

**CONSUMER
DATA
STANDARDS**

Consumer Experience Research Phase 3: Round 4 and 5

June 2020

Amending consent

Table of contents

Executive Summary	3
CX resources and Engagement	4
<hr/>	
Phase 3 Summary	5
Phase 3 Issues	6
<hr/>	
Research Approach	19
Approach	20
Session Overview and prototypes	23
<hr/>	
Amending Consent	30
Summary of Recommendations	44
<hr/>	
Outsourced Service Providers	48
<hr/>	
Complaints Process	52
<hr/>	
Trustworthiness and Propensity to Share	55
Switching Canvas	56

Executive summary

The Consumer Data Right

The Consumer Data Right (CDR) aims to give consumers control over information about themselves and share that information with accredited third parties. The CDR promotes competition, encourages innovation, and consumer empowerment.

The CDR's consent and transparency requirements will facilitate more consumer control, privacy conscious behaviour, and the development of trust as a competitive advantage.

For consumers, the CDR is a safe, secure, transparent, and government regulated ecosystem that consumers can opt in to.

For ADRs, the CDR facilitates effective pathways to consumer outcomes by enabling access to machine-readable data for more accurate, tailored, and real-time insights.

The Data Standards Body's Consumer Experience (CX) Workstream is helping organisations provide simple, informed, and trustworthy data sharing experiences with positive consumer outcomes in the short and long term.

Overview

This report contains findings and recommendations based on Phase 3, round 4 and 5 research. A qualitative approach was used with a total of 23 participants in 1:1 research sessions that ran for 60 minutes each.

Prototypes of the Consent Flow and related artefacts were used to facilitate insight generation. Participants were also asked to complete a series of activities to generate scores related to trustworthiness and propensity to share.

These two rounds of research focused on **amending consent**, including the ability to extend the duration of an existing consent, add/remove datasets, and add/remove uses, and create use-only consents.

A detailed research approach can be found on the [Consumer Data Standards website](#).

NB Phase 3 reports do not necessarily reflect the position or direction of the government or Data Standards Body. Recommendations found within these reports represent a set of possibilities that will be reviewed and considered and are subject to change. Reports will inform rules and data standards development but should not be seen as indicative of the CDR's direction.

CX resources and engagement

The insights and recommendations found in this report are shared for general community knowledge; to inform the direction of the CX Workstream and CDR more generally; and to support the rules and standards to be research-driven and centred on consumer consultation.

The Consumer Data Standards website contains the latest [CX Standards and CX Guidelines](#), which are also located on the [technical standards page](#).

The community can follow standards and guideline development on the relevant [CX consultation page](#) and on [GitHub](#).

CX reports containing insights and recommendations from ongoing consumer research and community workshops can be found in our [Knowledge Centre](#).

You can keep up to date with the CX Workstream's developments by signing up to our [mailing lists](#), subscribing to our [blog](#), and tracking issues on [Github](#).

You can contact the CX Workstream via email on cx@consumerdatastandards.gov.au.

Phase 3 research: Summary

Phase 3 Issues

This section contains a summary of key issues, findings, and recommendations relating to the areas investigated in Phase 3 CX research. These issues included:

Options for Energy: including various consent flow for the energy sector

Fine-grained control: exploring ways to give consumer more control over what data they share

New rules proposals: based on the creation of CX Standards and Guidelines for various issues including:

- The right to delete ([see more](#))
- Re-authorisation: extending the duration of an existing consent in a simplified manner ([see more](#))
- Additional amending consent items including: separation of collect/use, add/remove uses, add/remove datasets ([see more](#))

Simplified Consent: Exploring how consent could be simplified without impacting the quality of consent

Joint accounts: Consistency regarding how joint accounts are dealt with

Energy data language: Investigate and define data clusters and permission language to facilitate comprehension and informed consent

Phase 3 reports also provide findings and recommendations relating to trust, privacy, consumer-facing language, design patterns, and possible next steps.

Certain issues were examined comprehensively and conclusive recommendations have been made, while further work is recommended for other areas based on the research findings and proposals.

Energy consent model

What we did:

- Research focused on exploratory research related to data sharing in the energy sector, a simplification of the consent flow and data Authentication identifiers (account number and NMI)
- Prototypes that were tested to research this issue: [R1](#) | [R2](#)

Research objectives:

- Understand current consumer behaviours, pain points and needs regarding energy use cases and energy data
- Understand the consumer response to the sharing of energy data
- Understand how consumers expect data sharing to work
- Understand how trustworthy and privacy-preserving the sharing of energy data is perceived to be
- Understand how consumers currently interact with energy retailers, and how this shapes expectations and CDR accessibility
- Understand which identifiers consumers understand and can readily access for authentication purposes

What we found out: See R1/R2 report

- Consumers are digital users, just not with energy retailers (*pg 17*)
- Energy offers are hard to understand and compare, which makes it hard to understand who to switch to. (*pg 15*)
- There was high trust in the ACCC and the accreditation process but low confidence in government capabilities, including to handle data (*pg 18*)
- A variety of authentication identifiers could be used, but account number was the most familiar (*pg 24-26*)
- Non-account holders believe they should have access to their energy data (*pg 33*)

We propose:

- Consider how account numbers (or similarly common identifiers) could be used as authentication identifiers (*pg 28*)
- Define a model that allows 'delegated access' to non-account holders for data sharing purposes (*pg 33*)

Proposed next steps:

- Continue research on energy language, authentication, authorisation, and consent management based on the energy rules framework

Energy data language

What we did:

- Research was conducted to test data cluster and permission language to facilitate comprehension and informed consent
- Prototypes that were tested to research this issue: [R1](#) | [R2](#)

Research objectives:

- Understand the consumer response to the sharing of energy data
- Understand how comprehensible energy data and consent is
- Understand how trustworthy and privacy-preserving the sharing of energy data is perceived to be

What we found out: See R1/R2 report

- Energy data is difficult to comprehend but is recognised as necessary for certain use cases (pg 20)
- Participants expect data requests to be specific and relevant to the use case (pg 56)
- Some participants were uncomfortable with sharing certain permissions (e.g. occupation, hardship, physical address, payment information) (pg 22)
- There is concern that energy data can be used to discriminate (pg 19)

We propose:

- Separate payment, hardship, and concession details from other authorisation scopes. This separation will allow ADRs to provide a clear purpose and benefit for requesting these more sensitive datasets (pg 22)
- Consider fine-grained authorisation scopes driven by ADR use cases (pg 56)

Proposed next steps:

- Continue research on energy data language to facilitate comprehension and informed consent

Redundant data handling (1)

What we did:

- Research focused on consumer comprehension and perception of deletion/de-identification, and right to delete design patterns
- Prototypes that were tested to research this issue: [R1](#) | [R3](#)

Research objectives:

- Understand if the right to delete design pattern is an effective and contextual affordance.
- Understand if consumers comprehend what de-identification/deletion means.
- Understand if consumers understand the implications of electing (or not) to have their redundant data deleted, including the timing of this election.
- Understand the appropriate time and context for the right to delete election to occur.
- Understand how trustworthy and privacy-preserving de-identification is perceived to be.
- Validate if consumers expect a right to delete preference to be remembered by ADRs and applied every time.

- Validate if consumers expect the right to delete to be available for non-initiating joint account holders.

What we found out:

- Consumers expressed a preference for deletion as it was considered safer. *(R3 report, pg 42, 44)*
- Deletion by default, and de-identification as an 'opt-in' choice would better align with consumer expectations. *(R3 report, pg 44)*
- ADRs should be clear on why data may be kept even when it is no longer need for good/service provision. *(R3 report, pg 43)*
- Active choice ensures conscious selection. *(R1/R2 report, pg 43)*
- The general difference between de-identification and deletion is understood but not the risks *(R1/R2 report, pg 40-41)*
- The motivation to de-identify data is dependent on personal or collective gain. *(R1/R2 report, pg 42)*

Redundant data handling (2)

We propose:

- To reduce cognitive load, simplify consent, and increase consumer trust and confidence, redundant data should be deleted by default. *(R3 report, pg 44)*
- The de-identification of CDR data (redundant or otherwise) should always be an opt-in choice. *(R1/R2 report, pg 42, 45 | R3 report, pg 44)*
- If ADRs do need to retain data after withdrawal or expiry, they should provide a CDR Receipt following expiry/withdrawal that outlines which redundant data is being kept, why it is being kept, and how it will be treated when no longer required
- If deletion does not occur by default, ADRs should prompt consumers to exercise their right to delete whenever inaction on the part of the consumer may cause them to lose their right to election. *(R1/R2 report, pg 45)*

- If deletion does not occur by default, ADRs should present the same de-identification details regardless of whether it applies to redundant data or not, including:
 - that this data can be sold or disclosed to other parties without the consumer's consent
 - the kinds of persons they will give that data to why they would sell/disclose the data
 - that the consumer can't request de-identified data be deleted. *(R1/R2 report, pg 4)*
- ADRs should clearly explain why they may need to retain redundant data and include examples of legal, audit, or regulatory purposes. *(R3 report, pg 43)*

Proposed next steps:

- Consider deletion by default recommendation
- Consider a CDR Receipt following expiry/withdrawal that outlines which redundant data is being kept, why it is being kept, and how it will be treated when no longer required

New rules proposals

The DSB and ACCC agreed to conduct research on a number of items that may inform future CDR rules development. This covered how existing consents may be amended, including:

1. Extending the time period of an existing consent
2. Amending a consent to add or remove data
3. Amending a consent to add or remove uses
4. Allowing previously shared data to be used/carried over into a new consent
5. Separating collection and use to allow 'use only' or 'collection only' consents and withdrawals
6. Permitting withdrawal of authorisation only to allow use only consents to remain..
7. The creation of standards for simplified re-consent and re-authorisation for use any time after an original consent has been granted.

The following items were explored in Phase 3:

Items 1 and 7 were researched in a simplified re-authorisation prototype that only extended the duration of an existing consent

Items 3, 5, 6, and 7 were researched in a simplified use-only consent that requested an additional use and following consent withdrawal

Item 2 was researched in a simplified prototype that proposed a dataset be added for a new use

The concept of a 'consent history' to communicate that an existing consent has been amended and allow consumers to 'trace' a consent's history

Phase 3 did not explicitly cover:

- DH disclosure-only withdrawal flow
- A 'full' authorisation flow
- Item 4, to allow previously shared data to be carried over

Amending consent (1)

What we did:

- Research focused on extending duration, adding/removing uses, adding/removing data clusters and a simplified process that does not impact the quality of consent
- Prototypes that were tested to research this issue: [R4-1](#) | [R4-2](#) | [R5](#)

Research objectives:

- Provide consumers with the ability to amend consent while remaining empowered and in control.
- Provide consumers with simplified consent/amendment flows without compromising the quality of consent (or, while facilitating high quality consent).
- Understand what consumers expect to happen if/when they don't re-authorise.
- Understand the consumer's ability to recall the terms of the original consent.
- Understand if 'actively select' has any bearing on data cluster engagement/recollection ability.

