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

Your name and organisation

Name	Lisa Novier
Organisation (if applicable)	Envestnet | Yodlee
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, the proposed approach disapplies the appropriate parts of the Privacy Act.
Consent settings: respecting and protecting customers' authority over their data	
2	*Should there be a maximum duration for customer consent? What conditions should apply?*
	Yodlee's experience in other markets demonstrate that setting an arbitrary maximum duration limit for consent and inserting a mandatory periodic reauthorisation artificially creates customer friction and lowers customers' engagement with products, tools, and services that can meaningfully improve their financial wellbeing. The United Kingdom's open banking framework initially called for mandatory 90-day reauthorisation events. While this requirement was well intentioned, it failed to recognise that many customers had enrolled in a variety of product use cases, which in practice resulted in customers being forced to authorise with at least one of their third-party tools much more frequently than once every three months. Faced with frequent mandated reauthorisation events, a significant portion of open banking customers in the U.K. abandoned the use cases for which they had signed up, undermining the very purpose of the U.K.'s open banking regime. Regulators in the U.K. ultimately abandoned this requirement in favour of a more streamlined approach to limits on consent duration and customer reauthentication. The resulting consent management framework under the U.K.'s open banking system, which required regulatory amendments, were slow and not implemented until 2022, four years after the original regulation was implemented. Since those changes were implemented customer retention for open banking use cases has been materially higher. In the European Union, PSD2 required a mandatory reauthorisation every 90 days resulting in the same customer friction and drop-off issues mentioned above for the UK. Ultimately, the EU commission decided to revise the 90-day requirement in favour of a 180-day reauthorisation mandate, which did not completely resolve the issue but rather just pushed the problem 90 days in the future. In Australia, the maximum allowable duration of consent was originally 365 days. However, the upcoming amendment v5, is proposing an increase to seven years for business accounts due to the same customer friction issues experienced in other markets with mandatory reauthorisation events. Yodlee understands – and agrees with – the rationale underpinning a proposed mandatory reauthorisation requirement: ensuring that customers have full transparency into and control over how their data is being accessed and for what purpose. In practice, however, Yodlee offers that the MBIE would achieve a comparable outcome, or potentially more transparent outcome, by requiring data holders to provide customers with access to consent management dashboards and periodic notifications to review authorisations. Consent dashboards provide customers with a real-time holistic view of which third parties they have authorised to access their data and offer the opportunity to revoke data access in real time versus waiting for consent to expire. In a consent dashboard environment, customers are fully aware of who has access to their data and for what purpose, enabling full end user control. Required periodic notifications remind customers that they have active

	authorisations and can elicit action outside the data sharing workflow, reducing friction and encouraging uptake. Yodlee would also propose the MBIE consider the difference between the duration of data sharing consent and the duration for which data needs to be used and retained. For example, in a lending use case, the customer may only have to provide a one-time consent to access the data however, the data recipient may need to retain the data for a longer period to meet other lending regulatory obligations.
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?*
	As discussed in Yodlee's response to question #2, we recommend that data provider-enabled customer consent management dashboards be incorporated into MBIE's framework, as they would enable end users to revoke their authorisation at any time. Any specific requirements for ending authorisation (i.e., maximum period of authorisation and other events that may trigger authorisation ending) should, in our view, be incorporated into standards setting to provide the appropriate amount of flexibility to adjust to customer expectations and needs. Managing authorisation requirements through the standards would also ensure that the customer experience is centric to decisions and would reduce the risk of unnecessary re-consents to align with provisions of law. For example, we have seen instances where customers need to re-consent when one data holder acquires another data holder or one data recipient acquires another. When open banking was first implemented in the UK there was no requirement for consent management, however when reviewing the 90-day reauthentication requirement the FCA opted to mandate all data-providers introduce customer consent management. Since that introduction, consumers are more informed about who is accessing their account data and have the ability to easily revoke consent. This has increased trust in open banking.
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?*
	In Part 3 Section 34, the proposed obligations require data holders and accredited requestors: "(a) must have systems in place to enable the customer to view or end the authorisation; and (b) must ensure that those systems meet the requirements provided for by the regulations and standards (if any)". Yodlee would propose that the obligation to provide consent dashboards should be on the data holder. From a practical perspective, this approach enables the customer to view all authorisations for their data holder accounts in a single place versus having to log into each data recipient application to view consent across multiple applications. Data holder

