22 August 2019

Michael Palmyre
CX Lead | Consumer Data Standards
Australian Technology Park
Level 5, 13 Garden Street, Eveleigh NSW 2015
by email: Michael.Palmyre@data61.csiro.au
cc. cdr-data61@csiro.au

Dear Mr Palmyre

CX Consultation Draft | CDR Consent management and revocation

Thank you for the opportunity to comment on the Consumer Data Right (**CDR)** Consent management and revocation proposal.

Financial Rights 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.

We will address the issues of concern we have identified with the CDR Consent management and revocation from the perspective of the clients that we serve. While we attempt to constrain our comments to the Consent Management and Revocation process, we also refer to issues that remain with the Consumer Experience Guidelines Version 0.9.5, where they cross over.

Consent Management and Revocation

Management Dashboard

It is unclear whether the management dashboard will be made available outside of the CDR recipient's app. We suspect that many consumers will simply delete the app, rather than delete information within a CDR dashboard. It is also likely that consumers will have forgotten which apps they used and subsequently deleted. In re-constructing what consents a consumer has

provided when things go awry, it is important to have some way to find out what consents have been provided by a consumer – be it via a stand-alone central app or using their own banking app (as data holder).

Consistency

It is critical to ensure that access to a Management Dashboard is available to consumers in the same way on every app – otherwise consumers will be confused as to where to go to find and manage their consents. We note that component 4.5.1 states that

> *The data holder **must** provide a clear and consistent location for the consent management dashboard via which consent can be withdrawn.*

But this does not go to the need for consistency amongst many data holders.

Every Management Dashboard should be structured and look the same – otherwise consumers will be similarly confused and frustrated when searching through for their consents.

Information updated in one dashboard should be updated in all other CDR app dashboards at the same time- otherwise confusion may arise if there are any inconsistencies.

Landing page

The example wireframe uses the phrase "Data Share" as the name of the Consent Management Dashboard. "Data share" does not convey enough meaning to suggest that this is where a consumer would need to go to look at and manage the consents that they have provided. My Data Consents, My Data Sharing or something similar would provide more meaning. Whatever name is given it should be both meaningful and consistent across the open banking/CDR environment.

As currently proposed the management dashboard enables a

> *"consumer to view their data sharing arrangements from different perspectives, allowing them to see: the organisations that they are sharing data from and to; the products they are sharing data for; the use cases enabled by their data sharing; and the specific details for each of their data sharing arrangements."*

We support providing consumers the choice in the way they see or search for their consents as described above.

It is critical that industry isn't given the opportunity to pick and choose what the consumer sees first or obfuscates in some way the information that they need to see. The financial services and technology sectors are well versed at misleading consumers through information design to suit their own commercial purposes rather than serving the genuine interests of the consumer. Placing too much information, for example, about time based qualities of all the material shared up front will confuse and distract consumers. Burying the ability to withdraw consent too far down in the app is another way that would disempower consumers. Introducing too many pop-up hurdles to ask someone if they want to withdraw their consent is yet another way.

Consumers should be able to begin to easily see who they have provided consents to and withdraw that consent easily either from the landing page or after clicking once on the data recipient's basic information. Any further down begins to look like a hurdle.

Clarity and consistency on deletion and de-identification

We note that there seems to be a variety of terminology around the concept of deletion or de-identification of data. There needs to be consistency in clear terminology around these concepts and they should be well defined.

We are particularly concerned with attempts by the sector to delay full deletion of data by introducing the concept of a "temporary stop" on the use of the data. This is a clear attempt to hold on to customers and confuse consumer decision-making, consequently blurring the lines between deletion, de-identification and withdrawal of consent. Temporary stops or other attempts to place a consumer's data into a purgatory need to be curtailed.

Consent paper trails

Archived consents should retain full information regarding consents. This information should be able to exported, emailed or printed. It is important for the consumer, their representatives, financial counsellors, lawyers as well as ombudsmen, regulators and others to access this information. Consent management "paper trails" should be easily accessible to assist when things inevitably go wrong.

Revocation Confirmation

The pop-up "Are you sure" includes the statement:

> *Please ensure you are informed of the impact to your service before you stop sharing this data*

This feels redundant and reads like a warning not to proceed when the person would have just read this information.