What we found out: *See this (R4/R5) report*

- The need to 're-authorise' or 'renew' consent is seen as an important, positive, and trust-building intervention. *(pg 32)*
- Continued trust in the ADR, the perceived benefits provided by the product/service, and the consequences of expiry are motivations for re-authorisation. *(pg 33-34)*
- Participants expected to be reminded when their consent was about to expire. *(pg 35)*
- There was broad understanding of the 'renewal' process and that inaction would lead to consent expiry. *(pg 31)*
- The ability to recall the terms of an original consent varied, but the ability to recall improved after the amending consent process - suggesting that amending consent helps keep consents informed and current. *(pg 39-40)*
- Despite low abilities to describe CDR, there was overall trust in the ecosystem. *(pg 43)*
- Allowing datasets to be pre-selected did not negatively impact the quality of consent. *(pg 37)*

Amending consent (2)

We propose: *See this (R4/R5) report*

- Expiry notifications should be timely and include follow-up reminders. *(pg 31, 35)*
- The realised benefits of data sharing should be shown to consumers before they re-consent. *(pg 33)*
- Redundant data handling information should be re-surfaced. *(pg 34)*
- Consider dropping 'actively select' requirement for previously consented to datasets and uses. *(pg 37)*
- Provide transparency around the benefits and outcomes of data sharing, and distinguish between 'new' and 'existing' consents for datasets and uses. *(pg 42)*
- Provide a 'consent history' to allow changes to be tracked. *(pg 31)*
- Conduct consent quality research with consumers using real world CDR use cases. *(pg 39, 40, 41)*

Proposed next steps:

- Continue research and consultation on amending consent scenarios to refine and align
- Consider how joint accounts need to be factored into amending consent scenarios, including how 2 to authorise interacts with expiring consents

Joint accounts (1)

What we did:

- Research focused on joint account election, request and authorisation
- Prototypes that were tested to research this issue: [R1](#) | [R3-1](#) | [R3-2](#)

Research objectives:

- Understand the response to the sharing of joint account data from people who have held joint accounts.
- Understand the pre-existing barriers and needs for joint account holders that need to be considered for joint account data sharing.
- Understand how consumers expect joint account data sharing and management to work.
- Understand where and how joint accounts can be made available to share in a way that is intuitive, contextual, and also allows the user to be well-informed as to the pros and cons.
- Understand how privacy-preserving the sharing of joint account data is perceived to be.

- Understand what information needs to be communicated to consumers as requesters and as approvers of joint account elections.

What we found out:

- The authorisation flow is a natural context for a joint account to be elected. *(R1/R2 report, pg 30)*
- Comfort with joint account sharing is dependent on the account holder's relationship with the other account holder. *(R1/R2 report, pg 31)*
- Multi-party approval is expected; '2 to authorise' is aligned with mental models. *(R1/R2 report, pg 32 | R3 report, pg 36)*
- Joint account approval is conceptualised on a case by case basis *(R3 report, pg 36)*
- Confidence for JAH2 when going to authorise a joint account will depend on the provision of certain information. *(R3 report, pg 38-39)*
- There is a perception that joint account sharing will reveal personal information to the other joint account holder. *(R3 report, pg 40)*

Joint accounts (2)

We propose:

- Show unavailable joint accounts in the authorisation flow with election instructions. *(R1/R2 report, pg 37)*
- Allow election to occur during the authorisation flow. *(R1/R2 report, pg 38)*
- Although optional, 2 to authorise should be considered by DHs to align with consumer expectations. *(R3 report, pg 36)*
- Allow both joint account consumers to choose 1 or 2 to authorise in-flow. *(R1/R2 report, pg 38)*
- A 2 to authorise preference from either JAH should supersede a 1 to authorise preference by either account holder *(R3 report, pg 36)*
- Providing more information to JAH2 on who their data will be shared with and why can remove a key barrier to joint account election and sharing. *(R3 report, pg 38-39)*
- Consumers experiencing vulnerability may require specific, tailored experiences that more acutely address their needs to access an ADR service while maintaining their privacy and safety. *(R3 report, pg 40)*

Proposed next steps:

- Consider further work on '2 to authorise' for joint accounts, including for 'once-off' sharing requests
- Consider further work on how joint accounts function in amending consent scenarios
- Explore how the concept of joint account sharing applies to sectors beyond banking

Simplified Consent (1)

What we did:

- Tested which elements within the consent flow could be simplified and/or removed without negatively impacting the quality of consent.
- Experimented with:
 - The presentation of the sharing period and 'specific as to purpose' statement;
 - The separating out of various consent components, such as the right to delete
 - Removing 'actively select' requirements
 - Moving extra detail into 'dropdowns'
 - Removing certain steps in the flow
- Experimented with measures to assess the quality of consent, comprehension, trustworthiness, the level of perceived benefit, and propensity to share.
- Prototypes that were tested to research this issue: [R1](#) | [R2](#) | [R3](#) | [R4-1](#) | [R4-2](#) | [R5](#)

Research objectives:

- Understand if simplifying the Consent Flow has any impact on the quality of consent, trustworthiness, propensity to share, and confidence.

What we found out:

- Recollection of the 'sharing period' was difficult when it was presented alongside other information (*R3 report, pg 32*)
- Separating out components facilitates engagement for the 'right to delete' election (*R1/R2 report, pg 43*)
- Outlining the purpose of the request at the data cluster level facilitates control and informed consent (*R4/R5 report, pg 42*)
- Moving extra detail into dropdowns had no impact on consent quality for most participants
- Removing the actively select requirement for amending consent prototypes had no negative impact on consent quality (*R4/R5 report, pg 37*)
- Removing the authorisation step for certain amending consent scenarios had no negative impact on consent quality or trust (*R4/R5 report, pg 38*)
- In general, while omitting consent terms may 'simplify' the flow, it occurs at the expense of consent being informed

Simplified Consent (2)

We propose:

- Presenting the purpose at the data cluster level *(R4/R5 report, pg 42)*
- Consider removing the 'actively select' and 'cannot preselect' requirements for certain amending consent scenarios *(R4/R5 report, pg 37)*
- Consider removing the authorisation step when only the duration of consent is being extended *(R4/R5 report, pg 38)*
- Consider how to simplify consent over time, as consumers become confident and familiar with consent, to understand what can be removed without compromising the quality of consent or trust in the process *(R4/R5 report, pg 57-60)*

Proposed next steps:

- Continue experimenting with the simplification of consent in amending consent scenarios
- Consider where and how consumers can review accounts being shared to support the adding/removing of accounts during the amendment process

Fine-grained access/control

What we did:

- Explored where more control was sought by consumers
- This was conducted by assessing:
 - Levels of comfort and appropriateness with what and how much data was being requested for specified purposes
 - Where control was sought and exercised for adding/removing datasets and uses
- Prototypes that were tested to research this issue: [R2](#) | [R4-1](#) | [R4-2](#) | [R5](#)

Research objectives:

- Understand the consumer response to the sharing of energy data.
- Understand how trustworthy and privacy-preserving the sharing of energy data is perceived to be.
- Understand if simplifying the Consent Flow has any impact on the quality of consent, trustworthiness, propensity to share, and confidence (see findings on [Simplified Consent](#) for more information).

What we found out: See R1/R2 report

- Participants expect data requests to be specific and relevant to the use case (pg 22)
- Some participants were uncomfortable with sharing certain permissions (e.g. occupation, physical address, payment information in energy datasets) (pg 19, 22)
- Sensitive data can cause aversion, and what is seen as 'sensitive' depends on the person (pg 22)
- Occupation was also seen as irrelevant data for sharing in energy use cases. (p.22)

We propose:

- Fine-grained control should be driven by ADR use cases; this should allow ADRs to further minimise the data they are requesting (pg 22)
- For energy, payment, hardship, and concession details should be separated from other authorisation scopes so ADRs can provide a clear and distinct reason for requesting them (pg. 22)

Proposed next steps:

- Consider how to facilitate data minimisation based on ADR use cases

Research approach

1. What did we want to find out?
2. Who did we research with?
3. What did we do?

RESEARCH APPROACH

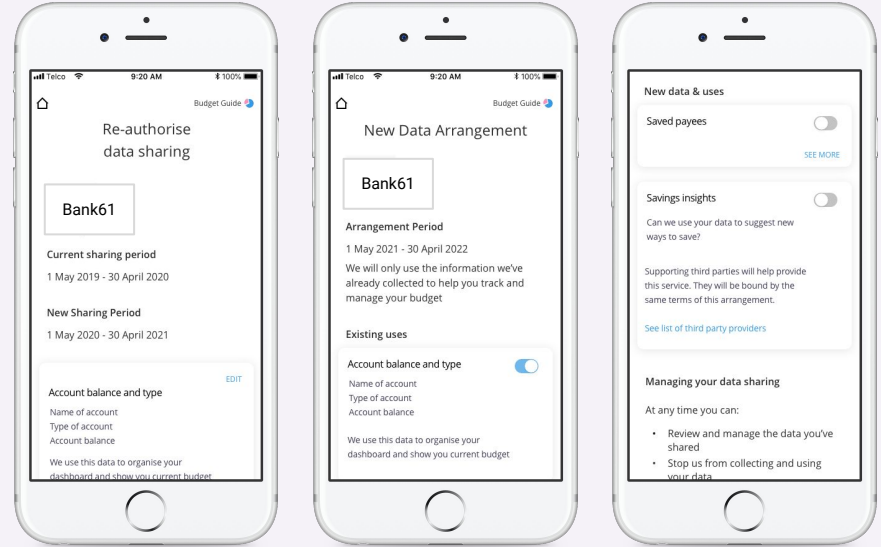
What did we want to find out?

We used a qualitative approach with 23 participants in 1:1 research sessions that ran for 60 minutes each.

For **Amending consent**, we wanted to:

- Provide consumers with the ability to amend consent while remaining empowered and in control.
- Provide consumers with simplified consent/amendment flows without compromising the quality of consent (or, while facilitating high quality consent).
- Understand what consumers expect to happen if/when they don't re-authorise.
- Understand the consumer's ability to recall the terms of the original consent.
- Understand if 'actively select' has any bearing on data cluster engagement/recollection ability.


Our research approach can be found on the [Consumer Data Standards website](#).