	dashboards provide better transparency to the customer as to who is the downstream holder of the data. Moreover, and as we discuss below, some data recipient intermediaries may not have direct relationships with end users. The specific dashboard requirements (i.e., what data needs to be present and how authorisation is presented for viewing and revocation of consent) should be managed in the standards. It is important to note that some data intermediaries do not have a direct relationship with the end customer. An obligation for intermediaries, as accredited data recipients, to provide authorisation dashboards would require those intermediaries to fundamentally change their business models and create login capabilities to end customers, leading to collection and storage of personal data that would not otherwise be necessary, undermining data minimisation frameworks that were purposefully developed to protect customer data.
Care during exchange: standards	
7	*Do you think the procedural requirements for making standards are appropriate? What else should be considered?*
	In some instances, critical updates to the standards will require immediate action. Based on our experience in other markets, this situation most often occurs with urgent security requests for change to mitigate risks to personal data and/or when there is a request for a break fix. Yodlee suggests that a process be created to enable a shortcut to approve critical, time sensitive requests for changes to the standards when necessary.
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?*
	Payments NZ API Centre Standard also include other financial services use cases including investments data and non-bank lending data that would be suitable for use in other sectors and are closely related to banking use cases.
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?*
	The high security standards of banking APIs could potentially create barriers to entry for smaller FinTechs that may be positioned to bring innovative solutions to market that can improve customers' financial wellbeing. Flexibility in the standards to incorporate a risk-based approach to required controls based on the size of the entity and number of customers is critical. This will allow the smaller entities to meet expectations for entry while also setting expectations for additional controls as the organization grows and adds additional customers. Based on Yodlee's experience in the Australian market, meeting the security standards has been a significant lift for some of our Consumer Data Right Representative clients, often delaying time to market and adding additional expense. In order to obtain entry in Australia,

[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.

	all participants must meet all requirements up front, even to perform a pilot with a client. Greater participation can be encouraged if smaller data recipients were given a risk-based approach to security standards. Accordingly, Yodlee proposes a risk-based approach permitting smaller participants to comply with a minimum set of security requirements to enable innovation and market entry in New Zealand, alongside a clear timeline to meet the higher, bank-level security standards based on factors including the growth in size of the company and volume of users. Yodlee would respectfully offer that the Bank of Canada has achieved what we consider to be an appropriate, risk-based balance for supervisory expectations under its implementation of Canada's Retail Payments Activities Act. In addition, MBIE should carefully consider how regulation may impact standard setting and the practical implementation of law. Regulation is important to protect customer interest, but it is as important to balance protection with customer experience to encourage adoption. Below are a few examples of how regulation can have unintended impacts with respect to customer control and experience. Example 1: Australia regulations require consent revocation to be sent from data recipients to data holders and data holders to data recipients. The technical standards mirror this requirement resulting in neither party "mastering" the consent and leading to synchronization issues. Additionally, Australia regulations require that revoked Data Holder access drives a hard deletion of CDR data at the Data Recipient. This requirement has been a major prohibitor to adoption for many Data Recipients, especially those who support Small to Medium business and Business Accounting use cases. Many Data Recipients are required to retain data for legal purposes, which has forced retention of screen scraping credential-based access. The consumer has a relationship with the Data Holder and the Data Recipient. As stated earlier, we believe consent revocation at the Data Holder should not drive an automatic data removal event at the Data Recipient. Rather, the consumer should have the ability to manage data retention with their data at the Data Recipient. Example 2: The recordkeeping requirements in the Australia CDR require data holders to make synchronous event logs, resulting in API and consent screen performance issues. Example 3: The Australia regulations include statements about inclusion/exclusion of certain fields, customers, and products (e.g., exclusion of date of birth). The standards need to accommodate a very wide set of products across the economy and these inclusions/exclusions has led to compromises in the specificity and usability of standards. A better outcome would have been pushing data element and product/scope requirements to be defined in the standards, rather than the regulations, allowing for flexibility in design to meet the needs of each specific use case. Example 4: The Australia regulation on unbundling of consents and scope of hat must be included in consents impacts user experience with information overload presented to the customer and multiple customer actions required. Defining the requirement for consent in the law and pushing the design of consent management to the standards enables a better customer experience, less friction, and encourage uptake.
Trust: accreditation of requestors	
11	*Should there be a class of accreditation for intermediaries? If so, what conditions should apply?*
	Yodlee is encouraged by the model set forth by the MBIE, which recognises that data intermediaries are partners to either or both the data holder and/or the data recipient and thus does not require a class of accreditation for intermediaries but rather relies on the existing Privacy Act to protect the downstream use of customer personal data.

