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

Your name and organisation

Name	Hamish Clareburt, Business Manager
Organisation (if applicable)	Utilities Disputes Limited: Tautohetohe Whaipainga (UDL)
Contact details	Hamish Clareburt 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?

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?

UDL is in broad agreement with the proposed approach and believes it is sensible to rely on established mechanisms under the Privacy Act where appropriate.

We acknowledge the importance of integrating the Privacy Act with the proposed Bill, and an automated system may mean Principal 6 type requests are processed more efficiently. We agree a timeframe that is shorter than the current 20 working days prescribed in the Privacy Act is important, particularly to unlock the intended benefits to consumers, who will require a much shorter timeframe if they are to be compare products in real time.

In the utilities sector improvements in customer access to consumption data has been noted by commentators (see for example Assessment of Electricity Price Review Implementation, recommendation C3 (Allen and Clarke)). The proposed approach will in part respond to such needs. As well as increasing business productivity the Bill has the ability to improve social outcomes for all consumers and particularly consumers experiencing hardship in the utilities sector.

Any automated system will need to be responsive when errors are discovered (see Privacy Principal 7/ clause 38 (2)(b)) and/or when a request may raise issues of vulnerability (see response q. 24 below). There is a risk of a two-tier system developing where a traditional Principal 6 request runs alongside the more efficient automated system.

This access question may in part be addressed by the accredited requestor, but UDL encourages reflection on this point. Such reflection may include the inclusion of clauses in the Bill and/or provision for regulations which set out the types of assistance to be provided to consumers who wish to access the automated approach; and/or a re-evaluation of the place of s 42 of the Privacy Act within the Bill.

There should also be a consistent and responsive pathway for consumers to access redress for any failure to adhere to appropriate standards which does not conflict with the role the Privacy Commissioner plays in enforcing the privacy principles that have been noted.

In terms of privacy, clause 19(3) of the Bill is important. Some legal relationships and/or goods and services may be more suited than others for permission to be given by a single person. However, utilities, can be shared amongst joint account holders. Their interests can diverge, and the information may not be easily attributed to individuals. `

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

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

In our view the length of consent may vary depending on how the information is to be used and the purpose of collection. Some purposes will have an ongoing quality; others may be short term. The maximum duration may differ.

For instance, a price comparison site for energy consumers may only need to retain the consent for a very short period if the customer is seeking a one-off real-time price comparison. Conversely, a customer may engage the same comparison service to actively

monitor the market over a period of time where it would be justified in providing some form of ongoing consent.

The Privacy Act's guidance on collection – lawful purpose, connected to a function or an activity – may be able to be developed to provide some limits (see Principal 1). Procedural safeguards such as those in clauses 31 and 34 will be important. A sunset clause based on losing contact with a consumer or a lack of consumer confirmation after a period could be added to the procedural safeguards.

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

We acknowledge the importance of aligning the approach with data governance tikanga for managing consent, which should include the ability to access a tikanga based method of seeking redress for any failure to adhere to appropriate standards. There are others that are more appropriately qualified to comment on what settings are required.

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

See our comments above in relation to consent. We note consent is called 'authorisation' in the draft law and rely on our comments above in terms of consent and adopting the relevant privacy principles. A mixed approach based on the Privacy Act principles and a fixed deadline for authorisation ending could be considered; the Australian CDR 12-month expiry period appears preferable to the shorter United Kingdom model.

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

As noted above, there are others who are more appropriately placed to comment on this question, but we acknowledge the guidance contained in the Māori Data Governance Model developed by Te Kāhui Raraunga.

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?

Section 30 requires express "authorisation" from the customer to another person - A.

Section 30 (3) requires A to take certain steps to facilitate the customer being reasonably informed and to use a certain method to obtain that authorisation (e.g., an affirmative action).

Customers may need to be protected from "authorising" a third party to act on their behalf without fully understanding the scope of what they are agreeing to. It is important their authority is clear and where possible does not refer to a different document.

As an example, we find customers often do not comprehend and/or read the terms and conditions of their electricity retailers. Accordingly, regulations could set out standards for the wording of an authorisation. It should be in plain English, concise and clear, preferably with clear examples illustrating what is being agreed too.

We are of the view the requirements for third parties to receive informed consent should be stricter depending on the potential consequences of actions being carried out. This may be better included in the specific regulations to be drafted for each business sector.

Care during exchange: standards
Do you think the procedural requirements for making standards are appropriate? What else should be considered?
We have no proposed comments to make on the standards themselves, only that we expect there will be appropriate provisions to ensure they are appropriately monitored and enforced and that consumers have an appropriate channel to redress any potential breach.
Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?
We have no specific comments on how the two interact, however, we repeat our comments above; there should be a consistent and responsive pathway for consumers to access redress for any failure to adhere to appropriate standards which does not conflict with the role the Privacy Commissioner.
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?
N/A
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?
N/A
Trust: accreditation of requestors
Should there be a class of accreditation for intermediaries? If so, what conditions should apply?
We repeat the comments we have made above and expect consumers will be provided with an appropriate channel to redress any potential breach by an accredited intermediary, short of having to rely on another body pursuing a statutory offence conviction. The Electricity Authority Registry Transfer Hub contains an obligation to become a member of a consumer dispute resolution scheme which may be one model to consider.
Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?
Given the scale of potential data held and the role a requestor can provide in terms of holding and accessing data, it would appear prudent and sensible to mandate some level of

[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.

insurance in in the same way some professions do, particularly in terms of facilitating redress to consumers from any breach of an appropriate standard.

