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

Your name and organisation

Name	Jo Spencer
Organisation (if applicable)	Sezoo
Contact details	Sezoo Pty Ltd Level 8, 460 Collins Street, Melbourne, 3000 Victoria Australia

[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.

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.

Responses to discussion document questions

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

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?

The Privacy Act has been identified as a critical consideration for the development of a data sharing ecosystem and the systems that are to be created, operational and governed under the draft law.

However, the privacy implications of the sharing of data to the primary (accredited) data recipient require additional consideration of:

- the purpose for sharing the requested data,
- the appropriate nature of the sharing model and solution,
- the roles of intermediaries and technical service providers,
- the minimisation of data provided (especially personal and sensitive data) and
- the use of technologies that can enhance the privacy of the data involved and the use of the data involved.

A customer-excluded, API-based data sharing model, as proposed and embedded in the draft Bill, provides visibility of customer interactions to the Data Holder. A customer-enabled data sharing model (decentralised, via the sharing of data with the customer and from there to the Accredited Requestor) would not allow correlation of customer activity.

There is an opportunity to improve on the approach taken in Australia and include the ability to identify specific data being shared for specific purposes, rather than relying on the interpretation of large data sets (e.g. bank account transactions for large periods of time) that provide far too much to the Accredited Requestor and imply a complex interaction model (without the customer involved).

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

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

The data sharing model proposed and enshrined by the Bill implies a considerable burden of data sharing consents for both the Customer, the Data Holder, and the Accredited Requestor.

In Australia, rather than enabling choice of service providers to a Customer, the same model as proposed here has resulted in a customer experience that creates a tighter binding of the Customer with their existing service providers (Data Holders) due to the consent management overheads.

The use of a customer-enabled sharing model implies an intrinsic and active sharing consent as part of the interaction. This simplifies the sharing process and the combination of shared data from multiple sources without the need for complex interaction models and consent management solutions.

Of course, the duration and meaning of active and informed consents should be aligned with the privacy implications and the purpose of sharing the data. Each data sharing service (use case) should have an expected re-confirmation by the customer. However, the experience from Australia is that the model proposed in NZ makes this very customer-intensive. The

need to re-authenticate the Customer through their Data Holder was found to be a significant impediment to continued service adoption. The re-confirmation with a Requestor, in this case, would be sensible.

The customer experience must be harmonised so that any coordinated orchestration of sharing data from multiple data sources (Data Holders) should be aligned.

Again, all of these challenges are negated or made much simpler using a customer-enabled data sharing model.

What settings for managing ongoing consent best align with data governance tikanga?

The consideration of the impacts (intended and unintended) of the single proposed approach to consent management to different cultural groups is essential. By creating additional dependencies on existing service providers, which demand additional management by customers through the proposed consent management approach, the customer choice and ability to change service providers becomes increasingly difficult.

Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?

The experience in Australia is untested as there are very few scenarios where consent would be expected to be provided for long periods.

The standardisation of consent timeframes is something that only applied to long-standing regular customer data sharing scenarios. These shouldn't be allowed to exist, unnecessarily. The continued sharing of customer transaction and commercial arrangement information should not become a norm, where the one-off sharing of specific data should suffice in nearly all scenarios.

Providing customers with the ability to define how long consent is applicable may sound like a good idea, but, in practice, this provides the opportunity for inconsistent arrangements, customer confusion and impacts to the services provided.

How well do the proposed requirements in the draft law and regulations align with data governance tikanga relating to control, consent and accountability?

We are unqualified to respond to this question.

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?

As mentioned above, the consent model proposed, resulting from a customer-excluded data sharing model, implies poor customer experience, large overheads on the commercial parties involved and serious limitations on the practical data sharing of data from multiple sources.

The use of shared data for secondary purposes by the Accredited Requestor isn't sufficiently controlled by the data definitions and the trusted nature of the data sharing model.

