CONSUMER
DATA
STANDARDS

CX Workshop: Consumer control

October 22 2019, Sydney

https://consumerdatastandards.org.au/

Context

CDR v1 data standards allow for the provision of consent at the level of a data cluster. The Data Standards Body (DSB) is now exploring ways to provide more fine-grained control for the regime.

To inform our thinking, the DSB has reviewed some of the literature on privacy, transparency, trust, personal information management, and control more generally.

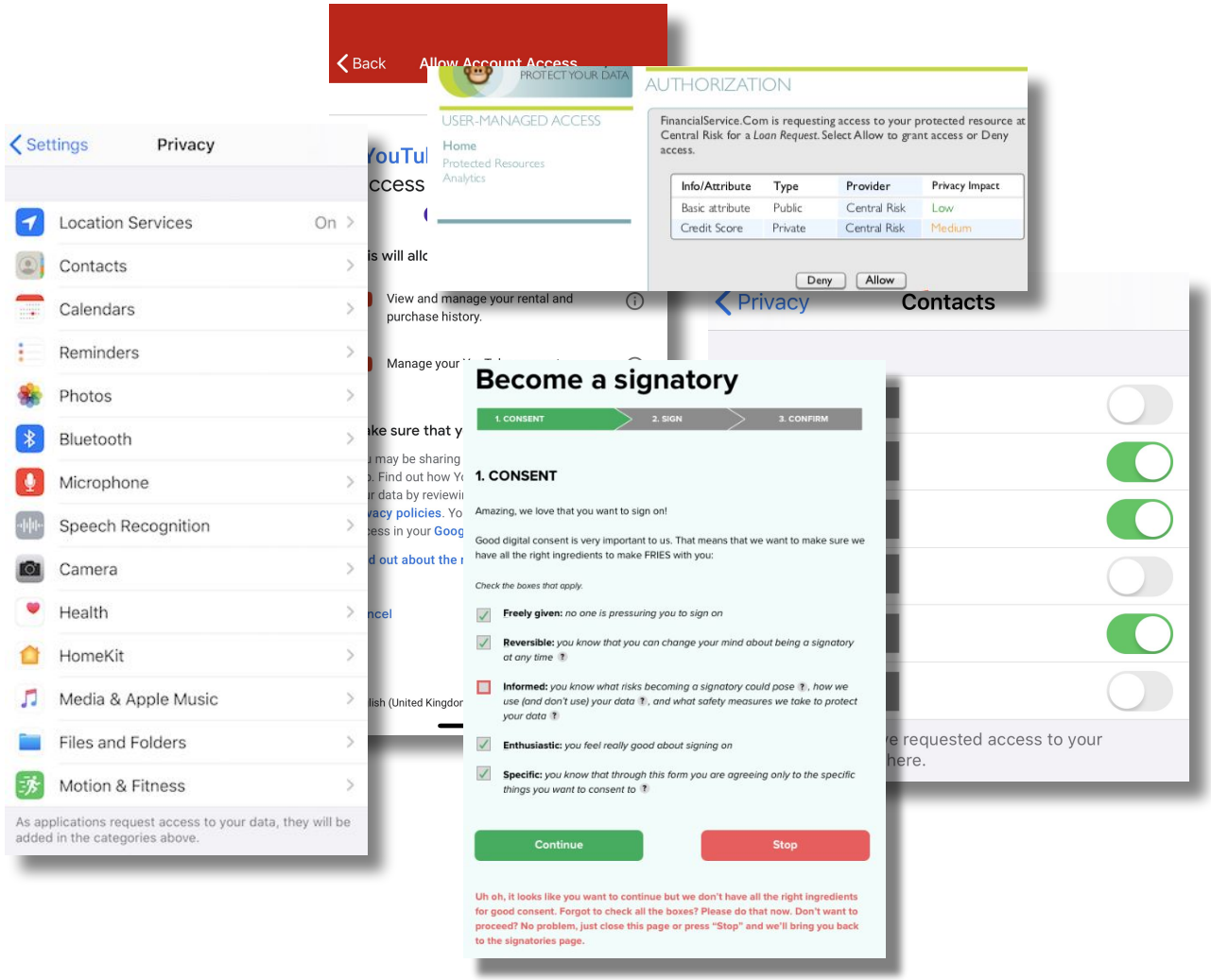
We've approached these topics from the perspectives of anthropology, sociology, behavioural economics, psychology, and computer science. Existing implementations were also reviewed.