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

We repeat our comments above and emphasise the need to co-design with Māori rather than simply consult.

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

N/A

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.*

Consideration should be given to inserting Te Tiriti principles into the purpose statement of the Bill. Such an insertion may better ensure the provisions are interpreted consistently in accordance with Te Tiriti. The administrative provisions addressing Māori concerns and culture may not best achieve this on their own.

This insertion would acknowledge the importance of Te Tiriti for all Aotearoa/ New Zealand. For example, it is typical for any new Government established consumer dispute resolution scheme to be required to incorporate Te Tiriti principles into its operation. This obligation is strengthened by the role played by the dispute resolution sector to the Government Centre of Dispute Resolution (GCDR) and the importance of its *Aotearoa Best Dispute Resolution* Framework self-assessment tool, which includes consistency with Te Tiriti as its first standard.

This approach ensures a process is more likely to conform to Te Tiriti principles and allow consistency in outcomes. It will also reduce any confusion or division between consumer data and how it is handled and treated.

We acknowledge the need to ensure the approach acknowledges the role iwi, hapū and Māori organisations have in acting for the collective benefit of whanau, which is a feature we encounter in our role. We reiterate the importance of co-design and involving the appropriate people to ensure barriers to access are not created.

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

We expect consideration will be given to the regulatory and cost burden any new regime can create. UDL deals with energy companies of varying size and scale.

While standards must be applied consistently, we expect the cost of compliance will be closely considered. In our experience vulnerable consumers will often rely on community-

based organisations, many of which operate as charities with low funding. Care needs to be taken to ensure their role is understood, particularly in facilitating the access needs of consumers, to ensure there are no unintended consequences by the definitions applied in the Bill.

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

As above, in our experience vulnerable consumers will often rely on community-based organisations to provide access to their data, many of which operate as charities with low funding. Care needs to be taken to ensure their role is understood, particularly in facilitating the access needs of consumers, to ensure there are no unintended consequences by the definitions applied in the Bill.

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

We repeat our comments above in relation to the role the GCDR plays in the consumer dispute resolution sector by promoting the principles of Te Tiriti into the sector. Accessibility and user focus are key elements of the GCDR self-assessment tool.

This approach in dispute resolution ensures a process is more likely to promote accessibility and inclusivity. Similar tools and self-assessment guides could be introduced to complement the introduction of the bill and promote accessibility.

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?

N/A

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

N/A

Preliminary provisions

What is your feedback on the purpose statement?

Please refer to our answer to question 15

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

N/A

Regulated data services

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

N/A

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?

UDL supports at this early stage of development, the attempt to integrate the Customer and Product Data Bill with the Privacy Act and particularly the importance of sections 49 and 57 (b) of the Privacy Act.

In the context of utilities, providers attempt to identify consumers experiencing vulnerability and their needs. This may be achieved by the person themselves applying for this status or is disclosed in interactions with the provider. In terms of the proposed Bill consideration of the needs of vulnerable consumers, their identification, and whether automated processes will be sufficient to assess this will likely need further reflection.

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?

N/A

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

We believe the obligation to publish and adhere to such policies is important, both in informing consumers as well as establishing a basis for redress when they are not adhered to. We have seen great benefit from the Electricity Authority's Consumer Care Guidelines and the impact they have had on customer policies maintained by electricity companies. Whilst they are not compulsory, as a consumer dispute resolution provider we can apply them as appropriate industry standards to provide effective redress for consumers.

Regulatory and enforcement matters

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

As stated above, monitoring and enforcement are key parts of ensuring the standards are adhered to and we support the Privacy Commissioner and MBIE being entitled to request records as part of an investigation into a potential breach.

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?

N/A

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?

See our comments above.

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

N/A

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

N/A

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

N/A

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

N/A

What is your feedback on the proposal to cap customer redress which could be made available under the regulations, in case of breach?

It is common to set a cap for redress and it appears appropriate that any amount can be reviewed and adjusted by the Minister of Commerce or Consumer Affairs. This will provide certainty to consumers and those who may be subject to the Bill. We express no comment on the amounts proposed in the discussion document.

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?

As stated above, we believe it is vital consumers have access to an appropriate channel for redress. UDL agrees the preferred method for dispute resolution between customers and data holders should be through the existing industry-disputes resolution schemes. Banking, Energy/Gas and Telecommunications already have existing schemes that consumers can engage with, should they have a dispute they are unable to resolve directly with their providers. We believe complaints that fall outside the jurisdictions of these schemes to be minimal, making the Disputes Tribunal, which does have some accessibility issues, a suitable backstop.

Also as stated above, careful consideration should be given to the role of the Privacy Commissioner and a dispute resolution scheme. The model generated in the discussion documents appears to rely on a clear distinction between the two, however, there may be some overlap where a privacy issue is combined with a consumer issue that may warrant compensation or redress. In our experience, the dispute resolution provider and the Privacy Commissioner should be empowered to agree a memorandum of understanding or process that can allow some form of collaboration to ensure consumers are properly catered for. At

present it appears there has been acknowledgment that MBIE and the Privacy Commissioner's jurisdictions are the only two that overlap, which is not our experience.

Other comments

In an automated system where there are intermediaries such as the accredited requestor and third parties, there may be an issue as to whether the customer is aware of what information is being passed on.

So, while the customer may have made a valid authorisation for specific data, a customer may not always be aware of the significance or scope of the information which has been authorised. The likelihood of this is likely to increase with advances in technology. Therefore, an assessment of this risk and the standard of data specification may require further assessment.