The design and societal implications on privacy considerations was not included sufficiently in the implementation of these types of solutions in both the UK and Australia. Please don't make the same mistakes as these jurisdictions.

Care during exchange: standards

Do you think the procedural requirements for making standards are appropriate? What else should be considered?

The setting of sector specific services and data requirements should be independent from the operating authority and should be managed by the appropriate domain governance body.

However, the standards for sharing data and the framework for how the services defined at a domain specific level must fit into a consistent governance framework, articulated and governed by the governance and operations authorities.

Definition of APIs is a very limited approach to standards development and does in no way provide standards best practice on data sharing, globally promoted using W3C data models, and various sharing interaction models (ISO18013-5, OIDC4VP etc.).

Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?

The ongoing dependency between the two laws (the bill and the Privacy Act) is clearly articulated. Whether or not the timing and terminologies used in the two laws are aligned will need to be considered.

The correlation of individual activities is also a privacy consideration and may not be adequately covered in the Privacy Act.

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?

The total focus on APIs and the sharing of data sets considered applicable by the Data Holders results in inconsistent customer expectations and the oversharing of data. API definitions are required for action initiation and sharing activities, but the API-centric approach fails to define a holistic customer service. Whilst this focus remains, Data Holders will continue to exert unreasonable commercial control over the customer cohort.

The data sharing models supported should be enhanced to support customer-enabled data sharing solutions which consider the use of verifiable credentials and other data structures.

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?

FAPI standards only enable secure end-point security and peer interactions and do not enable end-to-end authentication and non-repudiation of shared data.

Other standards are being adopted, for example in Europe for eIDAS v2, where API-focused solutions have been shown to be inappropriate for ecosystem evolutions.

Trust: accreditation of requestors

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

[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.

The need for accreditation of requestors and intermediaries must be appropriate to the purpose for which the data is shared, and the risks associated with the use of that data. The financial and societal impacts and implications should be assessed against the service definition. Those services and data requirements that are considered sufficiently risky should require an appropriate level of initial and on-gong accreditation, monitoring and consent.

The introduction of intermediaries makes data sharing ecosystems very complicated and the equivalent solutions in other jurisdictions have not easily accommodated these arrangements. Customers rarely understand the roles of intermediaries and the implications of their services.

Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?

The products and services provided by the accredited requestors should be sufficiently defined, such that the terms and conditions, customer redress/compensation and governance controls are managed by the appropriate regulator. The need for insurance for the data sharing environment would ideally not be required.

The implications of including intermediaries must be considered also by the appropriate product regulator.

The storage of data and the implications of a data breach should be covered by the Privacy Act.

In addition to appropriate insurance for Accredited Requestors, we would welcome consideration that Data Holders should have to set aside a provision (insurance if you will) the size of which is determined by the volume and sensitivity of the data they acquire. This would deter Data Holders from holding unnecessary information from other sources, purely for the purpose of providing services under this regime. This is a different approach to the penalty provisions provided by the Privacy Act (for example).

What accreditation criteria are most important to support the participation of Māori in the regime?

We are unqualified to respond to this question.

Do you have any other feedback on accreditation or other requirements on accredited requestors?

The need for accreditation must be appropriate to the service provided, the societal and financial risk to the customer, any secondary uses of the data and the trust in the ecosystem. For example, sharing product information would not require accreditation, but sharing transactional information would.

The approach to reducing the need for accreditation is to anonymise data as far as possible and not to share customer data unnecessarily.

Unlocking value for all

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.*

We are unqualified to respond to this question.

What are specific use cases which should be designed for, or encouraged for, business (including small businesses)?

Appropriate use cases are those that provide value to the customer and do not intrinsically or additionally lock the customer into a long-term commercial arrangement with a Data Holder.

Any use case that requires an inappropriate amount of base transaction data should be carefully reviewed. The provision of specific data sets, created in addition to existing information by the Data Holder, may be required to ensure appropriate data sharing requirements.

