Financial Rights LEGAL CENTRE

Submission by the

Financial Rights Legal Centre

Treasury

Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation 24 September 2018

October 2018

Financial Rights Legal Centre |PO BOX 538, Surry Hills 2010 | Tel (02) 9212 4216 |Fax (02) 9212 4711 | info@financialrights.org.au | www.financialrights.org.au | @Fin_Rights_CLC | ABN: 40 506 635 273

About the Financial Rights Legal Centre

The Financial Rights Legal Centre is a community legal centre that specialises in helping consumers understand and enforce their financial rights, especially low income and otherwise marginalised or vulnerable consumers. We provide free and independent financial counselling, legal advice and representation to individuals about a broad range of financial issues. Financial Rights operates the National Debt Helpline, which helps NSW consumers experiencing financial difficulties. We also operate the Insurance Law Service which provides advice nationally to consumers about insurance claims and debts to insurance companies, and the Mob Strong Debt Help services which assist Aboriginal and Torres Strait Islander Peoples with credit, debt and insurance matters. Financial Rights took close to 25,000 calls for advice or assistance during the 2017/2018 financial year.

Financial Rights also conducts research and collects data from our extensive contact with consumers and the legal consumer protection framework to lobby for changes to law and industry practice for the benefit of consumers. We also provide extensive web-based resources, other education resources, workshops, presentations and media comment.

This submission is an example of how CLCs utilise the expertise gained from their client work and help give voice to their clients' experiences to contribute to improving laws and legal processes and prevent some problems from arising altogether.

For Financial Rights Legal Centre submissions and publications go to
www.financialrights.org.au/submission/ or www.financialrights.org.au/publication/

Or sign up to our E-flyer at www.financialrights.org.au

National Debt Helpline 1800 007 007
Insurance Law Service 1300 663 464
Mob Strong Debt Help 1800 808 488

Monday – Friday 9.30am-4.30pm

Introduction

Thank you for the opportunity to comment on the *Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation.* In this submission the Financial Rights Legal Centre (**Financial Rights**) will predominantly address Proposal 2: Interaction of the Privacy Safeguards with the Privacy Act. Financial Rights has significant concerns with the complexity and weakness of the proposed new privacy framework, particularly regarding:

- the overarching confusing, convoluted and piecemeal nature of the CDR;
- the treatment of many data recipients as data holders; and
- the exemption of data holders from the Consumer Data Right (**CDR**) Privacy Safeguards.

Application of the CDR Privacy Safeguards with the Privacy Act

The safeguards detailed under the APPs are weak and do not adequately protect consumers

Financial Rights has made clear in previous submissions our concerns that the current Australian *Privacy Act* safeguards as detailed under the APPs are weak and do not offer adequate protections to consumers.[1] The introduction of the CDR is an explicit acknowledgement on the part of Treasury that the current APPs are out of date and insufficient. The appropriate and necessary response to this acknowledgement is a comprehensive review and strengthening of the *Privacy Act* and the APPs.

Implementing the CDR alongside the APPs will implement multiple privacy standards, which will be confusing for consumers and industry alike, and will leave consumers vulnerable to lower protections.

[1] Joint submission by the Financial Rights Legal Centre and Financial Counselling Australia to Treasury, Treasury Laws Amendment (Consumer Data Right) Bill 2018 http://financialrights.org.au/wp-content/uploads/2018/09/180907_CDRLegislation_Submission_FINAL.pdf; Joint consumer submission on the Open Banking: customers, choice, convenience, confidence Final Report, March 2018 http://financialrights.org.au/wp-content/uploads/2018/03/180323_OpenBanking_FinalReport_Sub_FINAL.pdf; Joint supplementary submission by the Financial Rights Legal Centre and Consumer Action Legal Centre Treasury Open Banking: customers, choice, convenience, confidence, December 2017 http://financialrights.org.au/wp-content/uploads/2017/10/171025-Open-Banking-Supplementary-Submission-FINAL.pdf, Joint submission by the Financial Rights Legal Centre and Consumer Action Legal Centre Treasury Open Banking: customers, choice, convenience, confidence, October 2017, http://financialrights.org.au/wp-content/uploads/2017/09/170922-FINAL-submission-open-banking-issues-paper.pdf; Submission by the Financial Rights Legal Centre Productivity Commission Draft Report: Data Availability and Use, October 2016 http://financialrights.org.au/wp-content/uploads/2016/12/161216_FRLCSubmission_draft-report-Data-Availability-use.pdf

