

CONSUMER  
DATA  
STANDARDS

# Consumer Experience Research Phase 3: Round 3

April 2020

Joint Accounts | De-identification and Deletion

# 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.

## Overview

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.

This report contains findings from Phase 3, Round 3 research. A qualitative approach was used with a total of 10 participants in 1:1 research sessions that ran for 90 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](#).

This round of research focused on [joint accounts](#), and the [right to delete](#).

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

# Executive summary

## Trustworthiness, Propensity to Share, Informed Consent

- The CDR is seen as better than existing practices
- Accreditation and regulation increase trustworthiness of the ecosystem, but perceptions of low government capabilities decrease confidence
- Trustworthiness is strongly tied to the perceived benefit of sharing
- Participants were able to recall the terms of consent with over 75% accuracy

### Please note:

- Concepts tested in research were used as artefacts to facilitate insight generation. Recommendations contained in this paper are preliminary.
- Concepts and recommendations contained in this paper should not be seen as indicative of final standards or guidelines.

## Joint Accounts

- This round suggested that '2 to authorise' aligned with data sharing mental models
- Confidence for JAH2 when going to authorise a joint account will depend on the provision of certain information
- Joint account approval is conceptualised on a case by case basis; messaging needs to be refined
- There is a perception that joint account sharing will reveal personal information to the other joint account holder

## 'Right to delete'

- The general difference between de-identification and deletion is understood
- Consumers expressed a preference for deletion as it was regarded as safer
- Deletion by default, and de-identification as an 'opt-in' choice would better align with consumer expectations
- ADRs should be clear on why data may be kept even when it is no longer need for good/service provision

# 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 ensure that rules and standards are 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 [cdr-data61-cx@csiro.au](mailto:cdr-data61-cx@csiro.au)

# 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?

This round, we used a qualitative approach and conducted ten 1-on-1 sessions that ran for 90 minutes each.

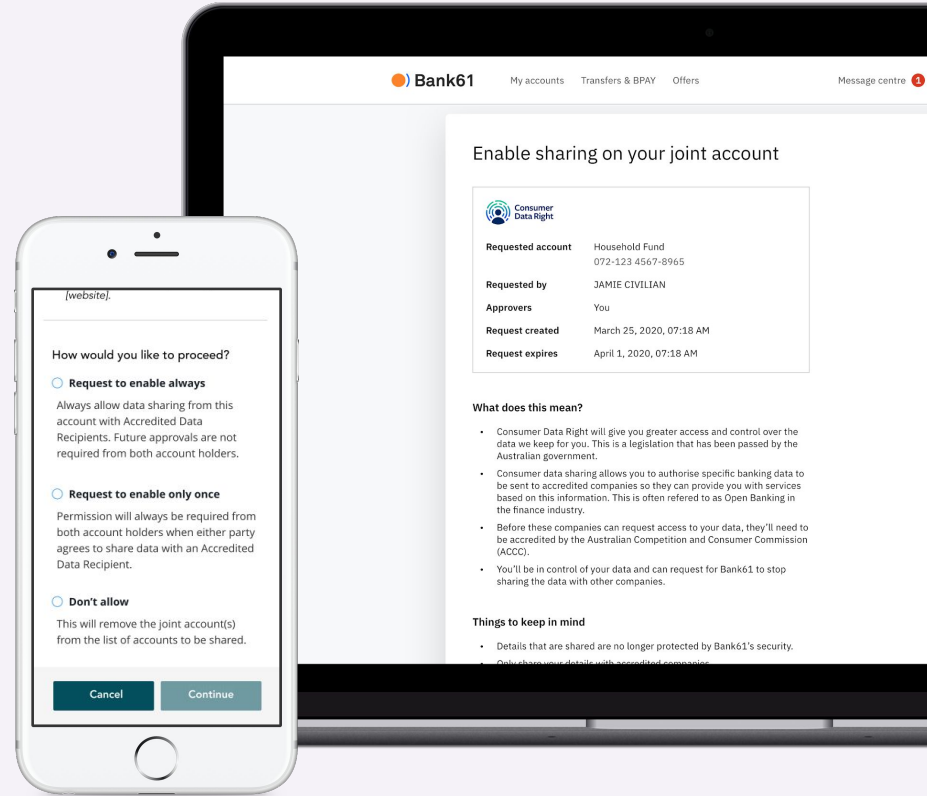
For **Joint Accounts**, we wanted to understand:

- how joint accounts can be made available intuitively, contextually, and in a way that allows the user to be well-informed
- the response to a refined in-flow election pattern; authorisation preferences; and the JAH2 experience

For **De-identification and Deletion**, we wanted to understand:

- if the right to delete design pattern is an effective and contextual affordance
- if consumers comprehend de-identification/deletion

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



## RESEARCH APPROACH

# Who did we research with?

We want to reduce our bias and research out risk by engaging a broad and diverse range of participants. We take a 'no edge cases' approach; 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, we focus on removing the barriers to CDR being inclusive and accessible, which will make CDR easier and simpler to access for everyone.