RESEARCH APPROACH

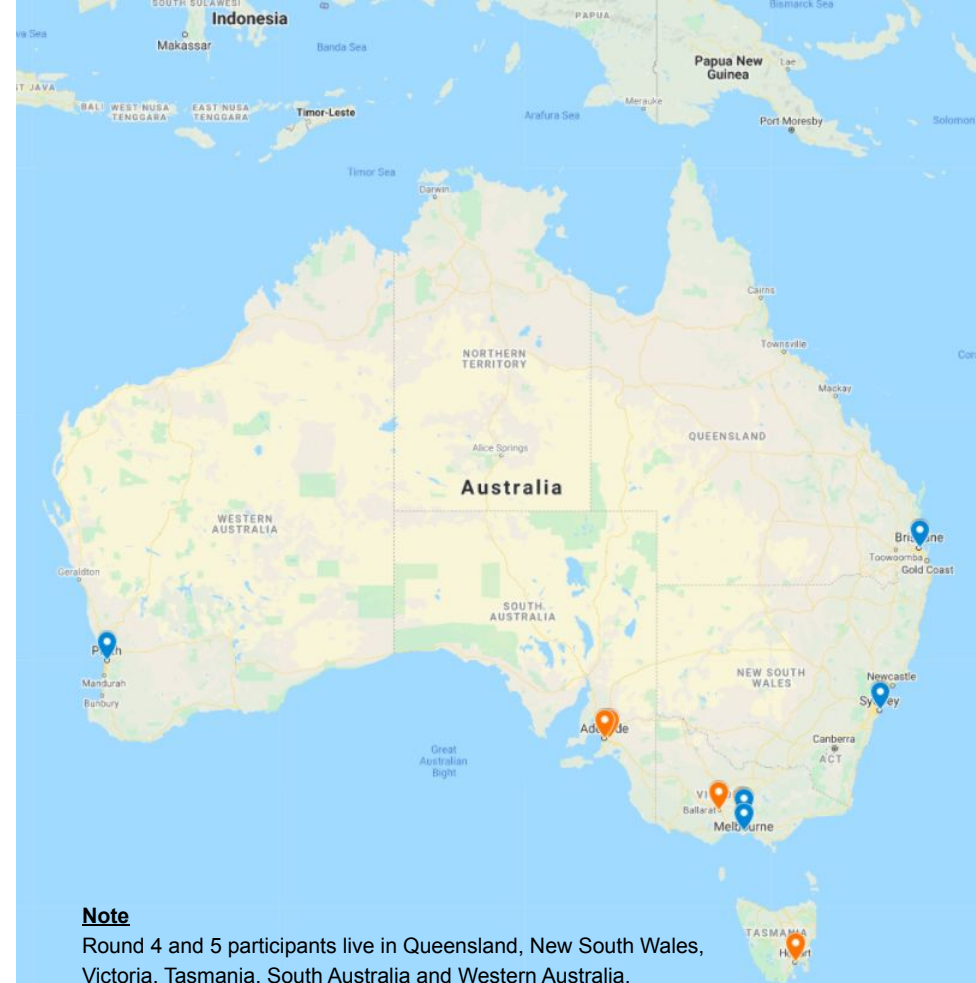
Who did we research with?

A broad and diverse range of participants were recruited to help reduce bias and research out risk. A 'no edge cases' approach has been taken; deeming certain groups and needs as not important is antithetical to the design of an inclusive CDR. Instead of focusing on those who are already likely and able to adopt CDR, the research focuses on removing the barriers to CDR being inclusive and accessible, which will make CDR easier and simpler to access for everyone.

The recruitment process strives to reflect the demographic percentages outlined in the [Australian Bureau of Statistics 2016 Census Data](#) , and explicitly recruits those who may be experiencing vulnerability or disadvantage.

Participants have varying levels of:

- Digital, financial, and data literacies and experiences
- Privacy awareness
- Confidence in the English language
- Trust in Government and commercial organisations



RESEARCH APPROACH

Who did we research with?

Round 4



R4P1

Unspecified, 61-70 years
QLD - Metro



R4P7

Female, 31-40 years
SA - Metro



R4P2

Male, 18-30 years
NSW - Metro



R4P8

Female, 18-30 years
NSW - Metro



R4P3

Female, 41-50 years
VIC - Suburban



R4P9

Male, 41-50 years
VIC - Metro



R4P4

Male, 71+ years
VIC - Suburban



R4P10

Male, 31-40 years
NSW - Metro



R4P5

Female, 41-50 years
VIC - Large town



R4P11

Female, 18-30 years
NSW - Suburban



R4P6

Male, 51-60 years
SA - Suburban



R4P12

Male, 31-40 years
TAS - Suburban

Round 5



R5P1

Female, 31-40 years
NSW - Metro



R5P7

Female, 61-70 years
VIC - Metro



R5P2

Female, 18-30 years
QLD - Metro



R5P8

Female, 18-30 years
VIC - Suburban



R5P3

Female, 51-60 years
VIC - Suburban



R5P9

Male, 41-50 years
WA - Metro



R5P4

Male, 61-70 years
NSW - Metro



R5P10

Female, 31-40 years
SA - Suburban



R5P5

Female, 31-40 years
WA - Large town



R5P11

Male, 41-50 years
VIC - Metro



R5P6

Female, 31-40 years
VIC - Metro

Engagement with participant:

- 3x times
- 2x times
- 1x time



Identity and diversity

- 4 have non-English speaking backgrounds
- 8 have migrated to Australia from another country
- 2 have accessibility needs
- 1 is of Aboriginal and/or Torres Strait Islander descent
- 6 identify as LGBTIQ+



Financial situation

- 14 are financially comfortable
- 7 have unstable financial situations
- 6 rely on a government allowance
- 5 have had extended periods of financial distress in their life



Level of financial literacy

- 6 have low financial literacy
- 11 have medium financial literacy
- 6 have high financial literacy



Level of digital literacy

- 1 has low digital literacy
- 11 have medium digital literacy
- 11 have high digital literacy



Level of privacy awareness

- 5 have low privacy awareness
- 10 have medium privacy awareness
- 8 have high privacy awareness

Session overview and prototypes

What did we do?

A qualitative approach was used to test low fidelity prototypes and to understand existing behaviours, expectations, and needs. Each session involved in-depth one-on-one interviews with participants for 60 minutes each.

To begin, we asked participants to recall the terms of their 'original' consent. We then gauged their expectations, behaviours, and needs in relation to data sharing while interacting with 'amending consent' prototypes. Upon completion, participants completed a form on comprehension to gauge their ability to recall the terms of their amended consent, followed by a series of questions on trustworthiness, perceived benefits of the use case, and their propensity to share data.

1 Interview:

Recall and comprehension of 'Original consent'

Can you tell me a little about the 'banking' task you completed?

- Who you shared data FROM and WITH?
- Why did you share that information? What was the benefit?
- What kind of data did you share?
- How long were you sharing data for?
- How would you stop sharing data?
- What happens to your data once you stop sharing?

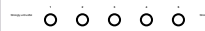
2 Form:

Trust, Benefit and Comfort

Let's say you're interested in saving money and managing your finances. You've been using a budgeting app that brings together a few of your financial accounts. By sharing your bank data with the app, they have been able to help reduce your spending and save more money. After a year of use, the app sends you an email. They want to know if you would like to re-allow the app to collect and use your data. If you decide to re-allow data sharing, the app will keep tracking your finances and suggest money-saving tips. If you decide NOT to re-allow data sharing, the app will no longer track your finances and will delete the data that you had shared before.

What level of trust do you have in this situation?

1-Strongly untrustful 2-Untrustful 3-Neutral 4-Trustful 5-Strongly trustful

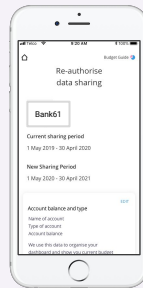


Why have you given this rating?

Long answer text

3 Prototype and Interview:

Amending consent



4 Form:

Comprehension of 'Amended consent'

I've shared data from [Bank 1] with [Budget Guide] so that I can [reduce my credit card expenses].

I've chosen to share the following types of data [data category or information].

The sharing period for my data is [4 months].

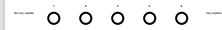
I might want to stop sharing my data because of [reason].

If I want to stop sharing my data I can do this by [clicking the 'Stop' button or the 'Stop' button on the 'Stop' page].

After I stop sharing my data, my data will be [deleted or de-identified].

How capable did you feel to stop sharing your data with Budget Guide?

1-Not very capable 2-Not capable 3-Neutral 4-Capable 5-Very capable



5 Form:

Trust and Propensity to share data

How much trust do you place in the process you've just been through?

1-Strongly untrustful 2-Untrustful 3-Neutral 4-Trustful 5-Strongly trustful



What changes to the experience could be made to increase your levels of trust?

Long answer text

Using the image as a reference, where would you place [the ADR's product]?



RESEARCH APPROACH

'Duration extended' experience

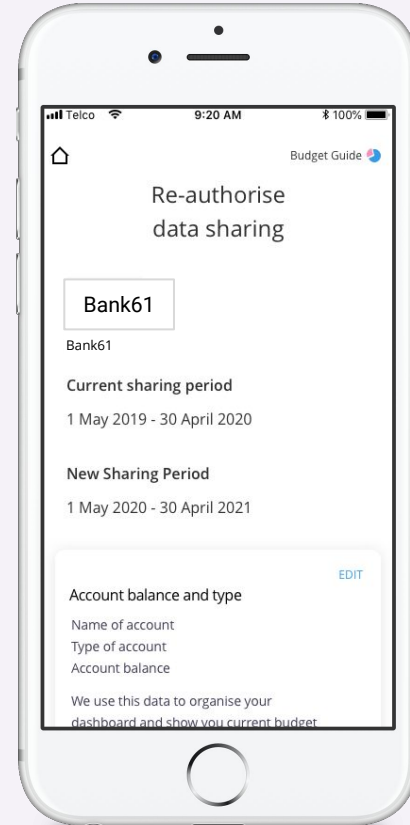
Prototype focus

- Amending consent, specifically in relation to extending consent duration, and removing datasets.
- Unspecified OSP involvement

Scenario

- Budget Guide, an ADR, is a budgeting app that allows consumers to save money and manage their finances. Real-world bank is the DH.
- Consumers are presented with a trigger email reminding them of their original consent expiry and the benefit to date.

View 'Duration extended' prototype



RESEARCH APPROACH

'Separation of collection and use' experience

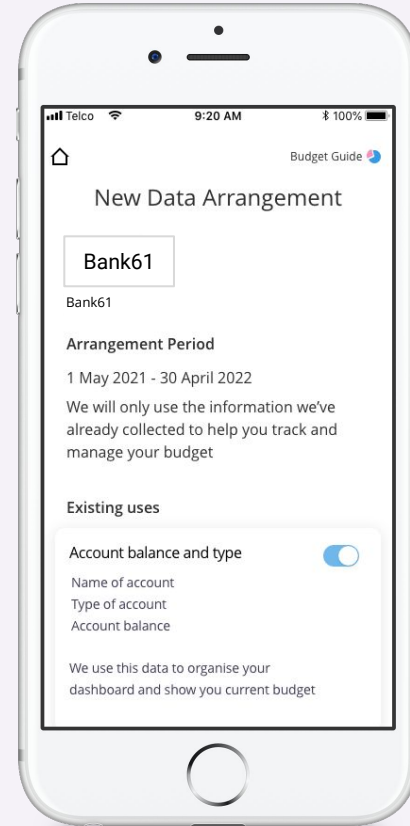
Prototype focus

Amending consent, specifically when disclosure expires and use continues.

Scenario

- Budget Guide, an ADR, is a budgeting app that allows consumers to save money and manage their finances. Real-world bank is the DH.
- Consumers are presented with a trigger email informing them that their original consent has lapsed. They are presented with the option to provide consent for 'use only.'