This second round proposal from Treasury with respect to a newly conceived application of Privacy Safeguards and Privacy Act protections to different CDR participants only serves to heighten our serious concerns with the CDR regime. The second round proposal is confusing and impractical.

We maintain that the CDR legislation should not be finalised nor implemented until the *Privacy Act* and the APPs are reviewed and strengthened.

Financial Rights cannot support the exemption of Data Holders from most, if not all, Privacy Safeguards. If the CDR is to be consumer focussed, increased privacy safeguards must be applied to all CDR data whether it is held by the Data Holder, an Accredited Data Recipient or an Accredited Person. The Open Banking Report makes it clear that the privacy protections applying to consumer data currently, as expressed by the Privacy and APPs are wholly inadequate to protect consumers in a modern data fuelled economy. The approach taken in the proposal is based squarely on the interests of data holders to not be burdened with stronger privacy safeguards and regulatory requirements rather than from a perspective of consumers wanting confidence in the handling of their data.

Financial Rights cannot support the proposal to allow Data Recipients to become Data Holders with respect to CDR data that they have collected or generated themselves and not as a result of the CDR. This is absurd. The entire point of the CDR regime is to build confidence in the use of CDR data. Increased privacy safeguards are essential to this. Creating a loophole to apply lower standards is not in the interests of consumers as it will expose them to exploitation and fewer protections, just as they are being encouraged to move data to new financial entities.

As for the different application of Privacy Safeguards Financial Rights notes that Treasury have provided no explanation or policy justification for the application of the Privacy Safeguards that they have chosen to apply to each category.

Why should a Data Holder only have privacy safeguards 1, 10, 11 and 13 apply? While we do not agree with the policy, we can at least comprehend that a Bank as a Data Holder would not want to have to apply privacy safeguards to data they already hold because it would be an additional regulatory burden. We however do not see the justification for privacy safe-guards to non-apply to a FinTech in their new capacity as a Data Holder.

It is also unclear why Privacy Safeguards 1, 3, 4, 5 will now apply to Accredited Persons but Privacy Safeguards 2, 6, 7, 8, 9, 10, 11 will apply to Accredited Data Recipients? Why should an Accredited Person have to maintain an Open and transparent management of CDR and not an Accredited Data Recipient? Treasury provide no explanation as to how an accredited person is different to an accredited data recipient for the purposes of applying the Privacy Safeguards. It is not clear at all from the draft legislation and proposal papers provided.

Even if there is some policy justification that can be explained - at a minimum, these proposals have introduced a bewildering level of complexity to an already confusing framework. To demonstrate the complexity we have updated the schema that we included in our first submission regarding the application of high and low protections based on our understanding of what Treasury are now proposing:

1. Transactional data held by a bank that may at some point in the future be CDR data (a data holder) but has yet to be requested to be ported, is currently and will continue to be subject to the APPs. Privacy Safeguard 1 will however apply.
2. This transaction data becomes "CDR data" once requested to be transferred to an accredited Data Participant where its transfer and use will be subject to CDR Privacy Safeguards 10 (Applies to the disclosure of CDR data and PS 11, PS 13 – Apply to the disclosure of CDR data and substituting for APPs 11 and 12 in respect of disclosed CDR data)
3. The transactional data continuing to be held by the original bank remains subject to the APPs and PS1.
4. CDR data collected and held by an Accredited Data Participant will be subject to the CDR Privacy Safeguards PS 2, PS 6, PS 7, PS 8 , PS 9, PS 10, PS 11 The Privacy Safeguards apply and substitute for the APPs. The APPs do not apply to an accredited data recipient of CDR data in relation to the CDR data that has been received or data derived from that data.
5. CDR data collected or generated by Accredited Data Participants and not as a result of the CDR, will be included in the definition of data holders and therefore not be subject to the privacy safeguards – but (maybe) Privacy Safeguard 1.
6. CDR data collected and held by an Accredited Person will be subject to the CDR Privacy Safeguards PS 1, PS 3, PS 4, PS 5 - The APPs apply concurrently, but with the more specific Privacy Safeguards prevailing.
7. CDR data collected or generated by an Accredited Person and not as a result of the CDR, will be included in the definition of data holders and therefore not be subject to the privacy safeguards – but (maybe) Privacy Safeguard 1.
8. Non-CDR Data held by Accredited Data Participants will be subject to the APPs (as reformed by proposed Subsection 6E(1D) of the *Privacy Act*)
9. Non-CDR Data held by Accredited Person will be subject to the APPs (as reformed by proposed Subsection 6E(1D) of the *Privacy Act*)
10. CDR data held by non-accredited parties who are "APP entities"[2] will be subject to the APPs, not the CDR privacy safeguards.
11. CDR data held by non-accredited parties who are not "APP entities" will neither be subject to the APPs nor the CDR privacy safeguards but only general consumer protections and law.

This proposed schema above is, on the face of it, confounding, complicated and will be a nightmare for both industry and consumers alike. How anyone (including lawyers) is supposed to navigate the proposed application of privacy safeguards is beyond us?

[2] Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses

We have been assured in consultations that consumers can take any disputes that arise and they will be told at this point which privacy safeguards will apply? This is in no way reassuring and suggests that consumers may not have any idea what protections will be applying at the initial stages of obtaining new FinTech products and services that use CDR data.

The policy straitjacket imposed on Treasury by Government to develop a consumer data portability regime without introducing much-needed economy-wide reforms to privacy laws seems, from our perspective, to be the reason Treasury is forced to tie itself up in knots in applying a variety of different standards in a variety of different situations.

The obvious and most straightforward solution is to review the *Privacy Act* and APPs, introduce higher privacy standards across the economy as is the case in the EU GDPR and apply them equally to all to better protect consumer interests.

The current approach is one centred on opening up consumer data to be exploited by the financial services industry to create new business models and businesses, and encourage competition and innovation. The approach assumes that consumer interests will then be served by this increase in competition and innovation. This is leading to poor to middling privacy protections for consumers with a needlessly convoluted patchwork of standards across different categories of people and entities.

At a minimum we would recommend that Treasury or the ACCC develop a plain English version of the CDR Privacy Framework to explain to consumers how it will work but we very much doubt whether such an exercise is possible.

We believe the approach needs to be flipped on its head and government must prioritise consumer interests in protecting, securing and using their data which are then used as the basis for encouraging industry innovation and competition to serve those needs appropriately.

Recommendations

1. **The CDR legislation should not be finalized nor implemented until the *Privacy Act* and the APPs are reviewed and strengthened.**
2. **If the Government does proceed with implementing the draft CDR legislation, the CDR Privacy Safeguards should apply to all CDR participants across the board.**
3. **Accredited data recipients should not be able to be treated as data holders and thus exempt from the Privacy Safeguards.**
4. **There should not be separate categories of "accredited person" and "accredited data recipient" without a clear rationale for this distinction and for the differing applications of the CDR Privacy Safeguards.**

Concluding Remarks

Thank you again for the opportunity to comment. If you have any questions or concerns regarding this submission please do not hesitate to contact Financial Rights on (02) 9212 4216.

Kind Regards,

Karen Cox
Coordinator
Financial Rights Legal Centre
[redacted]