Reference points

- Privacy
- Transparency
- Trust
- Personal information management
- Control
- Anthropology
- Sociology
- Behavioural economics
- Psychology
- Computer science
- Existing implementations

Consent

Consent-based data sharing is still emerging as a practice. Many principles exist around providing consumer control, but examples of consumer-facing interactions aren't as prevalent.



Privacy

Attitudes vs behaviour

The prevailing view is that there are 2 types of ‘user’:

- those who care about their privacy; and
- those who don’t

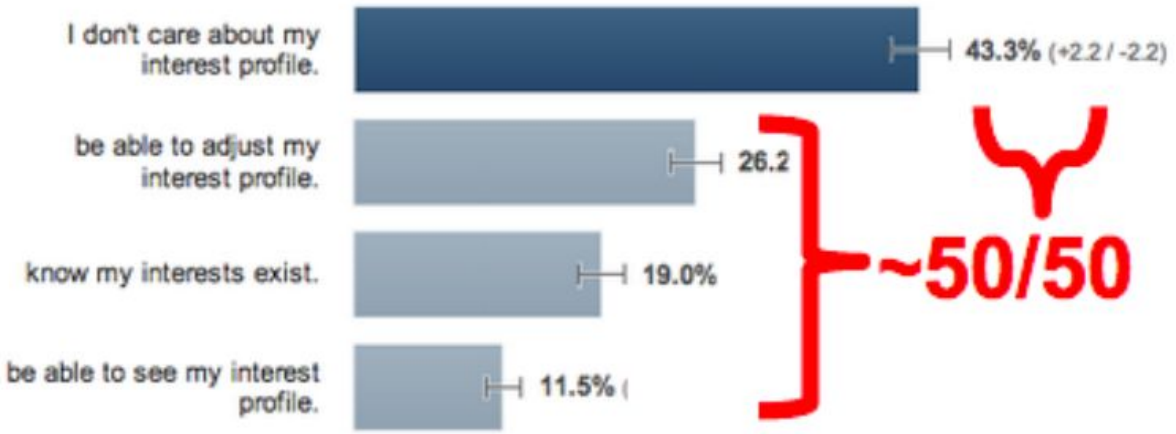
However, this is context dependent, and these attitudes can change over time.

When a breach of some sort occurs, things can shift dramatically and people become a lot more concerned about their privacy.

When designing something as significant as the CDR we should always act as if everyone cares about their privacy, even if they don’t appear to right now.

There is a tendency to see two types of ‘user’: those who care and those who don’t.

But, when breaches occur and awareness increases, people do care.



Control, trust and choice

Research shows that providing more control generally increases trust for those who seemingly do and don't care about their privacy.

There is a risk of creating choice overload, but more control doesn't necessarily 'overwhelm' or scare people off - especially when choices are presented appropriately.

Providing control

More control may lead to a '***control paradox***', where people partake in riskier behaviour as a result of having more control. This is similar to the 'moral hazard' effect in economics, where someone may take more risks when they are insured.

One way to address this when it comes to data sharing is by providing control throughout the consent model, not just before consent is given.

Current state | Future state

The CDR already tends to many of the issues raised previously by requiring consent to be informed, to not be bundled, and to be specific as to purpose. Consumers will now also have the right to deletion and a range of ways to review and manage their sharing arrangements on their dashboards.

While the consent flow has been identified as a priority area for consumer control possibilities, other directions we've identified include control over historical data access, pre-determining what to share on a DH dashboard, amending existing consents via dashboard and reauthorisation, or more fine-grained withdrawal.

The following pages contain a few tangible scenarios and examples of where consumer control may occur.

Existing controls

- Consent process
- Review/withdraw
- Right to delete

Possibilities

- Permission-level control
- Historical data
- Predetermined consent
- Amending consent via re-authorisation, dashboards
- Fine-grained withdrawal

Consumer control scenarios

The following slides contain hypothetical examples of how fine-grained control could exist in the CDR regime.

They were produced by the CX Workstream as workshop stimulus.