[View 'Separation of collection and use' prototype](#)



RESEARCH APPROACH

'Add or remove data and uses' experience

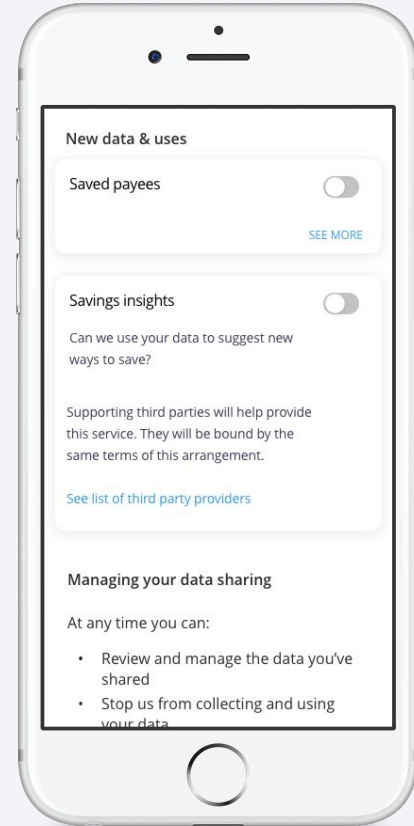
Prototype focus

- Amending consent, specifically in relation to adding and removing new data sets or uses.
- Explicit OSP involvement, i.e. to provide a feature
- OAIC's role in complaint handling

Scenario

- Budget Guide, an ADR, is a budgeting app that allows consumers to save money and manage their finances. Real-world bank is the DH.
- Consumers are presented with a trigger email reminding them of their original consent expiry and the benefit to date.

View 'Add or remove data and uses' prototype



RESEARCH APPROACH

Trustworthiness and Propensity to share

From consumer-participants, we wanted to understand:

- How trustworthy do they deem the CDR and its actors to be?
- What increases or decreases their propensity to share CDR data?

To answer these questions, participants completed a form containing a series of questions relating to trustworthiness, comprehension and their propensity to share data (adapted from [Greater than X's Phase 2 research](#)). Participants were asked to:

1. Mark their response using the **Likert scale** with a score from 1 to 5. '1' being a negative indicator, '3' being a neutral indicator, and '5' being a positive indicator.
2. Provide **open-ended responses** to more subjective questions.
3. Plot the tested use-case on a **Trust/Benefit scale** (adapted from [New Zealand's Data Futures Partnership](#)).

1
How much trust do you place in the process you've just been through?

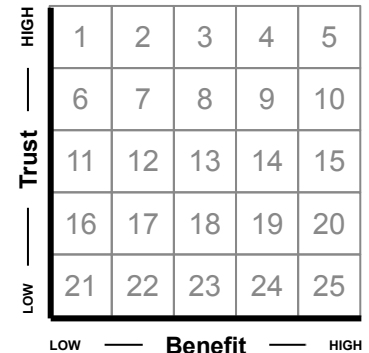
1-Strongly untrustful, 2-Untrustful, 3-Neutral, 4-Trustful, 5-Strongly trustful



2
What changes to the experience could be made to increase your levels of trust?

Long answer text

3
Using the image as a reference, where would you place [the ADR's product]?



Informed consent and Comprehension

Participants had to recall their consent terms multiple times. They were asked to recall:

- Who they were sharing data from and with (DH and ADR),
- Why they were sharing their data (perceived benefit),
- What types of data they elected to share,
- How long they were sharing data for (sharing period),
- Why they might stop sharing (risks or concerns),
- What happens if they stop sharing data,
- How they might stop sharing their data, and
- What would happen to their redundant data

When recalling original consent (after time), participants were verbally asked the above questions. Assessment and scoring was by proxy.

Directly after the Consent and Amending consent flows, participants were given a “fill in the blanks” style comprehension sheet to assess their understanding and memory of the prototype and task they had just completed.

I've shared data from [DH] with [ADR] so that I can [benefit/product purpose].

I've chosen to share the following types of data [data clusters or permissions].

The sharing period for my data is [12 months].

I am aware that by sharing this data I could risk the following [risks or concerns].

Some disadvantages of not sharing this data could be [consequence].

If I want to stop sharing my data I can do this by [contacting the ADR/DH or the ADR/DH Dashboard>Settings].

After I stop sharing my data, my data will be [deleted or de-identified].

Key insights for **Amending consent**

Consumer attitudes and experiences when amending an existing consent.

Broad understanding of 'renewal' process

Participants understood the re-authorisation/renewal proposition and easily completed tasks associated with the 3 scenarios presented.

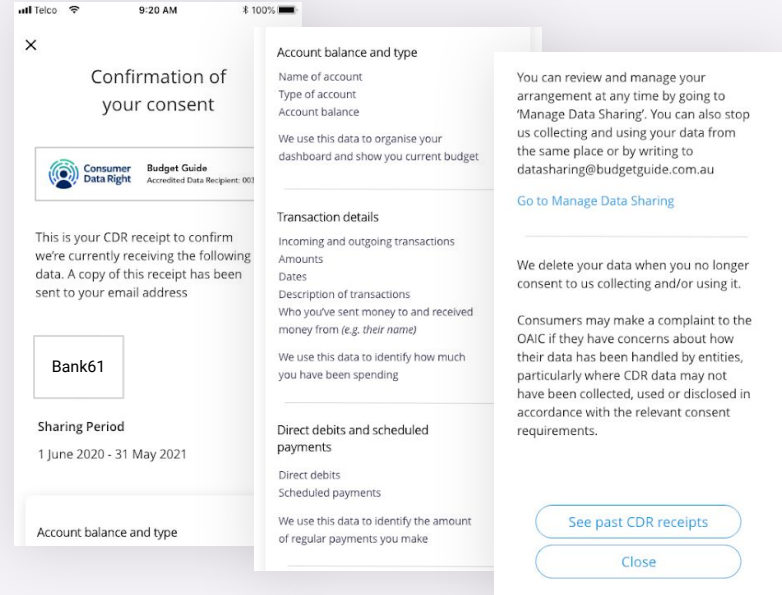
Participants expected that not acting on the notification would result in the expiry of their data sharing arrangement.

Some participants expected a clearer 'withdraw consent' option when reviewing the existing arrangement and also expected to see the bank accounts they were currently sharing.

Upon completion participants were provided with a CDR Receipt, which included the ability to 'See past CDR Receipts'. Participants generally understood that this would allow them to access a record or history of consents they had provided.

Research objective

F1: Provide consumers with the ability to amend consent while remaining empowered and in control



Recommendation

- Communicate that consent will expire if the request is not actioned
- Provide a clear 'withdraw consent' option in addition to allowing expiry by default
- ADRs should show which accounts data has been collected from - on CDR receipts, dashboards, and amending consent requests - and consumers should be able to initiate a process to add/remove accounts from the consent
- ADRs should provide a 'consent history' to allow consent changes to be tracked

AMENDING CONSENT

‘Re-authorisation’ or ‘renewal’ seen as a positive change

The need to ‘re-authorise’ or ‘renew’ consent is seen as positive and trust-building.

In contrast to existing data sharing experiences, where the onus is on the individual to opt-out, CDR’s finite sharing period and the requirement for consumers to actively consent to ongoing collection and use is seen as both empowering and transparent.

Research objective

F1: Provide consumers with the ability to amend consent while remaining empowered and in control

”

I think companies that are proactive about the data they're holding from you just seem more transparent, like I'm more aware that they've got my data and they're checking in to see that I still want them to have my data, and that's good for me as a consumer because I would forget that I have consented to give my data to an app.

— R5P8

I like that it does not automatically renew and you are reminded of how to stop sharing at regular points.

— R5P2

AMENDING CONSENT

Interest and motivation to renew tied to benefit

As has been noted with past rounds of research, the perceived benefit of a use case plays an important role in a participant's willingness to provide consent.

When deciding whether or not to provide their consent to extend or amend an existing consent, participants expressed the critical importance of understanding what benefits the service has provided first.

Research objective

F1: Provide consumers with the ability to amend consent while remaining empowered and in control

”

I'm still willing to crack on. I'll save 1500 dollars so I'm still willing to. My willingness is implied... the willingness is implied in everything I've done.

— R5P9

That's awesome that outlines what its benefits are and what its done for me specifically.

— R5P2

Recommendation

ADRs should present the realised benefits of data sharing as part of amending consent requests so consumers can assess the material value of providing consent.

AMENDING CONSENT

Consequences of expiry equally as important as benefits for continued sharing

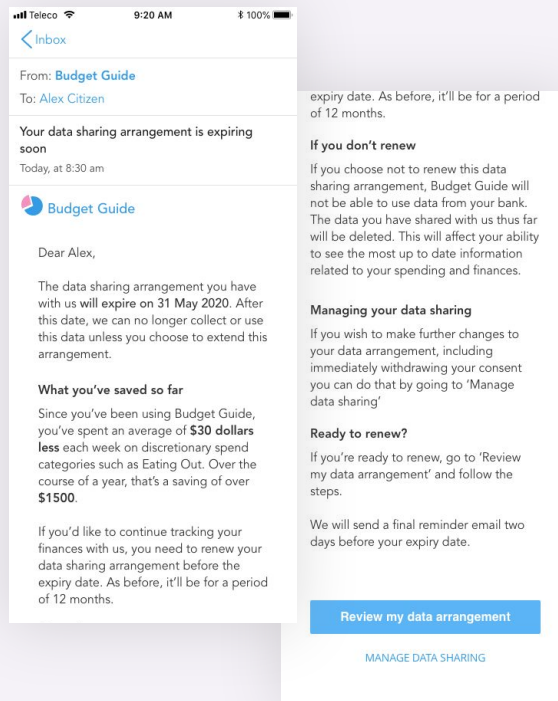
Participants recognised that their service would be impacted if they did not provide consent to amend or continue an existing consent. This included the ability to access things such as ‘historical insights’ or ‘past trends’.

Participants also expressed re-assurance when seeing data handling procedures outlined, giving them trust and confidence that their data preferences would be honoured.

To make an informed decision, it was important for participants to understand what would happen if they did not provide consent, including how it would impact their existing service.

Research objective

F3: Understand what consumers expect to happen if/when they don't re-authorise.



Recommendation

ADRs should outline the consequences of not continuing to consent - such as service or data loss. This should include information about how data will be handled if re-consent is not provided.

AMENDING CONSENT

Broad expectation for reminder mechanism to warn of expiry

Participants expressed both a high expectation and appetite for receiving reminders to warn them that their consent was about to expire.

Similar to renewal reminders in other industries, participants see the reminder as an opportunity to take action to prevent unintended loss of service and, in the case of CDR, deletion or de-identification of data.

There was also a broad expectation that if the first reminder was ignored there would be at least one follow-up reminder before consent expired.