The requirement for a long-term relationship in the provision of customer arrangement data must be clearly articulated and understood by customers.

What settings in the draft law or regulations should be included to support accessibility and inclusion?

The data sharing model proposed implies the use of online solutions. Without equivalent paper-based offerings and the ability to provide equivalent in-person or physically enabled services will exclude and disadvantage significant population groups.

A customer-enabled data sharing model can be applied in physical form, for example using verifiable credentials, such that the digital models and physical models can coexist.

The need for supported scenarios, where a customer requires support from a delegate or guardian, makes the data sharing model proposed extremely difficult. These types of supported demands have been investigated in other jurisdictions and models of supported interactions have been identified.

In what ways could regulated entities and other data-driven product and service providers be supported to be accessible and inclusive?

The nature of the data sharing model proposed makes this a significant challenge. No equivalent data sharing solutions have been able to address this sensitive and critical consideration.

Ethical use of data and action initiation

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 implementation of a technical ecosystem that enables only a section of the society to benefit has ethical considerations that must be addressed. This was evidenced in the OBIE report for June 2022. Sharing data digitally can be done using different models, but aligned physical, digitally enabled physical and purely digital models can be created to ensure the

highest possible reach of the provided services. The ecosystem must allow different models to evolve that ensures the implementation of services to the broadest customer base possible.

The proposed data sharing model (where the customer is excluded) results in unclear service definitions and the over-sharing of data.

A common consent user experience showing exactly what will be shared, for what purpose and for what period must be included in the establishment of the data sharing arrangement.

Are there other ways that ethical use of data and action initiation could be guided or required?

By making it clear what data items will be shared, retaining an audit of sharing arrangements accessible to the customer and consolidating existing arrangements for the customer, it will be easier for the customer to manage their arrangements without undue commercial influence.

Customer initiated and controlled revocation of a data sharing arrangement at the Data Holder or Accredited Requestor must be possible so that any service can be terminated with appropriate customer guidance and support but without undue customer friction.

Preliminary provisions

What is your feedback on the purpose statement?

The alignment of use cases and data use purposes must be defined and understood by the customer at the time of arrangement establishment. This includes whether or not a requestor is accredited or not for the specific data sharing scenario (and data set).

The limitation or deidentification of personal data must be achieved as much as is practical for the primary purpose of the requestor or third-party service. Inclusion of personal data for secondary purposes should not be possible except without expressed permission of the customer at the time of establishing the arrangement.

The data sharing model should enable selective disclosure and zero-knowledge proof solutions such that a minimal amount of data is required to be provided (especially personal data).

International standards, such as ***W3C data model***, support the provision of a purpose in the data sharing process and ecosystem governance framework.

If the shared data is used for secondary sharing scenarios, it should be possible for the provenance of the data to be verifiable and the initial source of the data to be discovered.

Do you agree with the territorial application? If not, what would you change and why?

Whether or not the provider operates in New Zealand or not would appear to be inappropriate. The data sharing arrangement must be for the purpose of sharing data from one service provider to another service provider, where both services are provided for operation in New Zealand and governed by the laws of the land and the regulations of appropriate New Zealand regulators.

Trying to accredit or regulate service providers where the services are to those outside New Zealand and not covered by the New Zealand regulations will be difficult, if not impossible.

Regulated data services

Do you think it is appropriate that the draft law does not allow a data holder to decline a valid request?

This challenge comes about from the data sharing model proposed.

The data sharing model proposed results in service control by the Data Holder and not the Customer. A "valid request" implies that the customer has agreed that the data should be shared. If the Data Holder doesn't trust the customer's request, it would appear to be a strange situation. However, the Data Holder might be able to re-confirm the request with the Customer prior to sharing the requested data.

The simpler approach is to provide the data to the customer and allow them to share it as they see fit. If control is required of the requestors, an accredited list of requesters and allowed data requests would allow the validity of the request (to whom and the data attributes to be shared) to be assessed by the Customer prior to sharing the data.