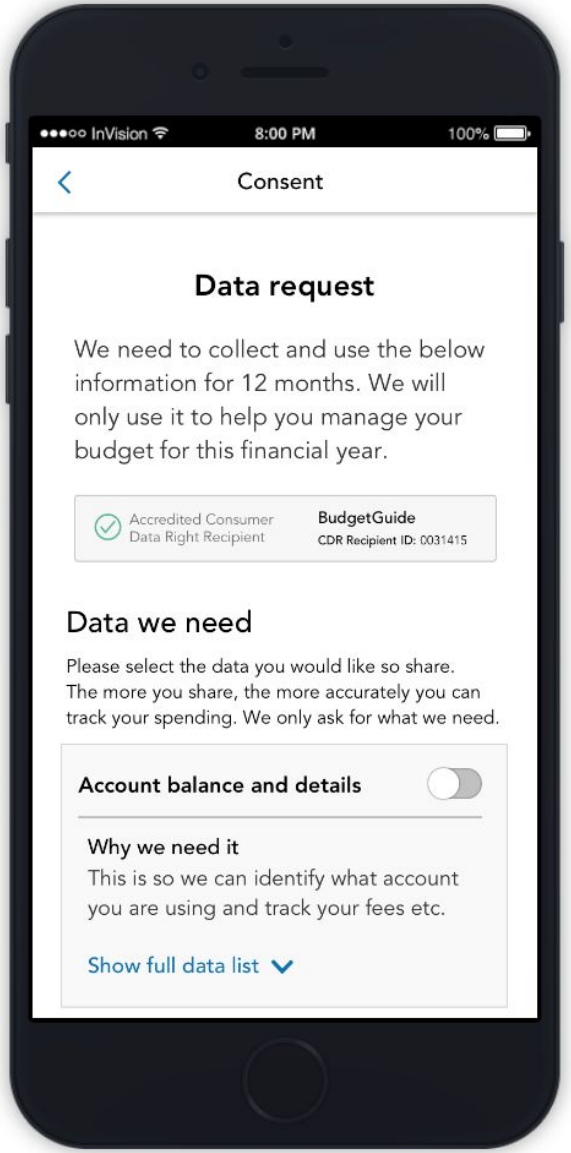
Permissions level control

In this scenario, the consumer is going through the consent flow and is happy to share most of the permissions of the '*Account balance and details*' data cluster, but not the '*Account mailing address*' permission as they feel this is personal information.

The data recipient can show this by toggling on all permissions only after a data cluster has been selected (similar to a select all functionality), allowing the consumer to unselect the desired permissions.

Considerations: What does this mean for data cluster language? Does it change? Clustering data aids comprehension, but are data clusters needed if only some permissions are required?

Please note: *The example shown is an interpretation of how this scenario could work. This is not a final design suggested by the CX Workstream.*