Research objective

F1: Provide consumers with the ability to amend consent while remaining empowered and in control

”

I guess you would be re-sending me an email, like, you know, maybe a day before, two days before, like just a heads up to, you know, entice me to re-sign [re-authorise]

— R5P1

Recommendation

ADRs should provide multiple reminders to warn consumers that their consent is about to expire. Such reminders should not be sent at unnecessarily high frequencies so as to cause notification fatigue.

AMENDING CONSENT

Limited value and trust seen in use-only consent

Participants were presented with a use-only consent to retain financial insights after an existing disclosure had expired.

The value of a use-only consent was not recognised by most participants as they expected only up-to-date data to be relevant.

Participants also questioned why the ADR would be holding on to data that should be deleted upon expiry, noting that they did not consent to it being kept for longer than 12 months.

The use-only prototype omitted both the authentication and authorisation steps from the Consent Flow. There were particular concerns around the DH being omitted not just from the authorisation step but the entire flow. The data was still associated with the DH even though authentication is not required for use.

Research objective

F1: Provide consumers with the ability to amend consent while remaining empowered and in control

F2: Provide consumers with simplified consent/amendment flows without compromising the quality of consent (or, while facilitating high quality consent).

”

I'm kind of surprised that I didn't have to sign in again. Because I technically no longer am consenting to use it within that period. I feel that I would have to re-sign in to keep giving them access.

— R4P11

Recommendation

- Consider the separation of collect/use as part of the ADR withdrawal flow
- The scenarios for collection and use separation, and use-only consents need to be better understood, as well as an outline of how these use cases are currently supported/not supported.
- Disclosure-only withdrawals should be revisited once use cases are better defined.
- DH presence in the consent flow is important for developing trust in the process even if the consumer has low levels of trust in the DH. This is because the DH is seen as an authoritative and legitimate actor.

AMENDING CONSENT

‘Pre-selected’ datasets do not reduce amending consent quality

Participants understood that pre-selected datasets and uses reflected originally consented to components. No decrease in the quality of consent was observed for the ‘pre-selected’ design pattern.

Participants were able to accurately describe the process they had been through and could accurately recall the datasets and uses they had consented to.

Prototype limitations meant that the 'Authorisation' and 'CDR receipt' screens did not always reflect what a participant consented to. Most participants noticed this and questioned the discrepancies between their chosen terms and these summary screens, suggesting a high level of engagement even in the absence of needing to actively select datasets and uses.

Research objective

F2: Provide consumers with simplified consent/amendment flows without compromising the quality of consent

F5: Understand if 'actively select' has any bearing on data cluster engagement/recollection ability.

The 'Edit' design pattern shows a form with three sections: 'Account balance and type', 'Transaction details', and 'Direct debits and scheduled payments'. Each section has a list of items and a brief description of their use. The 'Account balance and type' section includes 'Name of account', 'Type of account', and 'Account balance'. The 'Transaction details' section includes 'Incoming and outgoing transactions', 'Amounts', 'Dates', 'Description of transactions', and 'Who you've sent money to and received money from (e.g. their name)'. The 'Direct debits and scheduled payments' section includes 'Direct debits'. An 'EDIT' button is located in the top right corner of the form.

“Edit” design pattern used in ‘Duration extended’ prototype

The 'Toggle' design pattern shows a form with three sections: 'Existing uses', 'Transaction details', and 'Direct debits and scheduled payments'. Each section has a list of items and a brief description of their use. The 'Existing uses' section includes 'Account balance and type', 'Name of account', 'Type of account', and 'Account balance'. The 'Transaction details' section includes 'Incoming and outgoing transactions', 'Amounts', 'Dates', 'Description of transactions', and 'Who you've sent money to and received money from (e.g. their name)'. The 'Direct debits and scheduled payments' section includes 'Direct debits'. Each section has a toggle switch in the top right corner.

“Toggle” design pattern used in ‘Separation of collection and use’ and ‘Add or remove data and uses’ prototypes

Recommendation

For subsequent consent requests, allowing pre-selected datasets and uses for amending consent:

- Simplifies the consent flow
- Does not reduce engagement with datasets and uses
- Does not compromise the quality of consent

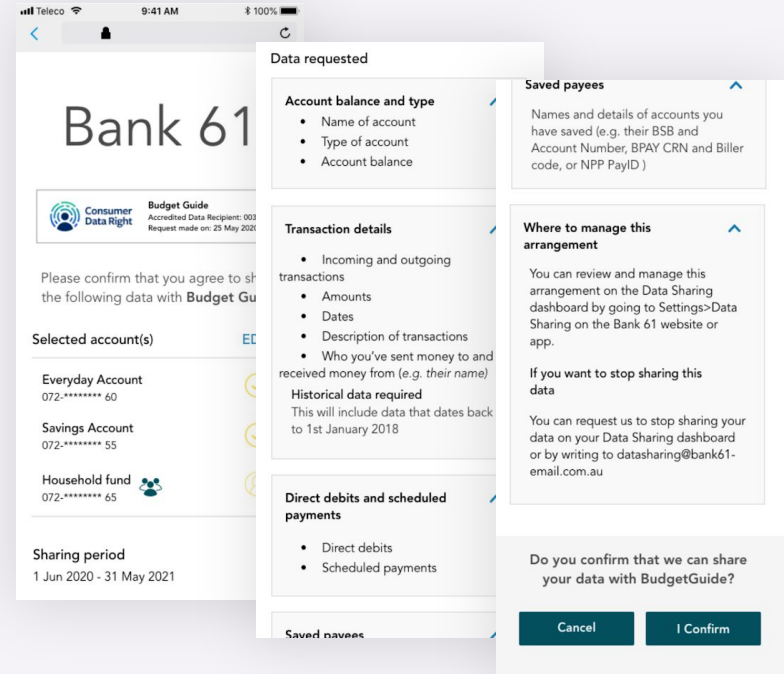
AMENDING CONSENT

Removing ‘authorisation’ did not impact comprehension or trust

For re-authorisation, where only the duration of an existing consent was being amended, we experimented with simplification by conflating the authentication and authorisation step.

Omitting the authorisation steps had no impact on the quality of consent or trust. Participants successfully completed the task with a high level of comprehension and recollection ability.

The presence of the participant’s DH plays a key role in creating trust in the process. For this prototype the DH appeared in the authentication step only, and this did not erode trust or informed consent. This differed to use-only consents where the absolute omission of the DH raised concerns.



Research objective

F2: Provide consumers with simplified consent/amendment flows without compromising the quality of consent (or, while facilitating high quality consent).

Recommendation

The authorisation flow could be omitted without compromising trust or consent quality, but this should only be considered where the only change to the consent is the duration of collection and use. Further research should be conducted to understand how this does or does not apply to other amending consent scenarios, such as adding/removing datasets and accounts.

AMENDING CONSENT

Ability to recall original consent varied

Participants could, on average, **recall the terms of their original consent with 78.3% accuracy**:

- **11 out of 23** participants recalled their original consent with **100% accuracy**
- **7 out of 23** participants scored **71-86%**
- **3 out of 23** participants scored **43-57%**
- **2 out of 23** participants scored **0-14%**

Generally, participants were able to recall the following terms of their original consent accurately:

- What would happen to their redundant data
- How to manage or revoke data sharing
- Who they were sharing their data from

Research objective

F4: Understand the consumer's ability to recall the terms of the original consent.

D3: Understand how informed consumers are when/after they have given consent.

”

It involved connecting to a bank. It involved a finance app, budgeting and planning.

Share information (account balance, transaction history, pending transactions) for the year and follow trends in spending behaviours and so forth.

Can stop sharing in settings, in the app to stop it.

There were two options either delete information entirely or just have it anonymised and used for research purposes.

— R5P11

AMENDING CONSENT

Recollection improved after amending consent

Participants had to recall their consent terms multiple times:

1. After completing the consent flow (their original consent)
2. During the session, we recapped the original consent
Note: Participants had previously completed the consent flow between one day to one month before the research session
3. After completing the amending consent flow

Averages remained similar for original consent (78.9%) and recalling original consent (78.3%).

However, after completing the amending consent flow, on average, participants were able to recall the terms of their consent with 94% accuracy, demonstrating a 16% improvement.

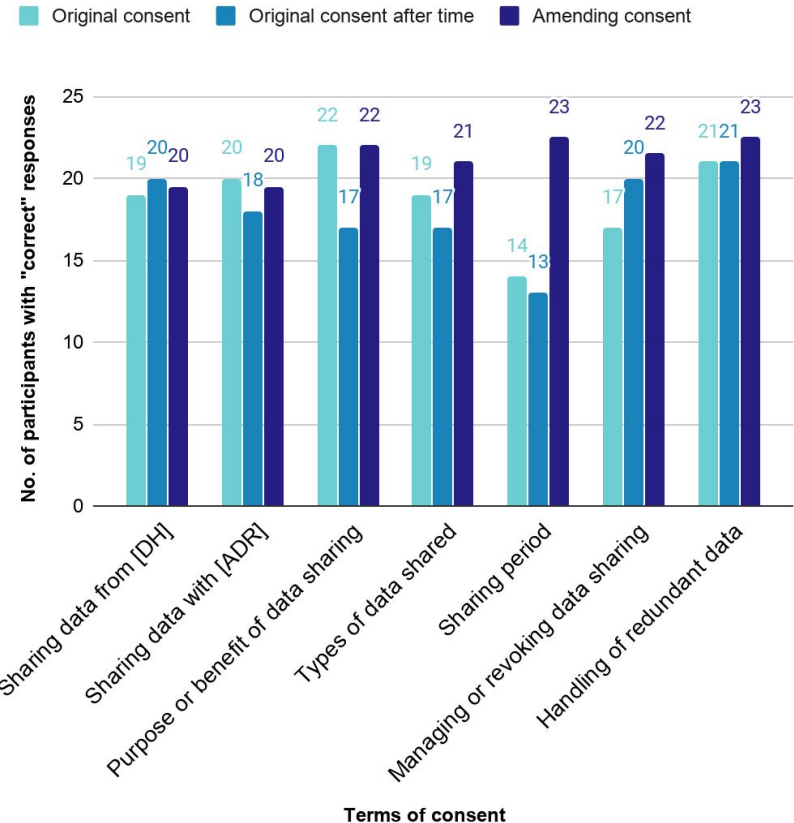
This suggests that familiarity with consent increases through repeated interactions with consent flows, helping consent remain current and informed.

Research objective

F4: Understand the consumer's ability to recall the terms of the original consent.

D3: Understand how informed consumers are when/after they have given consent.

Recalling terms of consent



AMENDING CONSENT

Participants recalled a mix of data clusters and permissions

When asked to recall what data they shared in their original consent most participants described **data clusters and permissions**, i.e. "Things like the account type, account information, account balances and transactions."

Some participants described their shared data at an **account level**, i.e. "sharing data from my joint account", while other participants simply referred to "bank data."

Research objective

- F4: Understand the consumer's ability to recall the terms of the original consent.
- D3: Understand how informed consumers are when/after they have given consent.

”

Current account and the savings accounts. Name, account number, transaction details.

— R4P8

Personal data, transactions and balance. The basic information you will find on a statement.

— R4P10

I just clicked on direct debits.