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?

This is a challenge with the proposed data sharing model and a customer-enabled model wouldn't have this challenge.

Protections

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?

Not only should the Data Holder and the Requestor of customer data retain audit of the sharing process, but a similar record must be available to the Customer. This would ensure that independent assessment of sharing events can be achieved, massively reducing the number of complaints and disputes.

The customer isn't involved in the proposed model and therefore the independent Customer record cannot be achieved. In a Customer-enabled sharing model, the Customer has to specifically and actively consent to the sharing activity and a Customer wallet keeps a independent record.

With the creation of authentic (signed) Customer audit record, the likely behaviour of Requestors and Data Holders will improve. A Customer record would provide non-repudiation of the data sharing process.

What are your views on the potential data policy requirements? Is there anything you would add or remove?

Alignment with the Privacy Act is assumed and a data retention policy for shared data must align with other interactions. The level of sensitivity of shared data must be considered and handled appropriately.

Obviously, a minimal amount of data must be shared (in line with privacy principles). Other jurisdictions have not provided sufficient granularity of transactional data. In sharing unfiltered transaction data, there is a massive potential for Customer profiling and other data analyses in addition to the purpose of the data sharing agreement.

Regulatory and enforcement matters

Are there any additional information gathering powers that MBIE will require to investigate and prosecute a breach?

MBIE capabilities must be aligned with the Privacy Act and the investigation powers aligned with those required to investigate any other breaches.

Administrative matters

Are the matters listed in clause 60 of the draft law the right balance of matters for the Minister to consider before recommending designation?

The Minister should be concerned with the potential for commercial partiality and favouritism.

The sharing ecosystem must promote Customer service migration (between Data Holders), and not lock Customers into retaining Data Holder relationships. Whilst this is intrinsic to the interests of Customers, the concern must be addressed.

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?

We are not qualified to respond to this question.

What should the closed register for data holders and accredited requestors contain to be of most use to participants?

This section fails to concern itself with the features of a "closed register" for Customers. The Customer must be able to assess the Requestor's accreditation for the requested Use Case (identifying the purpose of the sharing arrangement), prior to sharing the requested data.

The proposed register should also provide the maximum list of data items to be requested or shared under the defined use case.

The data should be cryptographically signed (using asymmetric key cryptography of appropriate strength), and the appropriate key management is required.

Which additional information in the closed register should be machine-readable?

All of it.

Is a yearly reporting date of 31 October for the period ending 30 June suitable? What alternative annual reporting period could be more practical?

Yearly is not unusual.

Should there be a requirement for data holders to provide real-time reporting on the performance of their CDR APIs? Why or why not?

Performance requirements of Data Holders in the proposed model are particularly hard to model and allow for technically.

Performance of a Data Holder in the proposed model may result in service denial and poor customer servicing. Performance metrics should be retained by all parties and used as necessary for requestor dispute and complaint management.

	By adopting a Customer-enabled (decentralised) data sharing model the performance overhead on the Data Holder is much easier to model and Data Holder sharing is decoupled from the Customer presentation of data to the Requestor. In this way, performance bottlenecks and single points of failure are removed.
	What is your feedback on the proposal to cap customer redress which could be made available under the regulations, in case of breach?
	Liability of inappropriate access and sharing and the secondary implications of the data use must be considered. The purpose of sharing events must be identified and used for assessment of the Requestor actions. Caps may result in adoption resistance by Data Holders and therefore result in imbalanced Customer service provision.
Complaints and disputes	
	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?
	This would appear to be sensible.

Other comments

Our primary concern is that only one data sharing model has been considered and this model will be locked into the provided law. Experience in Australia and the UK shows us that other data sharing models will become preferrable, and the established national ecosystem must be able to adapt easily to the introduction of these (and multiple) improved technical models. Again, in Australia, the solution design has resulted in the restriction of use cases, complex consent management solutions and requires expensive and restrictive participant overheads (predominantly accreditation overheads). New Zealand Aotearoa has the chance to define the data sharing ecosystem that does not make the same mistakes as these other jurisdictions.