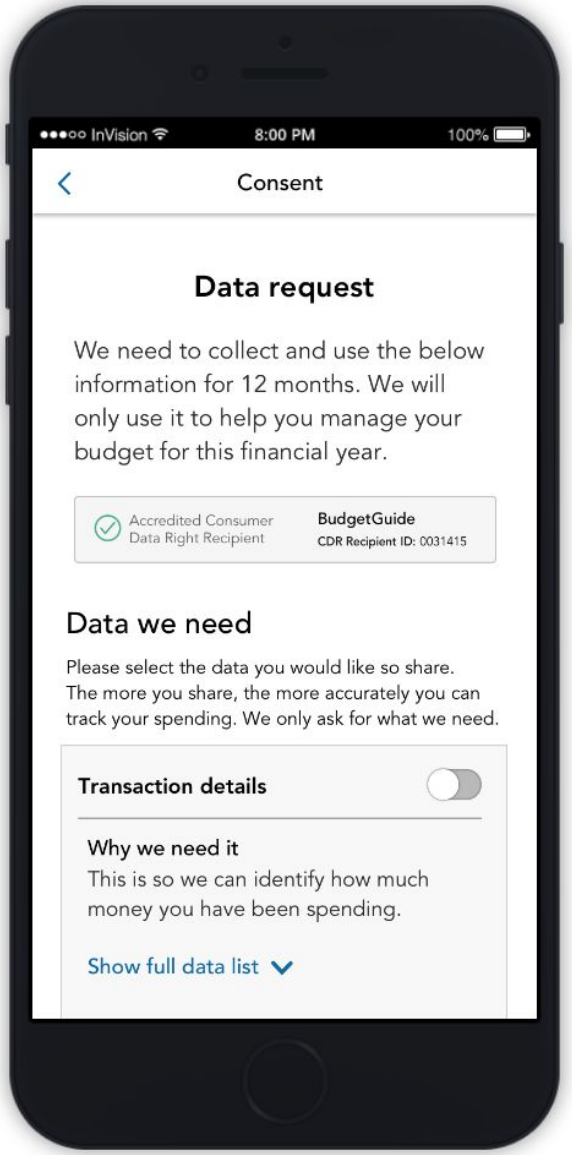


View prototype

Historical data

In this scenario, the consumer is going through the consent flow and does not want the data recipient accessing the past 3 years of historical data. The consumer wants to change the historical date range to be 1 year only.

As this would only apply to some data sets, it makes more sense to attach this level of control to the data cluster rather than frame it as an overall historical range.



[View prototype]

Please note: *The example shown is an interpretation of how this scenario could work. This is not a final design suggested by the CX Workstream.*

Predetermined preferences

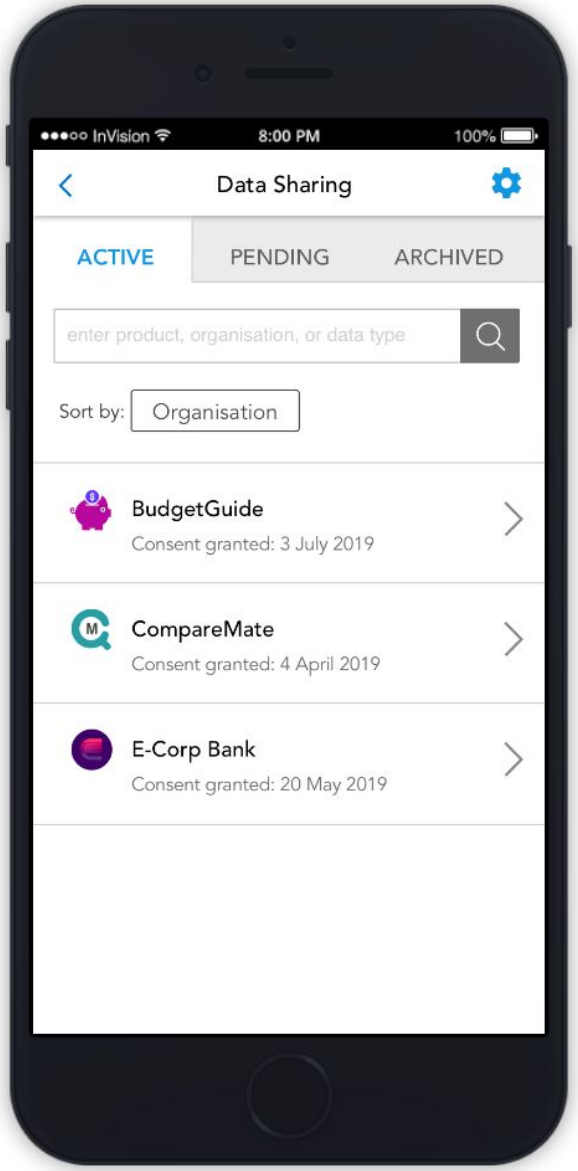
Data holder dashboard

In this scenario, consumer may not want to share certain data or may want to limit access to certain periods. They could do this by pre-determining what is shared by default on a data holder dashboard.

This could occur at the permission level as well as the data cluster level. It could also apply to joint account management, where a non-initiating account holder could predetermine what they are willing to have shared from their account by the other account holder.

Notification preferences could also occur at this level, allowing consumers to manage how they receive CDR receipts and ongoing notifications.