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

We are researching with participants who have varying levels of:

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



### Note

Round 3 participants live in Queensland, New South Wales, Victoria, South Australia and Western Australia.

# Who did we research with?



**R3P1**  
Male, 18-30 years  
NSW - Metro



**R3P6**  
Female, 51-60 years  
VIC - Suburban



**R3P2**  
Female, 41-50 years  
VIC - Large town



**R3P7**  
Female, 51-60 years  
SA - Rural



**R3P3**  
Female, 41-50 years  
WA - Metro



**R3P8**  
Unspecified, 61-70 years  
QLD - Metro



**R3P4**  
Female, 61-70 years  
VIC - Metro



**R3P9**  
Female, 41-50 years  
VIC - Suburban



**R3P5**  
Female, 51-60 years  
QLD - Rural



**R3P10**  
Female, 31-40 years  
NSW - Suburban



### Identity and diversity

- 4 are CALD
- 1 identifies as LGBTQI+
- 1 has accessibility needs



### Level of digital literacy

- 1 has low digital literacy
- 5 have medium digital literacy
- 4 have high digital literacy



### Level of privacy awareness

- 1 has low privacy awareness
- 3 have medium privacy awareness
- 6 have high privacy awareness



### Financial situation

- 5 are financially comfortable
- 2 have experienced financial distress
- 3 rely on Government payments



### Relationship with other Joint Account Holder

- 7 with a negative relationship
- 3 with an amicable relationship



### Level of financial literacy

- 5 have medium financial literacy
- 5 have high financial literacy

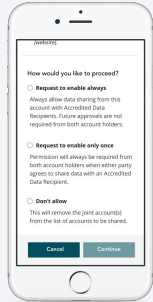


# Session overview and prototypes

# What did we do?

We tested two prototypes as concepts for insight generation in one-on-one participant interviews. After the first prototype, participants were asked a series of open-ended questions relating to the prototype and their attitudes, behaviours and needs.

### 1 Prototype: Requester/JAH1 experience



### 2 Form: Trustworthiness, comprehension and propensity to share data

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

1 - Strongly disagree, 2 - Disagree, 3 - Neutral, 4 - Agree, 5 - Strongly agree

1 2 3 4 5

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

Long answer text

I've shared data from [Country] with [Country] so that I can [Benefit of sharing data]. I've chosen to share the following types of data [Data selection or preferences]. The sharing period for my data is [Time period]. I might want to stop sharing my data because of [Reason for stopping]. If I want to stop sharing my data I can do this by [Action to stop sharing]. After I stop sharing my data, my data will be [Data retention or deletion].

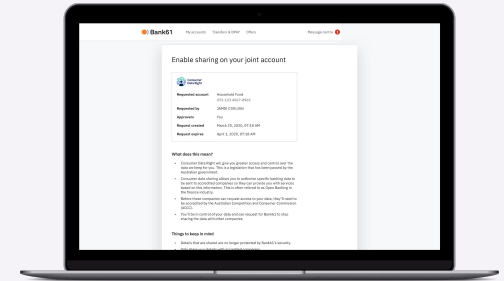
Using the image as a reference, where would you place the ADR's product?

	1	2	3	4
5	6	7	8	
9	10	11	12	
13	14	15	16	

Trust

Benefit

### 3 Prototype: Approver/JAH2 experience



## RESEARCH APPROACH

# Requester/JAH1 experience

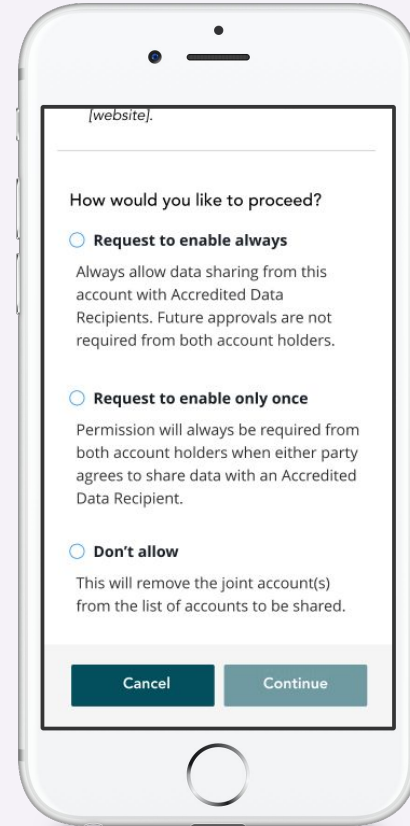
### Prototype focus

- Joint accounts (as the 'Requester' or JAH1)
- De-identification and deletion

### Scenario

- BudgetGuide, an ADR, is a budgeting app that allows consumers to save money and manage their finances
- Real-world bank is the DH, with whom the consumer has a joint account

[View 'Requester/JAH1' prototype](#)