MBIE must not embed technical design choices and definitions in the writing of the supporting law.

Our experience from leading the solution design process of CDR in Australia and the bank implementation within a large bank in Australia has shown us that the data sharing model proposed creates even more dependency on the customer's relationship with their existing service providers (Data Holders). This is contrary to the intention of the initiative, anti-competitive and restricts customer choice.

Our response consistently identifies the challenges with the implied sharing model, which appears to emulate the API-first, Data Holder <-> Requestor (direct connectivity) model used in other jurisdictions and implemented for the payments activities in New Zealand Aotearoa. Whilst this model is understandably useful for action initiation (payments), technical modelling for party identification, cryptographic solutions, interaction patterns, operational supporting systems has evolved since the design of these systems. A newer model, now being adopted across Europe for their identity authentication and credential sharing ecosystem (known as eIDAS v2) looks to the decentralised use of data, held by Customers in suitable digital wallets. This customer-enabled sharing mechanism allows Customers to hold information provided (issued) from multiple sources, and to present selected attributes from these sources. By putting the Customer in the middle of

these interactions, the consent solution is vastly simplified, and the Customer is able to feel in control of sharing only appropriate information with Requestors that they trust. We strongly recommend that the regime must not be limited, technically and legally, to old and restrictive thinking.

The sharing model proposed is service provider business focused, not customer focused. The evolution of Open Banking in the UK has enabled cloud-based accounting solutions, but there are a variety of solutions that are not easily enabled with the sharing mechanism. The inclusion of alternative sharing models is very hard, if not impossible, based on the lack of flexibility in these ecosystems and their legal frameworks. The combined sharing of different data from different Data Holders isn't practical given the complex interaction models in play. The intrinsic consent management model as a result of the proposed data-sharing model demands that customers manage their consents with the ecosystem of each of their existing Data Holders. This results in a significant, complex, and inconsistent customer overhead.

The complexities of similar solutions to that proposed have been shown to result in high levels of disputes and redress, leading to considerable overheads for operators. These disputes are predominantly due to the following reasons:

- No active customer consent at the point of data sharing – a customer-enabled (decentralised) sharing model is far more logical for Customers and active consent is involved in the process. The customer would also be provided with an authentic audit of the sharing activities.
- Inconsistent customer experiences - The customer User Experience (UX) has been left to evolve as the model is implemented. Learnings from the UK and Australia show that standard UX models are critical for ensuring consistent services across Data Holders and Requestors and providing trust by Customers.
- Poor customer authentication experience - the use of in-line Data Holder authentication for the establishment of a data sharing consent is particularly poor and can result in nefarious actors spoofing customers into providing bank access credentials thinking that they are providing them to an approved Data Holder (when they are not).
- Unclear, inconsistent and fractured consent management – The customer has no single source of consents that are active or historical. This drives the customer to rely further on existing Data Holders and results in resentment of the resulting customer lock-in.
- Inconsistent reach - the access to services is dependent on the coordination of services between a (gradually) growing group of participants which will not become easier or cheaper as the network expands. Alignment to standards is assumed, but the migration to new versions of standards is difficult and impacts customer experience.

The lack of a data sharing commercial model is a particularly limiting omission. The incentivisation of Data Holders, Action Initiators and Requestor must be possible and the appropriate exchange of value possible. Also, the visibility of these charges should be made clear to the customer (as in payment services) and the role of intermediaries and service providers must be visible to customers.

The adoption of Open Banking (UK) and Customer Data Right (Australia) services has been poor, and the long-term health of dependent Fintech service providers has been poor. This is predominantly due to the selected data sharing model and the lack of a suitable commercial model. New Zealand Aotearoa has a chance to do better, but from the look of the proposed bill and the proposed data sharing model, it will be the same poor outcome for citizens and businesses.