-organisation data sharing invoke complications which can be simplified by various forms of intermediary arrangements. The models which enable much functioning of intermediaries in Australia also focus on facilitating participation by removing accreditation barriers for those looking to partner. Under the current proposals, we don't observe either of these issues as requiring addressing. We wish to ensure however that white labelling under various partnership models is permissible.* *This will be important as we anticipate non-accredited data access through cooperation with accredited parties will be the best-suited path for some organisations and professional individuals. Many who refer consumers to use data capture services wish to maintain their brand image while recommending the intermediary's service. We believe 'co-branding' should be possible without implying the initiating party is the provider of the service through the use of clear disclosures.*
12	*Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?*
	The discussion document has emphasised a desire to empower a person to seek redress as appropriate. We consider insurance pertinent to elevate the chance of satisfactory outcomes. Prescriptive requirements would prove difficult due to the capacities of organisations to both obtain and pay for cover. The Australian insurance guidelines suggested parameters to define "adequate" cover, which was then attested to by participants. We feel this reasonable and do not oppose entity specific measures based on exposure and use.
13	*What accreditation criteria are most important to support the participation of Māori in the regime?*
	Illion believes the concept of free and ready access to data offers a powerful opportunity for Māori to gain mana as they receive information, knowledge and access to services which improve opportunity.

	Transparent and ethical use of data therefore becomes a necessary assurance for holistic success and appropriate governance should offer a state of noa.
14	*Do you have any other feedback on accreditation or other requirements on accredited requestors?*
	-
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)?*
	The most common use cases in Australia are: • *Validating an account prior to depositing of funds (during Point of Sale system setup or distribution of loan credits).* • *Ongoing monitoring of transactions to facilitate revolving lines of credit or dynamic repayments based on takings.*
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?*
	illion supports Option 1, and considers that Option 2 is introducing complexity we feel is beyond scope. De-identified data which is appropriately managed should be considered low risk. In many scenarios, use of data is a necessity to accommodate and improve on service provision. Rules which satisfactorily ensure proper de-identification and transparency for the consumer are supported but we wish to avoid additional 'opt-in' decisions for consumers where a degree of trust should be had for a government regulated regime.

20	*Are there other ways that ethical use of data and action initiation could be guided or required?*
	We are strongly supportive of any guiding principles which encourage the ethical use of data. We would support a guide, but also recognise that building principles into a licence regime is difficult. We encourage accountability for best endeavours to adhere to such a guide but would caution against "adherence to the guide" being a licence requirement as principles are by their nature not always interpreted consistently.
Preliminary provisions	
21	*What is your feedback on the purpose statement?*
	We believe the purpose statement captures both the immediate and ongoing needs as well as the right focus areas for execution. *The Strategic Assessment of the Consumer Data Right in Australia encouraged focused prioritisation to 'support ...user journeys rather than simple switching use cases' (Treasury 2022)[2]. We feel this is most evident by today's usage of alternative bank data access technologies. We therefore encourage that switching and product comparison not become the key focus derived from 'the Purpose'.*
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?*
	There are cases in the Consumer Bureau area where requests are declined, for example where a consumer has placed a credit ban on their file due to concerns around identity theft. So there may be conditions where a data holder has been informed of possible identity theft, or scenarios related to abuse and hardship that would represent reasonable situations for access to be declined or to take additional steps to validate to protect the customer.
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?*
	There will always be circumstances which make service provision difficult, whether due to systematic or ad-hoc failures. To minimise this risk, adequate guidance should be given during the customer journey, to enable the customer to request investigation by service providers so that the cause of the issue can be understood and rectified if necessary.
Protections	

[2] The Australian Government the Treasury 2022, *Consumer Data Right Strategic Assessment: Outcomes*, viewed 6 July 2023, Treasury, <https://treasury.gov.au/sites/default/files/2022-01/p2022-242997-outcomes-report_0.pdf>.

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?*
	We strongly support the need for record keeping and feel associated costs should be immaterial.
26	*What are your views on the potential data policy requirements? Is there anything you would add or remove?*
	-
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?*
	Known data supply issues.
31	*Which additional information in the closed register should be machine-readable?*
	A feed of known data supply issues, their impact and expected resolution times would allow participants to provide meaningful guidance to consumers who encounter errors and automatically trigger backup processes.
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, it is suitable.
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?*
	Yes. When technology fails it is the customer facing service which takes the blame. Poor uptime in Australia has caused much doubt in the ecosystem itself as opposed to the banks which are responsible for fuelling it. What is measured can be reported on and improved.

34	*What is your feedback on the proposal to cap customer redress which could be made available under the regulations, in case of breach?*
	-
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?*
	External dispute resolution is a valid consumer protection heavily relied on in Australia. We see no reason a person should be denied access in New Zealand. *We note that technological evolutions have ensued challenges in dispute resolution as it is often difficult to identify the 'responsible party'. Additionally mediators may have insufficient technical background, knowledge and understanding, and this can lead to disproportional responsibilities on smaller participants which bear the burden of resolution.*

Other comments

illion wishes to congratulate the individuals and organisations which have voluntarily invested time and resources to play a part in bringing Open Banking to New Zealand. We commend the MBIE for the clear and reasonable directives which have been developed thus far. The collaboration between Government and Industry to date has been exemplary.

We wish to draw attention to our support for the directive to address alternative technologies which are currently in use through other mediums. We caution against hastened, preventative measures and encourage focus on a successful implementation which will inevitably deprecate the need for inferior technologies which are less stable and capital intensive to maintain. It should be recognised also that there may continue to be an ongoing need where viable alternatives don't exist for other sectors or non-designated institutions.

We again emphasise the role of intermediaries to facilitate non-accredited data access and draw attention to scenario's where a consumer may not have a primary relationship with the accredited requestor. We feel this is an important consideration also when considering consent management requirements.

Finally, we note the Bill calls for authentication of identity and confirmation of authorisation prior to any action performed under the rules. These authentications and authorisations are user experience components which will be critical to the uptake and the success of the overall ecosystem, so we encourage strong consultation during the rule making stage so that these do not of themselves become roadblocks to uptake.