— R5P9

What I was sharing in there, yeah that's going to be hard. Bills?

— R4P7

Recommendations:

Post-go live research should be conducted with consumers using real world CDR services; these should use the same CX measures to assess consent quality, trustworthiness, and perceived benefit.

AMENDING CONSENT

Continual consideration of benefit and privacy while amending consent

This research continued to show that a participant's willingness to share their data was tied to the benefit they saw in the use case. Outlining the benefits realised in the last 12 months of data sharing helped participants assess the value of continuing to share their data.

All participants decided to continue sharing the pre-selected terms when amending consent, understanding the benefit to be directly tied to the datasets they had already shared.

Participants were also presented with unselected datasets and uses, and most participants actively decided against adding these as they either:

- Didn't see value in sharing this information, or
- Had concerns about privacy

Research objective

F5: Understand if 'actively select' has any bearing on data cluster engagement/recollection ability.

The screenshot shows a mobile-style interface for managing consent. It is divided into two main sections: 'Existing data' and 'New data & uses'. Under 'Existing data', there are three items: 'Account balance and type' (toggle on), 'Transaction details' (toggle on), and 'Direct debits and scheduled payments' (toggle on). Each item has a 'SEE MORE' link. Under 'New data & uses', there are two items: 'Saved payees' (toggle off) and 'Savings insights' (toggle off). The 'Savings insights' item has a sub-question: 'Can we use your data to suggest new ways to save?' and a note: 'Supporting third parties will help provide this service. They will be bound by the same terms of this arrangement.' Below this is a link: 'See list of third party providers'.

”

If I was going to be signing up for another year, that's information that you need... because they kind of need to know that stuff to budget your life.

I don't think they need Saved payees. I think that's their privacy and not mine... So I probably wouldn't tick that.

Savings insights. I'm just going to see the list of third party providers... I think they already have enough information to know ways for me to save...

— R5P6

Recommendations:

ADRs should distinguish between 'new' and 'existing' terms of consent. Consideration should be given to permitting 'pre-selected' datasets and uses for amending consent requests to facilitate this distinction.

Amending consent value propositions should clearly outline the material outcomes of past data sharing.

AMENDING CONSENT

Low knowledge of CDR does not impact overall trust in the process

Most participants were familiar with the term 'Consumer Data Right' and 'CDR', but were not able to describe CDR in detail. 'CDR' was commonly described as a "government standard" with "some kind of certification." Some participants also associated CDR with "privacy" and "data protection."

Before the consent flow, participants were given with the option to explore additional CDR Education, via a mock landing page with an 'About' and 'FAQs'. Engagement with this page did not affect a participant's ability to recall or describe CDR.

While CDR awareness had some influence over CDR trust, some participants had inherent and overwhelming concerns about privacy and data sharing regardless of how and where it occurred.

Research objective

F4: Understand the consumer's ability to recall the terms of the original consent.

D1: Understand if and how knowledge of CDR shapes trustworthiness and propensity to share.

Participant	Viewed CDR Education	Can recall term 'CDR'	Can describe term 'CDR'	Trust with 'CDR'
R5P1	✗	✓	✗	5-Strongly trustful
R5P2	✓	✗	✗	4-Trustful
R5P3	✗ *	✗	✗	4-Trustful
R5P4	✓	✗	✗	3-Neutral
R5P5	✗	✓	✗	4-Trustful
R5P6	✗	✓	✓	4-Trustful
R5P7	✗ *	✗	✗	2-Untrustful
R5P8	✓	✓	✓	5-Strongly trustful
R5P9	✗	✓	✗	4-Trustful
R5P10	✓	✓	✓	4-Trustful
R5P11	✓	✓	✓	4-Trustful

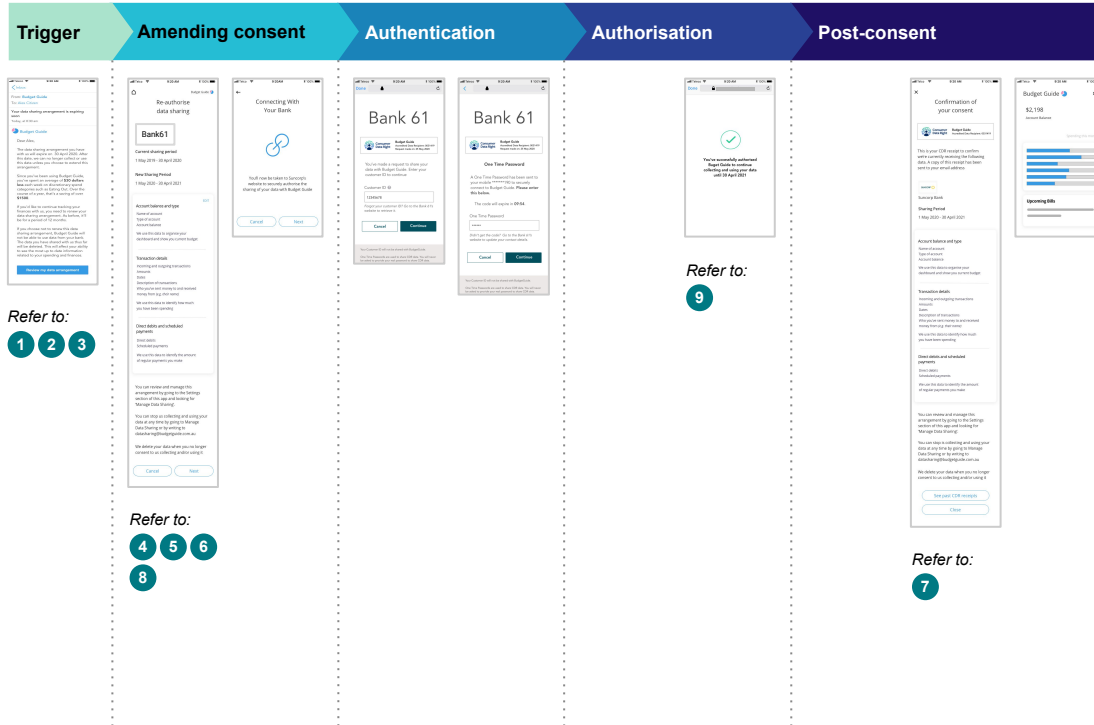
* While R5P3 and R5P7 have not viewed CDR Education, they have been exposed to the Consent Flow multiple times.

Recommendations

Experience overview and recommendations for:

- Simplified re-authorisation ('Items 1, 7')
- Separation of collect/use ('Items 3, 5, 6, 7')
- Add/remove datasets ('Item 2')

Duration extended



General 'amending consent' recommendations

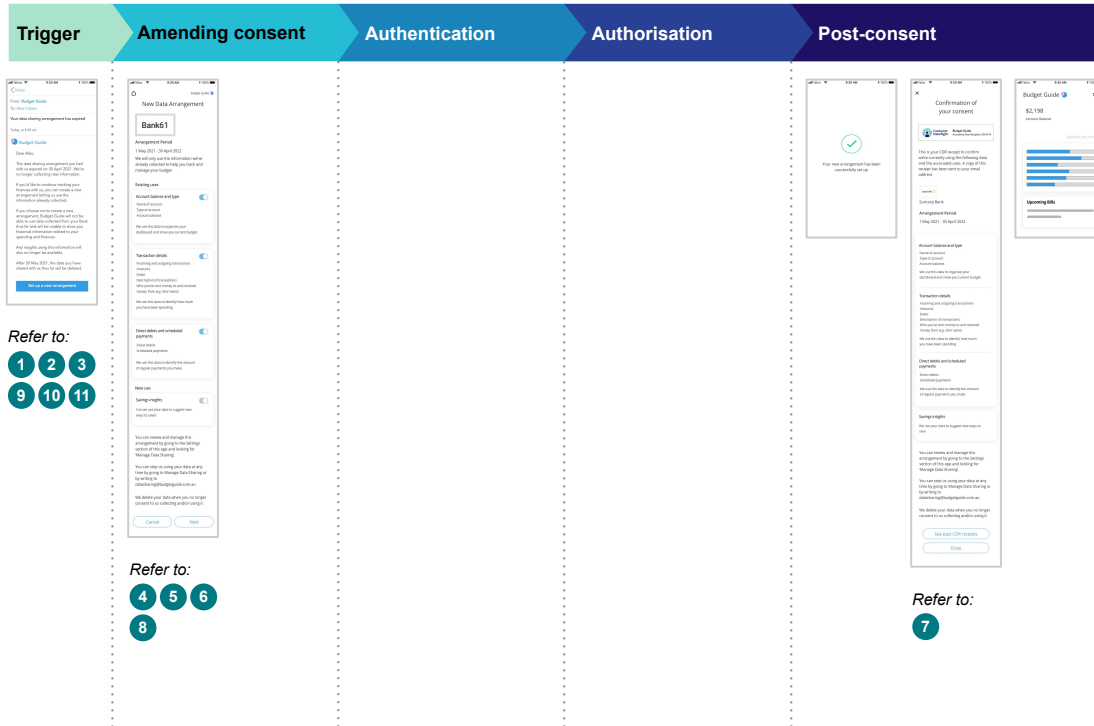
1. Expiry notifications should be timely and include follow-up reminders | [Insight on pg 31 and 35](#)
2. The realised benefits of data sharing should be shown to consumers before they re-consent | [Insight on pg 33](#)
3. Redundant data handling information should be re-surfaced | [Insight on pg 34](#)
4. Consider dropping 'actively select' requirement for previously consented to datasets and uses | [Insight on pg 37](#)
5. Provide transparency around the benefits and outcomes of data sharing, and distinguish between 'new' and 'existing' consents for datasets and uses | [Insight on pg 42](#)
6. Provide a 'consent history' to allow changes to be tracked | [Insight on pg 31](#)
7. Conduct consent quality research with consumers using real world ADRs | [Insight on pg 39, 40 and 41](#)

Simplified re-authorisation recommendations

8. The authorisation flow could be omitted without compromising trust or consent quality, but this should only be considered where the only change to the consent is the duration of collection and use. Further research should be conducted to understand how this does or does not apply to other amending consent scenarios, such as adding/removing datasets and accounts | [Insight on pg 38](#)
9. Further exploration and clarity needs to be provided for re-authorisations when '2 to authorise' preferences for joint accounts are in place