Revocation success

Emailing a summary of the revocation is important. People may want to be given the ability to have this texted but it is likely that such information via text will not be retained.

Revocation of a consumer's revocation or undoing revocation

An idea put forward at the Consent Management and Revocation workshop was that there be the ability for a consumer to revoke their revocation for a short time after they have had their revocation request confirmed. This would act in a way similar to the "undo" notice on services like Gmail.

Financial Rights cannot support such a service on the basis that this too acts as yet another way that businesses will seek to retain data and to dissuade the consumer from revoking consent. Such a notice will muddle decision-making capacity and only serves the commercial interests of data recipients. If a consumer regrets revoking their consent, they are still free to re-sign up to the service.

Joint account holders

It is unclear where and how a Management Dashboard will be accessed by a joint holder who has not downloaded the Data Recipient's app. We note that it is recommended that:

> *Following a joint account authorisation, the non-initiating account holder **should** be provided with instructions on how to review and revoke authorisation via a dashboard.*

Does this mean that the joint account holder will be forced to obtain the app or will they be able to use another app including their Bank/Data holder's app?

It should be made clear in the consent management dashboard who provided the consent. Many people may forget that they provided the consent.

Joint account holders should also have the option to not provide their phone and address details as a part of the data that is being ported. We see little reason why providing this information in full is necessary. There are however dangers in some family and domestic violence situations where access to this information could lead to serious consequences. Unless there is a clear justification for the collection and use of this data, it's inclusion needs to be re-considered

Consumer deletion right

As you would be aware a consumer deletion right will be added to the Consumer Data Right legislation in the next session of parliament. The legislative amendment will require the consumer data right rules to specify a requirement for accredited data recipients to delete all or part of the CDR data in response to a valid request by a CDR consumer for the CDR data to be deleted. It is important therefore that the consent regime and consent management and revocation dashboard reflect this ability in the first iteration of the consent regime.

Stored overseas

In line with protections under the CDR regarding overseas disclosure of CDR data by accredited data recipients (Privacy Safeguard 8), information regarding overseas storage needs to be included in the consent management and revocation dashboard. Consumers should also be given the choice to have their data removed from overseas storage.

Data de-identification

As per Component 2.13.1 consumers should be provided with information about what de-identification means, how it will be de-identified and genuine examples of how de-identified data may be put to use. However the information needs to be realistic and should not be provided in a way that provides false or unrealistic assurance that their data will not be able to be re-identified. In other words we believe that this information should provide a warning to consumers of the dangers of de-identification. As the Office of the Victorian Information Commissioner recently found:

De-identifying large and complex datasets is difficult, and in some cases may be impossible.[1]

The results of any breach can and has in other contexts led to re-identification which can lead to serious consequences for consumers. This warning/information should be available both in the consent management and revocation dashboard but also be provided at the time of data being requested.[2]

We note that the Consumer Experience Guidelines Version 0.9.5 Component 2.12.1 states that:

> *The data recipient should state the intended purpose(s) of de-identifying CDR data when requesting this consent.*

The example wireframe used on page 53 does not however provide any real information about such use and merely states:

> *We use de-identified data for purposes other than those stated here.*

This is meaningless. Understanding that this may just be an example, it is not a good one. More specific guidance on what is required should be provided. Data recipients should, for example be prevented from describing the use of de-identified data in a broad or bland manner. Stating, for example, that "we use de-identified data to improve our product" should not be acceptable. More detail should be required.

Cancel v stop sharing buttons

The "cancel" and "stop sharing" buttons in the wireframe proposal are the same size and colour – this could be potentially confusing and may need to be differentiated.

Language

We note that Component 2.4.2 of the Consumer Experience Guidelines version 0.9.5 states that:

> *CDR information should have full translation functionality and be fully screen-reader accessible.*

The ability to translate the app into many languages should always be available and be a straight forward and accessible process.

[1] Annan Boag, Assistant Commissioner, Privacy and Assurance Myki incident- lessons for organisations , August 15, 2019 https://ovic.vic.gov.au/blog/myki-incident-lessons-for-organisations/

[2] Components 2.12 and 2.13 of the Consumer Experience Guidelines Version 0.9.5

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
Chief Executive Officer
Financial Rights Legal Centre
Direct: (02) 8204 1340
E-mail: karen.cox@financialrights.org.au