Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

14 October 2018

ACCC

By email: ACCC-CDR@accc.gov.au
By email: Kathryn.Wardell@Treasury.gov.au

RE: Consumer Data Right Rules Framework

This submission is made by the Australian Privacy Foundation in response to the ACCC consultation on the Consumer Data Right Rules Framework (CDR Rules).

The Foundation has made a separate submission to Treasury about the CDR.

The Foundation

The Foundation is the nation's preeminent civil society organisation concerned with privacy. It is politically unaligned. Its board features experts from the legal, health, information technology, management and other sectors.

Detailed information about the organisation's objectives and constitution are available on its website at www.privacy.org.au. The site also features many of the submissions and position papers from the Foundation over the past thirty years.

1. **General obligations and structure of the Rules Framework**

<u>The status of the CDR Rules</u>

The CDR Rules are critical for the effectiveness and fairness of the CDR. There is a power to make the Rules in the CDR Bill. However, we would contend this does not go far enough. The CDR Rules must be enforceable at law.

Recommendation:

- **The CDR Rules must be enforceable at law and particularly in EDR**

Access to Justice

It is our understanding that the definition of Accredited will require membership of an authorised External Dispute Resolution (EDR) scheme. In this case, the requirement for financial services providers there would be a requirement to join the Australian Financial Complaints Authority.

Access to justice is a key consumer right. The requirement to be in an EDR must be included in the CDR Bill. It is not sufficient to put it in the CDR Rules. It is also important that there is a clear right under the law to claim compensation for a breach of the CDR Rules.

Recommendations:

- **The requirement to be in EDR to be accredited must be stated clearly in the Bill**
- **Consumers must be able to seek compensation in EDR or Court for a breach of the law or CDR Rules**

2. Sharing data with third party recipients

The Foundation supports the principles outlined in this section.

3. CDR consumer – who may take advantage of the CDR

No comment.

4. Data holder – who is obliged to share data?

No comment.

5. Data sets – what data is within scope?

The Foundation expects the CDR Rules to cause widespread confusion in the big 4 banks about what personal information the consumer is entitled to. Currently, a consumer is entitled to personal information under:

- Australian Privacy Principles
- For personal credit – National Credit Act

The drafting of the Australian Privacy Principles on access is quite wide and it is likely that the CDR will be narrower. The CDR Rules specifically need to flag to all involved that consumers still have access rights to information that may go beyond the CDR.

The Foundation also notes that there are inherent dangers for consumers in reciprocity requirements. There is a big difference between providing equivalent and standardized data and making a requirement for reciprocity. A right to get data is not reciprocity. Reciprocity is a requirement to share data equally. To restate, "if I share my data, you must share your data on the exact same terms." This goes further than the principles outlined in CDR. It allows the possibility of some firms to bully banks into complying with particular high standards.

The main concern for the Foundation is that reciprocity will be used to bully banks to provide data when the bank knows or suspects the business representing the consumer is predatory. It is almost certain that the introduction of the CDR will bring with it businesses designed to prey on people by using this process. It will also mean that consumers are likely to be conned into transferring their services based on misrepresentation of the data obtained using CDR. In this context, reciprocity should not be introduced until there is evidence it is necessary.

It is also essential that the ACCC carefully consider a range of methods to protect consumers from predatory behaviour using the CDR.

No comment on the remainder of this section.

Recommendations:

1. **The Foundation notes the need to be clear to data holders that consumers have a range of rights to their personal information (not just the CDR)**
2. **Consumers need to be protected from predatory behaviour that exploits the CDR**
3. **Reciprocity should not be introduced**

6. Accreditation

Accreditation must not be granted to an applicant unless it is a member of an EDR recognised by the ACCC. This must be in the CDR Bill and in the CDR Rules. The CDR Rules should specifically provide that a failure to be in EDR or to pay a determination made by EDR is immediate cause for a revocation of the accreditation. The banks are already in EDR. However, there will be financial services providers who seek to use the CDR which are not currently required to be in EDR. It is essential that all people dealing with the consumer's data are in EDR.

It is essential that consumers have clear access to justice if there is a breach or misuse of their data.

The Foundation does not support two tiers of accreditation.

Recommendations:

- **All accredited service providers using CDR must be in EDR (including foreign entities)**
- **A failure to maintain membership or pay a determination is immediate cause for accreditation to be withdrawn**
- **The Foundation does not support two tiers of accreditation**

7. The Register

No comment.

8. Consent

Generally, the Foundation supports the principles set out to ensure consent works for consumers.

The Foundation does want to point out that there are major problems with making sure consent is freely given and informed. The Privacy Principles sets out a whole range of requirements for consent, however, there is a systemic lack of compliance. There has been no obvious enforcement on this by the OAIC. It is in that context that it is essential that the CDR Rules set out in prescriptive detail what is required to get consent and that this works.

The Foundation is very concerned that people will be misled and pressured into data comparison and transfer of services when it is not in the person's best interests. One of the ways to ensure this does not happen is to be very prescriptive about consent.

The Foundation strongly supports a right to delete redundant information. This should be enshrined in the CDR Rules. De-identification is known to be ineffective and it likely to be less effective as time goes on.

In particular, consent for joint accounts must be from both parties. This is essential to prevent data being moved without the knowledge or consent of the other party. It can be very dangerous for information to be moved without the consent of the joint account holder where one party is a victim of family violence. In our view, the joint accounts should not be able to be accessed at all for another 12 months while the issues with joint accounts are reviewed carefully.

It is relevant to note that banks are poor at handling joint accounts. The old paper signature process is a thing of the past and many joint accounts are accessible through ATMs, online banking and telephone banking. To make an account two to sign is almost impossible in the current environment for ordinary consumers who still need to use ebanking. It is impractical to go into the branch for every transaction. Banks need to innovate further in this area to ensure that customers who have financial abusive partners have better control of their money.

Finally, it is essential that consumers have a range of methods available to withdraw services. First and foremost, the consumer must be able to email to withdraw consent, manage deletion or make a complaint. Email is incredibly important as it provides a receipt/copy to be used as evidence. The email address should be available on websites and listed on the EDR website in the IDR details. Other options that should be available are a dashboard in online banking. However, any major changes need to be confirmed via email so the consumer has a record.

Recommendations:

- **Consent should be subject to prescriptive rules to ensure all consumers are freely giving consent.**
- **Joint accounts should not be included in the CDR for the next 12 months to enable a careful review of the issues.**
- **Consumers must be able to withdraw services, manage their data (including deletion) and raise a dispute via email (dedicated email address) or by online banking with confirmation in writing of any significant changes.**
- **The consent should expire in 90 days.**

9. Authorisation and authentication process

The Foundation supports the process as set out in the paper. The Foundation supports setting service level standards for authorisation and authentication.

10. Providing consumer data to consumers

Supported.

11. Making generic product data generally available

No comment.

12. Use of data

The Foundation strongly supports the requirement to obtain consent for the specific uses of the data and that the data can only be used in that way.

The Foundation does not support any right for consumers to transfer the data to a non-accredited entity. If the consumer wants to do this they can do it themselves. It is very likely that this process would be abused.

13. Rules in relation to privacy safeguards

Supported.

14. Obligations on data holders

Supported.

15. Dispute resolution

Supported**.** The CDR Rules need to provide detail so that AFCA can clearly award compensation for breaches.

16. Data standards body

Supported. We consider that it is essential that a privacy advocate should also sit on the Advisory Committee.

Yours sincerely

Dr Bruce Baer Arnold
Vice-Chair

Kat Lane
Vice-Chair