22 July 2023

Consumer Data Right Project Team
Commerce, Consumers and Communications
Ministry of Business, Innovation & Employment
PO Box 1473
Wellington 6140
New Zealand

By Email: consumerdataright@mbie.govt.nz

Dear Sir/Madam

Equifax Submission on Discussion Document: Unlocking value from our customer data

1. We are grateful for the opportunity to submit on the Discussion Document: Unlocking value from our customer data. We make this submission further to our submission dated 19 October 2020 on the Discussion Document: Options for establishing a consumer data right in New Zealand.

2. With the limited time available to submit on this discussion document we do not intend to respond to most questions listed below but would like to draw attention to some key issues that we consider should be incorporated into this regime.

3. As previously advised, Equifax is a global information solutions company. We use data, innovative analytics, technology and industry expertise to help consumers 'live their financial best' and to transform knowledge into insights that help lenders and others make better credit decisions.

4. We understand that primarily the proposed Consumer Data Right ("**CDR**") is to benefit consumers be able to access their information safely and easily to facilitate the uptake of innovative products and services. We support this intention but consider that incentives also need to be given to businesses to justify the investment in becoming an accredited requestor, otherwise the ecosystem will not develop as intended, and ultimately consumers will not obtain the potential benefits.

5. We consider there are a couple of key elements needed to obtain both the benefits to consumers and the benefits to businesses. First, is that the system needs to be efficient and not add undue cost to facilitate the benefits. Therefore, regulation should be limited to the minimum necessary to ensure the security of consumers' data, especially considering the CDR regime is limited to 'read only' rights at this stage. Secondly, any new regulation should not exceed the protections already provided by the Privacy Act 2020 ("**Privacy Act**"), which having recently been reviewed, should currently be considered fit for purpose.

6. One area we are concerned that the CDR may attempt to exceed the protections in the Privacy Act, is in relation to deidentified information (see para 143 Discussion Document). Under IPP10 of the Privacy Act agencies may use personal information for purposes other than for which it was collected if it "*(i) is to be used in a form in which the individual concerned is not identified; or (ii) is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned".*

7. We consider that once data is deidentified there is no harm to the individual in it being used in an aggregated form. An example of a use of consumer data that MBIE gave in its presentation to the public on 18 July 2023, was a budgeting app using a consumer's banking information to help consumers with budgeting. However, not only could an individual's data be used to help them, but the aggregated data could be used to create insights at a macro level, for example, analysing trends

that assist or hinder people in meeting their budgeting needs. These insights may also lead to further innovation of services.

8. Our other area of focus, as noted in our earlier submission, is that we support a dedicated implementation and enforcement body that represents all interested parties, as is the approach that has been taken in the UK, with the establishment of the Open Banking Implementation Entity (OBIE), an industry funded body overseen by the Competition and Markets Authority (CMA).

9. We note that Part 4 of the Bill, which contains regulatory and enforcement powers and penalties, is largely not drafted at present. However, the discussion document (para 32) indicates that MBIE will be the implementation body, which if it has a dedicated unit within it for CDR implementation and compliance, we support.

Set out below are the responses (in highlights) to some of your specific questions. We advise our submission does not contain any confidential information.

If you would like to discuss these further please do not hesitate to contact the author on Privacy of natural persons

Yours faithfully

Deborah Malaghan
Head of Legal

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

Your name and organisation

Name	Deborah Malaghan
Organisation (if applicable)	Equifax Information Services and Solutions Limited
Contact details	deborah.malaghan@equifax.com

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?
Consent settings: respecting and protecting customers' authority over their data
Should there be a maximum duration for customer consent? What conditions should apply?
We do not consider a maximum duration is necessary to ensure benefit remains for consumer and business. Re-consenting will result in 'consent fatigue' and lack of benefit to the end consumer. We have subscribers to our credit reporting business, such as banks, who have enduring consents with their customers to access their credit information throughout the term of their credit arrangement. We consider consent should be linked to the term of the services. For ongoing consents, we support a requirement to remind consumers about that consent every 12 months.
What settings for managing ongoing consent best align with data governance tikanga?
Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?
Consent for ongoing data capture should be tied to the specific use case.

How well do the proposed requirements in the draft law and regulations align with data governance tikanga relating to control, consent and accountability?
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?
Care during exchange: standards
Do you think the procedural requirements for making standards are appropriate? What else should be considered?
We agree that the standards should be created by the dedicated implementation body in consultation with relevant stakeholders.
Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?
Yes
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?
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?
Trust: accreditation of requestors
Should there be a class of accreditation for intermediaries? If so, what conditions should apply?
No. The proposed regime of including intermediaries as accredited requestors appears effective. Accredited Requestors can then on-share consented data for specific use cases to

[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.

third parties under Privacy Act rules. This meets existing and planned use cases for CDR data.

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

Yes. Public liability

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

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

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.*

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

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

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

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? [could not type answer below] As mentioned in our cover letter, we consider the CDR regime should not exceed the protections in the Privacy Act, which regulating de-identified information would. The value in the aggregated data would be lost to the detriment of the consumer if obtaining consent for this use is a requirement.

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

Preliminary provisions

What is your feedback on the purpose statement?

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

Regulated data services

Do you think it is appropriate that the draft law does not allow a data holder to decline a valid request? Yes. This provides a strong incentive for businesses to attain accreditation and fulfils the objective of the regime to benefit consumers.

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

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?

What are your views on the potential data policy requirements? Is there anything you would add or remove?
Regulatory and enforcement matters
Are there any additional information gathering powers that MBIE will require to investigate and prosecute a 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?
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?
What should the closed register for data holders and accredited requestors contain to be of most use to participants?
Which additional information in the closed register should be machine-readable?
Is a yearly reporting date of 31 October for the period ending 30 June suitable? What alternative annual reporting period could be more practical?
Should there be a requirement for data holders to provide real-time reporting on the performance of their CDR APIs? Why or why not?
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

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