Please note: *The example shown is an interpretation of how this scenario could work. This is not a final design suggested by the CX Workstream.*



View prototype

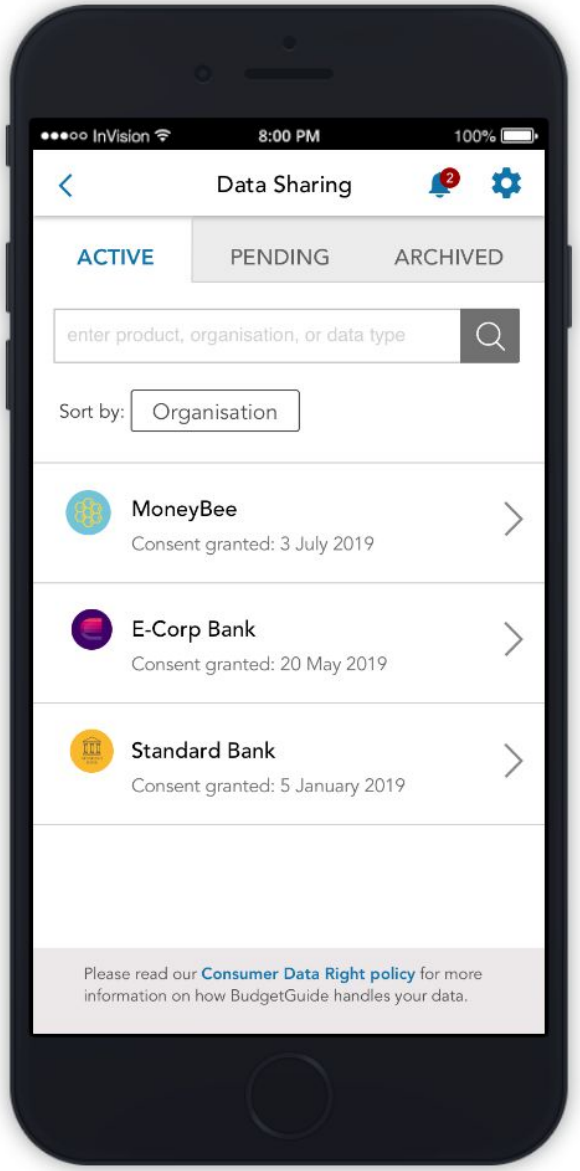
Predetermined preferences

Data recipient dashboard

In this scenario, the consumer may want to pre-determine to always have their redundant data deleted.

If a consumer always prefers to have their data deleted instead of de-identified, they shouldn't have to continue stating that preference. This preference should be remembered and this could occur in settings or ideally, whenever they have the opportunity to make this election.

Please note: *The example shown is an interpretation of how this scenario could work. This is not a final design suggested by the CX Workstream.*



View prototype

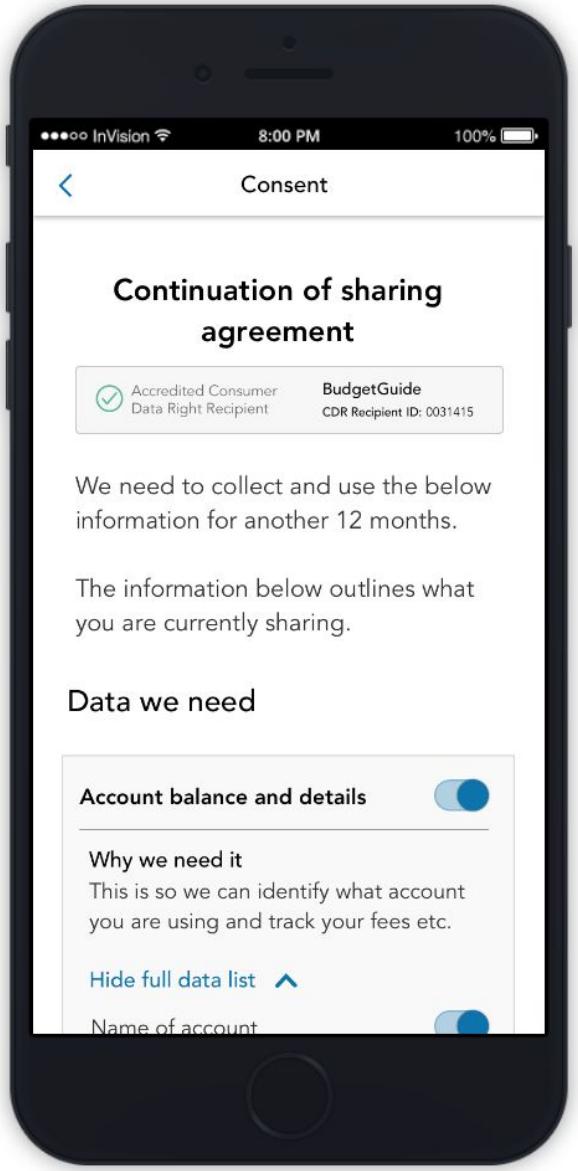
Reauthorisation

In this scenario, a 3 month trial has completed and the consumer is asked to reauthorise.