AMENDING CONSENT — RECOMMENDATIONS

Separation of collection and use



General 'amending consent' recommendations

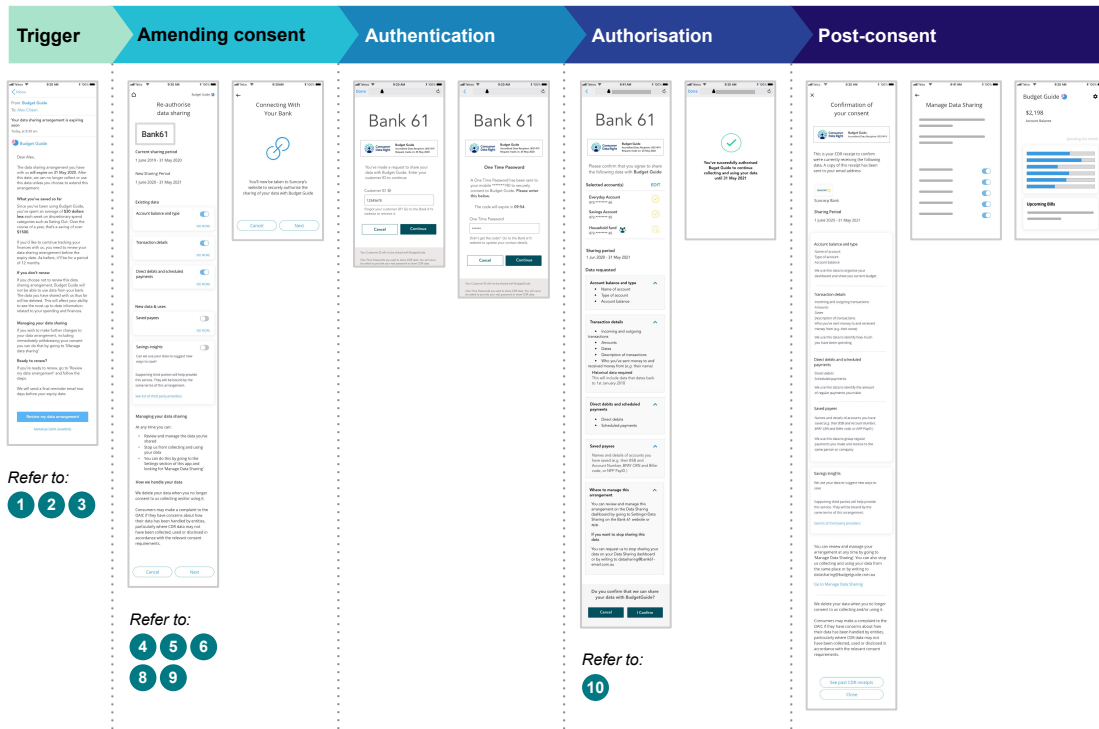
1. Expiry notifications should be timely and include follow-up reminders | [Insight on pg 31 and 35](#)
2. The realised benefits of data sharing should be shown to consumers before they re-consent | [Insight on pg 33](#)
3. Redundant data handling information should be re-surfaced | [Insight on pg 34](#)
4. Consider dropping 'actively select' requirement for previously consented to datasets and uses | [Insight on pg 37](#)
5. Provide transparency around the benefits and outcomes of data sharing, and distinguish between 'new' and 'existing' consents for datasets and uses | [Insight on pg 42](#)
6. Provide a 'consent history' to allow changes to be tracked | [Insight on pg 31](#)
7. Conduct consent quality research with consumers using real world ADRs | [Insight on pg 39, 40 and 41](#)

Separation of collect/use recommendations

8. The scenarios for collection and use separation and use-only consents need to be better understood, as well as an outline of how these use cases are currently supported/not supported | [Insight on pg 36](#)
9. Consider the separation of collection/use as part of the ADR withdrawal flow [Insight on pg 36](#)
10. Disclosure-only withdrawals from DH dashboards should be revisited once use cases are better defined | [Insight on pg 36](#)
11. DH presence in the consent flow is important for developing trust in the process even if the consumer has low levels of trust in the DH. This is because the DH is seen as an authoritative and legitimate actor | [Insight on pg 36](#)

AMENDING CONSENT — RECOMMENDATIONS

Add or remove data and uses



General 'amending consent' recommendations

1. Expiry notifications should be timely and include follow-up reminders | [Insight on pg 31 and 35](#)
2. The realised benefits of data sharing should be shown to consumers before they re-consent | [Insight on pg 33](#)
3. Redundant data handling information should be re-surfaced | [Insight on pg 34](#)
4. Consider dropping 'actively select' requirement for previously consented to datasets and uses | [Insight on pg 37](#)
5. Provide transparency around the benefits and outcomes of data sharing, and distinguish between 'new' and 'existing' consents for datasets and uses | [Insight on pg 42](#)
6. Provide a 'consent history' to allow changes to be tracked | [Insight on pg 31](#)
7. Conduct consent quality research with consumers using real world ADRs | [Insight on pg 39, 40 and 41](#)

Add/remove datasets recommendations

8. Surface 'withdraw consent' options at various stages in the amending consent process | [Insight on pg 31](#)
9. ADRs should present accounts to consumers at various points, including on dashboards, CDR receipts, amending consent requests, and consumers should be able to initiate a process to add/remove accounts from the ADR side | [Insight on pg 31](#)
10. Further exploration and clarity needs to be provided for re-authorisations when '2 to authorise' preferences for joint accounts are in place

Key insights for Outsourced Service Providers (OSP)

Consumer attitudes towards Outsourced Service Provider involvement in CDR

OUTSOURCED SERVICE PROVIDERS

Relationship is with the ADR, not the OSP

In Round 4, participants were not made aware of any relationships between the ADR and OSPs. In this scenario, they believed that third parties could not access or mediate their CDR data by default.

In Round 5, participants were presented with the option to enable a 'Savings Insight' feature that would introduce an OSP into the process. Most participants understood this proposition and raised concerns about the ADR using an OSP.

Participants in both rounds initially expected only to be dealing with the ADR. While the ADR was trusted, this trust did not extend to OSPs. When given a choice, most participants preferred not to activate the 'Savings Insight' feature that would introduce OSPs and allow them to access or mediate their data.

There was an innate distrust towards OSP involvement which raised concerns about the ADR's trustworthiness and integrity.

Research objectives

D4. Understand if consumers have a propensity to share their data with the CDR.

F1: Provide consumers with the ability to amend consent while remaining empowered and in control.

”

If someone [third party] is behind this I think I should know... So far I haven't seen any other name than Budget Guide.

— R4P10

It would make me not rate Budget Guide as highly. That they will be shared onwards to a third party. There's a risk of that data being breached or how that data is being accessed.

— R4P9

Nah don't like it. They're doing it for a reason. They're doing it for market research. I feel like I'm being data mined. I don't see another reason for them being involved.

— R5P7

OUTSOURCED SERVICE PROVIDERS

Transparency is key

There was an expectation that any OSP involvement would be explicitly stated, and that explicit consent would be required.

Specifically, participants wanted to know:

- **Who the OSP was:** Depending on the reputation and ethics of the Outsourced Service Provider (OSP), participants said that they might stop sharing data and lose trust in the ADR.
- **How their data would be accessed and handled:** Participants wanted to know the level of control they would have over OSP access, mediation, and use.
- **Why the OSP was involved:** Participants wanted to understand how they would benefit from sharing with OSPs, and why the ADR had a relationship with them.
- **What the "trade-offs" were:** Participants wanted to know how the OSP benefitted from involvement, and sought additional assurance that their data would not be used in unintended ways.

Research objectives

D4. Understand if consumers have a propensity to share their data with the CDR.

F1: Provide consumers with the ability to amend consent while remaining empowered and in control.

”

I'd probably need to know who these people are. You always have to wonder. If they're getting your details for some kind exchange. I'd hope they were reputable companies I knew of already... Why do I need to let these guys have my information.

— R5P6

Recommendations

- ADRs should be transparent about OSP/intermediary involvement and present to the consumer the requirements detailed in Rule 7.2(4)(b)-(d):
 - A list of OSPs and their location;
 - The nature of the services they provide;
 - The data that may be disclosed to them;
 - Whether or not they are accredited
- This should also include what the OSP/intermediary is doing in relation to that specific consent and data, for example: collection; use; transformation; storage; de-identification; etc.

OUTSOURCED SERVICE PROVIDERS

Attitudes varied from cautiously 'okay' to strongly adverse

Most participants had an inherent aversion to OSP involvement. They had concerns around compliance and the handling of their data. While there was an understanding that the OSP would be "within the constraints of the CDR," they were not confident that OSPs would conform to the terms of the consent and CDR. Participants questioned the OSP's data retention policies and assumed that the OSP would on-sell their data to other companies.

While there was a reluctance to share personal data with third parties, some participants expressed more comfort if:

- the consumer benefit was clear,
- their data was "unnamed," and
- there was greater enforcement around OSP involvement

Research objectives

D4. Understand if consumers have a propensity to share their data with the CDR.

F1: Provide consumers with the ability to amend consent while remaining empowered and in control.

”

The moment I see supporting third parties will help provide this service straightaway, I'm going no.

—R5P9

It's a modern corporate world, I think it would be impossible not to, it couldn't function without outsourcing. It doesn't bother me so much. The rational choice is to turn it on or off... I would worry depending on how they were doing it that it would be susceptible to data mining.

— R4P4

I'd like to be asked about it. Because they have my email address and stuff, right. I don't want that to be linked to me. If it's going to be linked to me in any way. I want to know how it's being used.

— R4P3

Recommendations

ADRs should consider providing a high level of transparency, control, and certainty around OSP/intermediary involvement

Key insights for **Complaints Process**

Consumer attitudes and expectations around how complaints are made and handled

ROLE OF OAIC

Awareness of OAIC* is low, but trust in their ability to regulate is high

Although no participants were familiar with the term ‘OAIC’ (Office of the Australian Information Commissioner*), or awareness that the office existed, OAIC was broadly perceived to be a body that would regulate or oversee aspects of CDR compliance.

Some participants correctly believed that the OAIC would oversee privacy aspects of the CDR, but most participants interpreted OAIC’s role to be broad and not privacy specific.

Similar to previous rounds of research, the involvement of an independent entity to regulate CDR actors contributed to higher levels of trust in the process and also positively affected a consumer’s propensity to share data.

Research objectives

D2: We want to understand how trustworthy consumers deem the CDR

D4: Understand if consumers have a propensity to share their data with the CDR

”

All of those government things are in place, whether it's the financial regulators whatever. At some point, if it turned out they were dodgy at some point, I'd have some recourse. That was my assumption.

— R5P9

Definitely instills confidence in the app... these guys are kinda saying we're not going to do anything wrong and we've told the government and they've backed us on the fact that we're doing the right thing.

— R5P10

I think there always need to be a neutral body when it comes to private companies dealing with public.

— R5P5

Recommendation

- Information around OAIC involvement should be included in the CDR consent model, especially consent and amending consent flows
- Greater awareness of OAIC may also be helped by including overviews and educational content as part of CDR education campaigns

ROLE OF OAIC

High confidence that avenues of dispute and complaint resolution available

Most participants were unfamiliar with existing complaints processes but were confident that they could find the relevant information online if they needed to make a complaint in relation to the CDR.

Participants expressed high levels of trust in the OAIC's role and likened it to more familiar processes and terms such as various Australian ombudsman agencies.

Research objectives

D2: We want to understand how trustworthy consumers deem the CDR

D4: Understand if consumers have a propensity to share their data with the CDR

”

These days we just google it and try to find it on google. And it hopefully take you to the right place.

— R5P4

I guess if it was in the app, if the OAIC was pretty prominent in the app, but I would just probably Google it and go along with like, on my own journey with that.

