

Kathryn Wardell
Structural Reform Group
The Treasury
Langton Crescent
PARKES ACT 2600
Via email: data@treasury.gov.au

12 October 2018

Thank you for the opportunity to provide a submission on the draft *Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation and Designation Instrument for Open Banking*.

We appreciate having had the opportunity to discuss those documents with Treasury on 2 October 2018.

Impact of Provisions for further consultation

In our earlier submission, we identified issues relating to:

- Reciprocity under the consumer data right
- Interaction between the credit reporting system and the consumer data right
- The automatic application of the definition of ‘CDR data’ to derived data held by a data holder
- The definition of ‘CDR data’ and how it would apply to matters not within the scope of the consumer data right (e.g. data exchanges outside the CDR regime)
- Third parties exploiting the consumer’s right to data

Subject to our comments in respect of the credit reporting system, we think that the provisions for further consultation address most of these issues. We note that the amended provisions do not appear to address our concerns regard third parties exploiting the consumer’s right to data. In respect to this issue, we note that it may be appropriate to include an ability for the Rules to designate certain words or phrases as protected, so that they cannot be used by non-authorised businesses. This could include the phrases, ‘consumer data right’; ‘accredited person’; ‘accredited data recipient’ and ‘open banking’.

In respect to the concept of reciprocity, we note that to give effect to the examples for ‘equivalent data – designated entity’ and ‘equivalent data – not designated entity’ outlined in *Proposal 3: Reciprocity*, the ACCC will need to review their current position of not making rules regarding reciprocity in the first version of the rules. Our view is that the effective and fair operation of the Consumer Data Right (CDR) requires the ACCC to develop rules creating reciprocity obligations, and our separate submission to the ACCC’s draft framework will include an outline for how this might operate.

Interaction between the credit reporting system and the consumer data right

When assessing an application for credit, the credit provider's ability to successfully undertake a risk and responsible lending assessment is dependent on the availability and accessibility of relevant, accurate, and up-to-date data about the customer. The credit reporting system established under Part IIIA of the Privacy Act provides such data in respect to consumer's existing consumer credit arrangements. The consumer data right – in particular, the Open Banking regime – will provide access to additional data sets in respect of those consumer credit arrangements, together with other data relevant to the risk and responsible lending assessment (e.g. data for income and living expense verification). Importantly, the Open Banking regime will ensure such data is obtained via a secure, reliable and efficient process that represents a significant improvement in current approaches to obtaining similar data (e.g. copies of paper statements, or “screen scraping” internet banking websites that require disclosure of customer internet banking credentials).

On that basis, the CDR/Open Banking regime and the credit reporting system will operate in a complementary way with similar levels of data quality and data security.

Regarding our comments in our earlier submission about the interaction between the credit reporting system and the consumer data right, we note:

- CDR intermediaries being caught by the definition of ‘credit reporting body’ (CRB) – subject to making the actual regulations, this has been addressed through the introduction of a regulation making power to vary the application of Part IIIA.

Recommendation: Treasury should consult on the drafting of the relevant regulation.

- Credit reporting information obtained by a credit provider from a CRB being caught by the definition of ‘CDR data’ and, so, being subject to access under the consumer data rules – the Designation Instrument identifies information “that was observed or provided by the person”. It appears that the reference to “observed” refers to being observed by the data holder when establishing the product. This could mean that the credit reporting information obtained by the credit provider from a CRB would be captured by the Designation Instrument.

Recommendation: That the Designation Instrument be clarified on this point and, if the intent is to generally include information ‘observed by the data holder’, that there be a specific exemption of credit reporting data (for the reasons outlined in our earlier submission).

We note the following additional ways in which the credit reporting system and the consumer data right overlap. Where we consider this to raise problems, we have recommended a solution. Otherwise, we have simply noted the interaction for completeness.

1. Paragraph 5.1 of the Privacy (Credit Reporting) Code 2014 (CR Code) prohibits a credit reporting body from collecting “personal information about an individual’s activities in relation to consumer credit that is not credit information”. To the extent that the data available through the consumer data right involves collecting data in relation to a credit account (which would include certain products offered businesses

such as telcos and utilities) that goes beyond the meaning of ‘credit information’, this appears to limit a CRB’s ability to participate in the consumer data regime.

2. Subject to the above comment, if a credit reporting body collects information under the consumer data rules that meets the definition of ‘credit information’, that information would be subject to the requirements of both the consumer data right regime and Part IIIA.
3. Data that is derived by a credit provider from data obtained under the consumer data rules and through credit reporting system will be both ‘CDR data’ and ‘credit eligibility information’ (referred to below as ‘dual derived data’) – a key example would be a credit score created by the credit provider that utilises both types of data. We note that this will create several overlaps between the provisions of Part IIIA (and the CR Code) and the Privacy Safeguards. These include:
 - Privacy safeguard 5: For completeness, we note that a credit provider that has dual derived data will be required to notify the consumer in accordance with Privacy Safeguard 5 and sections 21B and 21C of the Privacy Act. Based on the matters below, that notification may be confusing to the consumer.
 - Privacy safeguards 6 and 7: These safeguards and the use and disclosure provisions of Part IIIA (and the CR Code) will apply to the dual derived data. Part IIIA prescribes the circumstances and purposes for which credit eligibility data may be used or disclosed – unlike the consumer data right, this regime is generally not based on the consumer’s consent.

