Law Council
OF AUSTRALIA

*Office of the President*

**18 January 2019**

Mr Daniel McAuliffe
Manager
Consumer Data Right Team
Structural Reform Group
The Treasury
Langton Crescent
PARKES ACT 2600

By email: data@treasury.gov.au

Dear Mr McAuliffe

**Consumer Data Right Rules – Draft Privacy Impact Assessment**

1. Thank you for the opportunity to provide comments on the first version of the Privacy Impact Assessment (**the PIA**) for the Consumer Data Right Rules (**the CDR Rules**).

2. The Law Council is grateful for the input of its Privacy Law Committee of the Business Law Section and the Queensland Law Society and in the preparation of this submission.

3. The Law Council's primary concerns, and suggested recommendations, are summarised as follows:

    - Further clarity is required regarding the consent framework. The Law Council recommends legislating for a definition of 'valid consent'. As a minimum, the Law Council recommends enhancing Recommendation 3 of the PIA as outlined in this submission.

    - Many of the mitigation strategies applied in the risk assessment are legal and regulatory measures, leaving the assessment of risk open to the flawed assumption that laws will always be complied with. The risk should be comprehensively evaluated.

    - Clarification is needed as to whether the finding regarding credit reporting agencies is accurately summarised.

    - The Law Council recommends changing 'should' to 'must' in Recommendation 9, to read that 'All significant changes to the CDR legislation or Rules must be accompanied by further PIAs …'.

    - The Law Council remains concerned that the Bill is overly broad and unnecessarily complex. The Law Council recommends the Bill be amended to

*Telephone* +61 2 6246 3788 • *Fax* +61 2 6248 0639 • *Email* mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra • 19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
*www.lawcouncil.asn.au*

narrow the scope and simplify the provisions to improve accessibility of the proposed regime.

**Background**

4. The Law Council notes the first version of the PIA for the CDR is based on the CDR regulatory framework proposed in the Treasury Laws Amendment (Consumer Data Right) Bill 2018 (**the Bill**), which is expected to be introduced into the Federal Parliament early this year. The Law Council provided a submission to the Treasury on 7 September 2018 regarding the Exposure Draft of the Bill.

**The PIA – Consent Framework**

5. Recommendation 3 of the PIA states:

> *The ACCC should continue to work with the OAIC to ensure that the Rules create a consent framework that ensures consent is genuine, and protects vulnerable individuals.*

6. The PIA further states at page 118 that:

> *Risk mitigation strategies rest on the assumption that the Rules will require consumer consent to be voluntarily given, express, informed, specific as to purpose, time limited and easily withdrawn.*

7. The Law Council has previously made submissions about the approach to consent. The Law Council is particularly concerned that, for a regime said to be driven by consent, there is a lack of clarity around what is meant by consent and how consent is to be evidenced. In the Law Council's view, this needs to be rectified for consumers and data holders before the framework is introduced. One measure that could address the lack of clarity, and the associated risks that arise from this, would be to legislate a definition for 'valid consent', which would include these ideas at page 118 of 'voluntarily given, express, informed, specific as to purpose, time limited and easily withdrawn'. Another measure is to provide for a set of minimum prescribed standards and some standard language. The consent issues are particularly complex in industries such as banking or telecommunications where it is not unusual for multiple individuals to have a joint account or share the service and still have different needs and preferences in respect of their data and privacy needs. This is especially sensitive and complex in matters where there is hardship or disputes involving joint account holders or joint users of services or utilities.

8. The Law Council further recommends that Treasury consider a nuanced approach to defining consent (including evidencing such consent), and, to placing time limits on the validity of a consumer's consent. That is, 'time limited' and 'specific as to purpose' should be linked, so that the time period suits the intended use. For example, where consumer data is to be used by a recipient on a one-off basis, a shorter period of time of valid consent should be applied than where consumer data is to be used by a recipient on an ongoing basis.

9. Whilst the Law Council welcomes the requirements that have been mentioned around consent, the Law Council is concerned that there is no mention in the PIA about re-certifying consent where consumer data is to be used by a recipient on an ongoing basis. It is the position of the Law Council that requirements for recertification should also form part of the definition of 'valid consent' or consideration of 'time limited'.

10. As a minimum, the Law Council suggests that Recommendation 3 be refined to include a greater degree of certainty for affected parties, and especially for 'vulnerable individuals'.

**The PIA – Risk Assessment and Mitigation**

11. The Law Council notes that the PIA provides a risk assessment that is low. However, this is based on the assumption that the law will always be complied with. It is the position of the Law Council that this is a flawed assumption.

12. Many of the noted risks and the respective mitigation strategies are almost exclusively focused on legal and regulatory measures. There appears to be very limited focus on Consumer Data Standards or technical measures. Many of the 'risk likelihood following application of mitigation strategies' are rated as 'rare' or 'unlikely' solely on the legal and regulatory matters as noted. For example, Potential Privacy Risks numbered 3.5 to 3.11 inclusively. The Law Council is concerned that the PIA outcomes appear to rely on the assumption that laws are automatically and correctly applied at all times and their passage or mere existence operates as a control in its own right.

13. Accordingly, the Law Council is concerned that the risk does not appear to have been fully or properly evaluated.

14. Further in regard to risk assessment, the PIA states at page 47 that:

> *The risks identified in this section have been assessed according to a modified version of the Treasury's risk rating matrix.*

15. The Law Council notes that this does not appear to follow the format of the risk assessment currently being applied by the OAIC pursuant to section 33C of the *Privacy Act 1988* (Cth) (**Privacy Act**). The Law Council considers that consistency and alignment would be more appropriate.