	In contrast both the Australia and the U.K., the CDR representative and agency models respectively have created added layers of bureaucracy and expense for both intermediaries and their clients, leading to increased costs for participation. Additionally, these models' requirements create additional liabilities for intermediaries to manage the risk of their clients rather than each client being held accountable for the safety and security of the personal data they collect through existing legislation. Given the robustness of the consent, data security, and data privacy requirements in each of these markets for data holders, data recipients, and their partners, it is not clear that end users see any additional protection from having the additional accreditation models set forth under either the representative or agency models for intermediaries.
12	*Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?*
	Accredited requestors should at a minimum hold cyber insurance commensurate to the risk a breach at that entity could create. Cyber insurance can provide assurance that the accredited requestor is properly managing this risk and is able make a customer whole in the event of unauthorized access or disclosure of customer data. It is critically important, however, that any such insurance requirements be risk tailored. Yodlee suggests the MBIE carefully consider both insurance and security requirements as discussed in response #10. Having a risk-based approach that permits smaller entities to have a tiered approach to meeting insurance and security requirements based on factors such as size and number of customers could make market entry easier for startups and encourage innovation.
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?*
	It is critically important that the MBIE develop an accreditation process that is as streamlined as possible to enable government to process applications efficiently and not create bottlenecks in adoption. In the UK, the accreditation process can take upwards of one year which has caused delays in adoption.
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)?
	As small business use cases have high value, Yodlee would like to highlight the importance of low-friction data sharing for small businesses. Business accounting is by far one of the most important use cases the system should be designed to enable. Small businesses need access to their accounting data in the applications they use to manage their business. Facilitating business lending should also be encouraged as it promotes innovation and more competitive and affordable options for business to grow through lending. Australia requires a nomination process to give nominated business representatives authority to act on behalf of the company. In practice, this has resulted in the use of a paper form by banks that requires manual handling by both the business and the banks. Yodlee would suggest that the rights to request to view data and initiate action related to the data be the same as the rights an individual has with respect to the existing data holder accounts. Introducing a separate process to validate rights already extended to individual at the data holder create undue customer friction and discourages end user uptake.
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?*
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?*
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?*
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?*
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?*
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?*
	The designation of what information should be contained in the closed register should be managed through the standards to be most useful for participants. Manging through the standards will provide the flexibility to modify the information available on the closed register to meet the needs of participants. Importantly, the closed register will be useful if it facilitates the onboarding of accredited recipients and clients of intermediaries, including automating the onboarding process for approved 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?*
	Yes, a yearly reporting date of 31 October for the period ending 30 June 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, there should be a requirement for data holders to provide real-time reporting on the performance of their CDR APIs, for both for performance and consent, to enable transparency into the quality of data holder APIs and drive accountability for performance. To fully enable a positive customer experience, data holders should be held accountable to a set of performance KPIs for APIs and consent processes with consequences for non-compliance with performance targets. In addition, real-time reporting will provide transparency to data recipients on data holder performance and enable an understanding of whether the root cause of issues is a result of data holder performance issues.
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?*

Other comments

Section 23 – Outsourced providers

Yodlee would recommend the definition of outsourced provider to more specific and targeted to entities who have a role in the use of customer data on behalf of the data holder or accredited requestor. The broad nature of proposed definition may unintentionally create a requirement to disclose to the customer all outsourced providers including those managing technology or other services however not specifically handling or managing customer data creating confusion for the customer who may believe all disclosed outsourced providers have access to their data as well as created undue burden on the data holders and accredited recipients. Although documentation provided by the MBIE clarifies the difference between an outsourced provider required to be disclosed under the draft bill and other outsourced services, the definition in the bill is not specific enough to stand on its own without further clarification. Additionally, the difference between when an intermediary may be an outsourced provider and when they are a participant in their own right is not clearly defined in the draft bill. Yodlee would like to request that the draft bill be more explicit to avoid future confusion once enacted into law.