During reauthorisation, the consumer wants to expand the arrangement to include other permissions. The data recipient would like the consumer to extend the duration to 12 months, but the consumer would like to amend the date.

During our consumer research we saw the desire for a ‘trial’, where a consumer may want to try out data sharing with a small amount of data for a short period, and then expand their sharing arrangement. This could include data shared, the purpose(s) of sharing, and the duration of sharing (e.g. to have it align with things like subscriptions or the financial year).

Please note: *The example shown is an interpretation of how this scenario could work. This is not a final design suggested by the CX Workstream.*



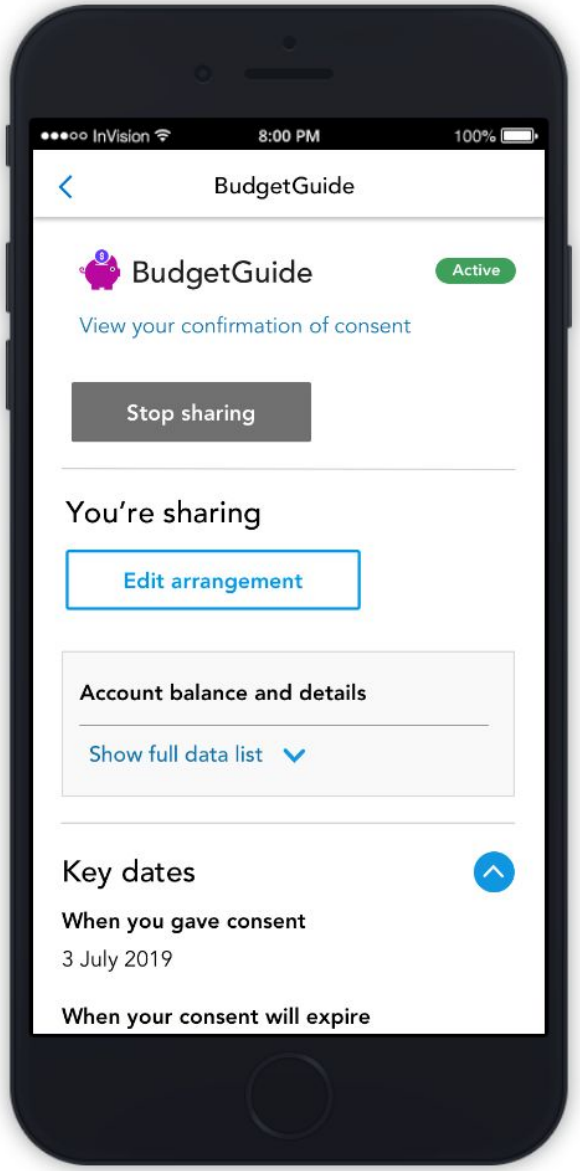
View prototype

Fine-grained withdrawal

In this scenario, a consumer may want to stop sharing some but not all data. A trigger may cause caused the consumer to reconsider their data sharing arrangement, including (a) the consumer regretting the extent of what they have shared and; (b) an event occurs (e.g. data breach, moral panic, awareness shift) and the consumer no longer wants to share certain information.

By ‘amending’ a sharing arrangement to de/select certain data types, the consumer is effectively ‘withdrawing’ a portion of the arrangement.

Please note: *The example shown is an interpretation of how this scenario could work. This is not a final design suggested by the CX Workstream.*



View prototype

Considerations

All of the previous scenarios raise the following questions:

- What if the selected data/durations conflict with what is required for the use case?
- What if permissions-level control conflicts with data clusters/language?
- When amending consents, do consumers need to go through the full consent flow again (authenticate-authorise)?
- Are these valid and appropriate ways to provide more control? Are there others? What are the priorities?

THANK YOU

Consumer Data Standards | Consumer Experience Workstream

t +61 2 9490 5722
e CDR-Data61-CX@csiro.au
w consumerdatastandards.org.au