The restrictions on use and disclosure under both regimes are, however, subject to uses and disclosures that are “required or authorised by or under an Australian law”¹ On this basis, the dual derived data will be *permitted* to be used and disclosed in the circumstances set out in Part IIIA. Given the careful and restricted design of the Part IIIA use and disclosure regime, we consider this to be appropriate.

However, it will also mean that the dual derived data may be used or disclosed in circumstances not permitted by Part IIIA, subject to satisfying the consumer data rules – most notably, by obtaining the express consent of the consumer. This would permit credit providers to use credit eligibility information (provided it is dual derived data) for marketing purposes – subject to obtaining consumer consent. This is contrary to one of the key principles of Part IIIA.

Recommendation: That the use and disclosure of dual derived data be made subject to the restrictions in Part IIIA – notwithstanding that sub-paragraphs

¹ See: sub-paragraphs 21G(2)(d) and (3)(f) of the Privacy Act for CP’s use or disclosure of ‘credit eligibility information’. We note that both the consumer data right and Part IIIA establish circumstances in which the data ‘must not’ be used, rather than directly authorising the particular uses and disclosures. We suggest that Treasury consider whether the two regimes genuinely ‘authorise’ the relevant uses and disclosures. If the regimes do not ‘authorise’ the relevant uses and disclosures, the restrictions of both regimes will apply – significantly impacting on the ability of a credit provider to use or disclose dual derived data.

21G(2)(d) and (3)(f) of the Privacy Act may permit the use or disclosure based on the consumer data rules.

- Privacy safeguard 8: Part IIIA permits cross-border disclosure of credit eligibility information in certain circumstances. We note that, unlike Privacy safeguards 6 and 7, this safeguard is not qualified by the reference to ‘required or authorised’ under an Australian law.

Recommendation: This safeguard be qualified to permit cross border disclosures where required or authorised by an Australian law (noting our comment in footnote 1 regarding the meaning of ‘authorised by or under an Australian law’).

Further to the above, we note that where Part IIIA permits the disclosure of credit eligibility information to a person without an Australian link, the Act deems the credit provider to be responsible for acts of the recipient that would constitute a breach of the relevant law.

Recommendation: Treasury consider whether the Bill should include a rule making power that would permit the ACCC to deem the disclosing entity responsible for the acts of the overseas recipient (where they would be inconsistent with the consumer data rules) if they are not accredited or do not meet the other conditions specified (if any).

- Privacy safeguard 11: For completeness, if a credit provider (i.e. accredited data recipient) discloses dual derived data in accordance with Part IIIA (as contemplated by s56EI(1)(c)(i)), we understand that this will not be a disclosure ‘required by the consumer data rules’ – as per s56EM(2), such that this Privacy safeguard won’t apply to that disclosure.
- Privacy safeguard 12: The requirements of this safeguard and s21S of the Privacy Act will both apply to dual derived data. While the requirements are broadly the same, we recommend that for simplicity credit providers be subject to one regime only.

Recommendation: Credit providers be exempt from the requirements of Privacy safeguard 12 in respect of dual derived data (on the basis that s21S provides equivalent protection).

Further to the above, to the extent that a credit reporting body obtains CDR data which is ‘credit information’ within the meaning of Part IIIA or creates dual derived data, there will be an inconsistency in the obligations under this Privacy safeguard and the retention periods set out in s20W of the Privacy Act. While the safeguard provides an exemption where the accredited data recipient is ‘required’ by law to retain data, the retention regime under Part IIIA imposes destruction/deidentification requires, rather than a requirement to retain.

The retention periods in Part IIIA have been carefully chosen based on the nature of the data. It seems incongruous to require a credit reporting body to

destroy or de-identify data that was obtained under the consumer data rules, where that data may be more up-to-date than credit information obtained under the framework set out in Part IIIA.

Recommendation: That CRBs be exempted from the requirements of s56EN(2) of the CDR Bill, where it is otherwise subject to retention periods set out in s20W of the Privacy Act.

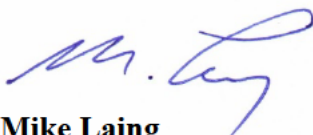
- Privacy safeguard 13: A credit provider which holds dual derived data will be subject to this Privacy safeguard and s21V of the Privacy Act. Part IIIA and the CR Code set out a comprehensive process for the correction of credit eligibility information by credit providers, which is tailored to the nature of the data (e.g. it includes requiring the credit provider to consult with other credit providers or credit reporting bodies as required). It would not be appropriate to then overlay a separate process on top of that.

Recommendation: That credit providers be exempt from the requirements of Privacy safeguard 13 in respect of dual derived data.

4. For the recommendations made in respect of Privacy safeguards 6, 7 and 13, we believe that the changes suggested should be incorporated into the Bill, rather than relying on the ACCC rules making power. This would be consistent with how the interaction between the consumer data right and the APPs is addressed. In addition, the issues raised in respect to those safeguards are not limited to the Open Banking regime and will apply to all sectors that involve 'credit providers' under Part IIIA (such as telcos and utilities).

If you have any questions about this submission, please feel free to contact me on [REDACTED] or at [REDACTED] or Michael Blyth on [REDACTED] or at [REDACTED].

Yours sincerely,



Mike Laing
Executive Chairman