**The PIA – Credit Reporting**

16. The PIA concludes on page 83 that:

> *the CDR system will not authorise credit reporting agencies to undertake actions that they are otherwise prohibited from doing under the law (e.g. under Part IIIA of the Privacy Act).*

17. However, subsection 56EC(3) of the CDR Bill expressly notes the relationship of the legislation with Part IIIA the Privacy Act, stating that:

> *This Division does not limit Part IIIA (about credit reporting) of the Privacy Act 1988. However, the regulations may declare that in specified circumstances that Part applies in relation to CDR data as if specified provisions of that Part were omitted, modified or varied as specified in the declaration.*

18. The Law Council is concerned that subsection 56EC(3) of the CDR Bill allows certain actions of credit reporting agencies that would normally be prohibited to be performed, and therefore questions the accuracy of the aforementioned PIA conclusion.

**The PIA – Further PIAs**

19. The Law Council notes that Recommendation 9 of the PIA states:

> *All significant changes to the CDR legislation or Rules should be accompanied by further PIAs, conducted in accordance with the OAIC Guide to undertaking privacy impact assessments and following engagement with privacy and consumer representatives.*

20. With regard to significant changes still to occur to the CDR legislation or Rules, the Law Council recommends that the Treasury engage with the Australian Competition and Consumer Commission to postpone the Open Banking commencement date and establish a feasible timeframe to achieve implementation across all Authorised Deposit-taking Institutions simultaneously.

21. It appears therefore that Recommendation 9, whilst perhaps necessary, should be amended to ensure that any significant changes must be accompanied by further PIAs, and that any proposed amendments will be properly consulted before implementation.

**The CDR Bill**

22. While the Treasury is not currently consulting on the CDR Bill or Rules, the Law Council refers to its previous submission, and the concerns expressed that the proposed regime is overly broad and unnecessarily complex. The Law Council recommends the Bill be amended to narrow the scope and simplify the provisions to improve accessibility of the proposed regime.

23. The Law Council would welcome the removal of 'associated with' from the definition in section 56AI. However, the definition remains very broad given the inclusion of data 'wholly or partly derived from the other CDR data …'. Potentially this will create a broad regime based entirely on factual matters as to the particular data flow in question. This will make it difficult to assure transparency and consistency.

24. The Law Council would also welcome the reference to confidentiality as a consideration. However, note that where the confidential information is not '*personal information*' as defined by section 6 of the Privacy Act, the OAIC will need additional jurisdiction to address and administer concerns in respect of non-personal information.[1]

25. In addition, extra-territorial operation of the CDR regime and the Privacy Act will require additional guidance. It is difficult to see how the connection to Australia is to be established. Paragraph 56AO(3)(c) extends application of the CDR regime where:

> *the act or omission occurs wholly outside Australia, and an Australian person suffers, or is likely to suffer, financial or other disadvantage as a result of the act or omission.*

Guidance on this matter will be particularly important. It is not clear how paragraph 56AO(3)(c) aligns with the 'Australian link' test set out in subsections 5B(2) and (3) of the Privacy Act. The phrase 'carries on business in Australia' in paragraph 5B(3)(b) of the Privacy Act is not defined in the Act. The OAIC, in the *Australian Privacy Principles*

[1] *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFA 4.

*Guidelines*, suggests that other areas of the law in which the phrase arises may provide some guidance. To that end, the OAIC suggests:[2]

> *An entity may carry on business in Australia despite the bulk of its business being conducted outside Australia,[3] or the entity not having a place of business in Australia,[4] provided there is some activity in Australia that forms part of the entity's business.[5] …*
>
> *Where an entity merely has a website that can be accessed from Australia, this is generally not sufficient to establish that the website operator is 'carrying on a business' in Australia.[6]*

26. The Bill is still very complex which may create difficulties regarding interpretation.

**The CDR Rules**

27. Consideration should be given as to how the Rules can address some of the unintended consequences and complexities noted above.

Thank you for the opportunity to provide these comments.

The Law Council would be pleased to elaborate on the above issues, if required.

Please contact Dr Natasha Molt, Director of Policy, Policy Division (02 6246 3754 or at natasha.molt@lawcouncil.asn.au), in the first instance should you require further information or clarification.

Yours sincerely

**Arthur Moses SC**
**President**

[2] Office of the Australian Information Commission, *Australian Privacy Principles Guidelines: Privacy Act 1988* (February 2014) < https://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/APP-guidelines-combined-set-v1.pdf >.
[3] *Gebo Investments (Labuan) Limited v Signatory Investments Pty Limited* [2005] NSWSC 544, [39] ('*Gebo Investments*'); *Norcast SárL v Bradken Limited (No 2)* [2013] FCA 235, [255] citing *Gebo Investments* [2005] NSWSC 544; *Luckins v Highway Motel (Carnarvon) Pty Ltd* (1975) 133 CLR 164.
[4] *Bray v F Hoffman-La Roche Ltd* [2002] FCA 243 [63]; *Luckins v Highway Motel (Carnarvon) Pty Ltd* (1975) 133 CLR 164.
[5] *Australian Securities and Investments Commission v ActiveSuper Pty Ltd (No 1)* [2012] FCA 1519, [47]; *Gebo Investments* [2005] NSWSC 544, [33].
[6] *Gebo Investments* [2005] NSWSC 544.