— R5P2

I'm vaguely aware of telecommunication ombudsman and a lot of statute bodies... I imagine it would deal with a lot of the things we've talked about... unauthorised data sharing and so forth.

— R5P11

Recommendation

Where complaints information is referenced, it may be useful to provide brief explanations around consumer rights and how they may find more information regarding the complaints or disputes process

Key insights for **Trustworthiness and Propensity to share**

Consumer attitudes around trust and their propensity to share CDR data.





TRUSTWORTHINESS & PROPENSITY TO SHARE

Switching canvas

This switching canvas provides an overview of consumer behaviour and attitudes towards data sharing and CDR.

This includes aggregated themes from 7 rounds of consumer research with 71 participants over a 12 month period.

Note: Phase 3 themes have been tagged [R#], with # referencing the research round. Themes specific to these rounds (Round 4 and 5) have also been highlighted in a darker shade.

	Factors that <u>decrease</u> propensity to share	Factors that <u>increase</u> propensity to share
Current methods	<p> I'm fine with the way things are (apathetic to change)</p> <ul style="list-style-type: none"> Societal acceptance of current data sharing methods [R1,R3,R4,R5] No benefit/value from ADR's product [R1,R2,R3,R4,R5] General hesitance to share personal data [R3,R4,R5] 	<p> I'm dissatisfied with current solutions</p> <ul style="list-style-type: none"> General understanding of current data sharing methods [R2,R4] Involvement of authoritative and recognisable parties [R2,R3,R4,R5] Transparency of ADR accreditation fosters trust [R2,R3]
CDR process	<p> I'm averse to CDR proposition(s)</p> <ul style="list-style-type: none"> Low confidence in the Government's ability to enforce or handle data [R1,R2,R3] Effort and uncertainty when withdrawing consent [R5] Fear of on-selling and unsolicited interactions [R2,R3,R4,R5] Access, use and mediation of data by unknown entities [R4,R5] CDR is "new" and "unknown" [R3,R4,R5] General concerns about ADR's data handling policies and practices [R2,R3,R4,R5] 	<p> I'm drawn to CDR proposition(s)</p> <ul style="list-style-type: none"> Clear benefit/value from ADR's product [R1,R2,R3,R4,R5] CDR creates simple, easy and informed consent when data sharing [R2,R3,R4,R5] CDR facilitates an increase in data literacy [R2,R3,R4,R5] Greater control and management of data [R2,R3,R4,R5] Requested data is minimised and specific as to purpose [R2,R3,R4,R5] Trust in ADR and CDR process is built over time [R4,R5] Familiarity with parties involved [R2,R3,R4,R5]

Trustworthiness increases over time

Trustworthiness was assessed at various points in the process including before and after completing the consent flow for the first time, and before and after completing the amending consent flows.

Similar to previous research, participants were cautious about sharing their data when first asked to do so (2.9). Most participants indicated a higher level of trust after completing the consent flow (3.3). This was attributed to the level of control they were given; the ability to withdraw consent; the deletion of redundant data; government accreditation and regulation; and the legitimating presence of the data holder.

Trust was highest before going through the amending consent flow (4.1) due to increased familiarity, an existing willingness to share data, and the absence of any negative impacts.

While trust was still high after completing the amending consent flow (3.9), the average trustworthiness score decreased slightly due to the newfound presence of an outsourced provider that negatively impacted trust in the ADR and process.

	Before original consent ¹	After original consent ²	Before amending consent ³	After amending consent ⁴
Lowest score from participants	1-Strongly untrustful	1-Strongly untrustful	3-Neutral	2-Untrustful
Highest score from participants	5-Strongly trustful	5-Strongly trustful	5-Strongly trustful	5-Strongly trustful
Average score*	2.9 <i>indicating 2-Untrustful to 3-Neutral</i>	3.3 <i>indicating 3-Neutral to 4-Trustful</i>	4.1 <i>indicating 4-Trustful to 5-Very trustful</i>	3.9 <i>indicating 3-Neutral to 4-Trustful</i>

¹ Before completing the original consent flow scores from 15 participants.

² After completing the original consent flow scores from 21 participants.

³ Before completing the amending consent flow scores from 23 participants.

⁴ After completing the amending consent flow scores from 22 participants.

* Scores were given on a 5-point Likert scale, with 1 being 'strongly untrustful' and 5 being 'strongly trustful'

Research objective

D2: Understand how trustworthy consumers deem the CDR.

Preference for the CDR increases over time

After going through the original and amending consent flows, participants assessed their attitudes towards the CDR process.

When comparing the CDR with current data sharing methods:

- After the original consent, on average, participants gave a response of 3.3, indicating '3-Indifferent' to '4-A bit better.'
- After amending consent, the average increased to 4.0, indicating '4-A bit better.'

Throughout participants have commented on the ease, transparency and security of the process, and newfound control of their data. However, after amending consent, participants suggested that their increased preference for CDR was due to the explicit requests for consent and proactive reminders from the ADR. Some participants also saw the CDR as an opportunity to create consistency in an otherwise inconsistent landscape.

Research objectives

D2: Understand how trustworthy consumers deem the CDR.

D4: Understand if consumers have a propensity to share their data with the CDR.

”

It was much more transparent and informative than signing up to Tinder through Facebook.

—R5P5, when asked 'How does this way of sharing data compare to current ways of sharing data?'

Sometimes I give out my information blindly this was more resourceful.

—R4P2, when asked 'How does this way of sharing data compare to current ways of sharing data?'

I like that it does not automatically renew and you are reminded of how to stop sharing at regular points.

—R5P2, when asked 'How does this way of sharing data compare to current ways of sharing data?'

Comfort with CDR increases over time

After going through the original and amending consent flows, participants assessed their attitudes towards the CDR process.

When assessing their comfort with the CDR (as the new way of data sharing):

- After the original consent, on average, participants gave a response of 2.9, indicating '2-Uncomfortable' to '3-Indifferent.'
- After amending consent, the average increased to 3.7, indicating '3-Indifferent' to '4-Comfortable.'

Participants remarked that their increase in comfort was due to the familiarity of the process and the proven realisation of terms made during the Consent flow. They also expressed the need for more information around the CDR and greater consumer adoption before they could feel completely comfortable.

Research objectives

D2: Understand how trustworthy consumers deem the CDR.

D4: Understand if consumers have a propensity to share their data with the CDR.

”

This is a good approach for explicit data sharing. I'd like to see it instead of just signing onto "you agree to share your data with unnamed third parties" types of clauses.

—R5P11, when asked 'How comfortable would you be if this was the new way of doing things?'

It would be consistent whereby it is currently not consistent.

—R4P4, when asked 'How does this way of sharing data compare to current ways of sharing data?' and 'How comfortable would you be if this was the new way of doing things?'

If this was the new way to do things, I would assume that most people would be on board. I could get information from other peoples experiences.

—R5P2, when asked 'How comfortable would you be if this was the new way of doing things?'

Comfort with sharing bank data increases over time

Before going through the original and amending consent flows, participants assessed their level of comfort around data sharing.

- Before the original consent, on average, participants gave a response of 2.9, indicating '2-Uncomfortable' to '3-Indifferent.'
- Before amending consent, the average increased to 4.0, indicating '3-Indifferent' to '4-Comfortable.'

After an initial hesitance, participants suggested that based on "a year without any issue and saving money" that they would be more comfortable to share bank data. They appreciated the ADR's proactive reminder at the end of the sharing period. They found reassurance in the ability to opt-out and the handling of data. While participants understood that their amended consent would be voluntary, some interpreted the alternative (deletion of their redundant data) as a "threat."

Research objectives

D2: Understand how trustworthy consumers deem the CDR.

D4: Understand if consumers have a propensity to share their data with the CDR.

”

I'd feel comfortable to continue using the app and giving my data because I had clearly benefited from allowing its use, and felt as though the company had followed through on their promise to check in on willingness to share my information with them. I don't think they could do anything else to make me more comfortable to share my data, aside from reiterating in full what that access means and how to withdraw it.

— R5P8, when asked 'How comfortable would you be in this situation?'

I can make a choice to stop and go back if I need to. I have not consented to my data being deleted and it feels like a threat continue or else.

— R4P3, when asked 'How comfortable would you be in this situation?'

Perceived benefit was consistently high for the budgeting use case

Before going through the original and amending consent flows, participants assessed the benefit of sharing their bank data for budgeting and account aggregation.

On average, participants gave a Likert response of 3.9, indicating '3-Neutral' to '4-Beneficial' before the original consent. This average increased slightly (4.0) before amending consent.

Most participants saw the benefit in the ADR's value proposition, referencing short and long term changes to their spending and habits. While some participants did see not benefit from the ADR's value proposition, they saw benefit in the CDR process. Broadly, they commented on a consistent and easier experience when sharing and revoking data with organisations and the belief that government involvement meant added security.

Research objectives

D2: Understand how trustworthy consumers deem the CDR.

D4: Understand if consumers have a propensity to share their data with the CDR.

”

If it is saving me money I would probably continue. I would eventually phase it out once I felt I had formed good financial habits.

— R5P2, when asked 'What level of benefit do you see in this situation?'

I'm obviously able to track my spending more effectively, and this allows me to personally save money. I am also having my data protected by a government app rather than insecurely storing it in a google doc or elsewhere.

— R5P8, when asked 'What level of benefit do you see in this situation?'

It would help keep track of finances, and also make it easy to get their data to other organisations

— R4P1, when asked 'What level of benefit do you see in this situation?'

Willingness to share data increases over time

After going through the original and amending consent flows, participants assessed the willingness to share their data.

- After the original consent, on average, participants gave a Likert response of 2.9, indicating '2-Unwilling' to '3-Neutral.'
- After amending consent, the average increased to 3.9, indicating '3-Neutral' to '4-Willing.'

Generally, participants explained that their willingness to share data would naturally increase after a year of positive experiences. When amending consent, most participants were willing to share the same data. They reiterated that they would only share data that was specific to the purpose. Participants also attributed their willingness to share to the transparent process and constant assurance of data protection.

In a real-world situation, participants explained that they would investigate the ADR and any affiliated OSPs to understand their ethics and data handling processes before data sharing. The absence of the DH during the 'Use only' scenario negatively impacted their perception of the ADR and process.

Research objectives

D4: Understand if consumers have a propensity to share their data with the CDR.

”

If it was working with the existing level of data sharing I would continue with this level unless I was shown the extra value of sharing more and reassured that it was safe to do so.

— R5P2, when asked 'How willing would you be to share your own bank data with [the ADR]?'

I feel like the correct regulations are being adhered to and I can withdraw consent at any time safely; if I cannot then I am able to access authorities myself.

— R5P8, when asked 'How willing would you be to share your own bank data with [the ADR]?'

I'm just not familiar with them, I'd have to do more research.

— R4P2, when asked 'How willing would you be to share your own bank data with [the ADR]?'

Data Standards Body | Consumer Experience Workstream

t +61 2 9490 5722

e cx@consumerdatastandards.gov.au

w consumerdatastandards.gov.au