## RESEARCH APPROACH

# Approver/JAH2 experience

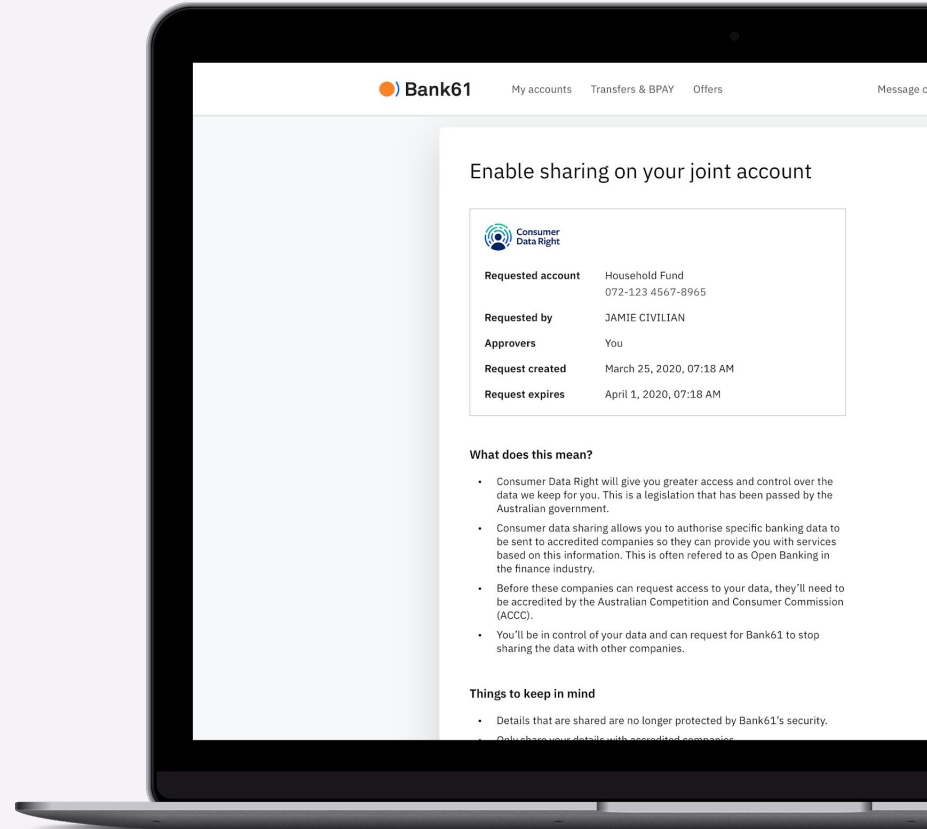
### Prototype focus

- Joint accounts (as the 'Approver' or JAH2)
- De-identification and deletion

### Scenario

- Consumer receives a 'request' notification/comms from their bank (DH)
- Bank61 is the DH, with whom the consumer has a joint account

View 'Approver/JAH2' prototype



## RESEARCH APPROACH

# Trustworthiness and Propensity to share

From consumer-participants, we wanted to understand:

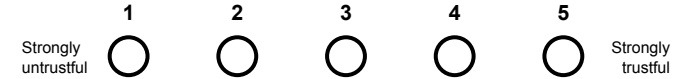
- How trustworthy do they deem the CDR and its actors to be?
- What increases or decreases their propensity to share CDR data?

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

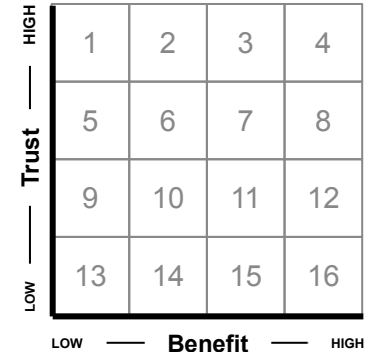


2  
What changes to the experience could be made to increase your levels of trust?

Long answer text

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

Select number ▼



## RESEARCH APPROACH

# Informed consent and Comprehension

Participants were given a “fill in the blanks” style comprehension sheet to assess their understanding and memory of the task they had just completed.

By doing this, participants 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 (personally identified risks or concerns),
- How they might stop sharing their data, and
- What would happen to their redundant data.

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 might want to stop sharing my data because of [ risks or concerns ].

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 **Trustworthiness and Propensity to share**

Understanding consumer attitudes around trust and their propensity to share CDR data.

## TRUSTWORTHINESS & PROPENSITY TO SHARE

# Switching canvas

This switching canvas has been adapted from [Greater than X's Design Toolkit](#) to provide an overview of consumer behaviour and attitude towards data sharing and the CDR.

This canvas presents aggregated themes from 5 rounds of consumer research (Phase 2 and 3) with 48 participants.

**Note:** Phase 3 themes have been tagged [R#], with # referencing the research round. Themes specific to this round (Round 3) 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	<ul style="list-style-type: none"><li>I'm fine with the way things are (apathetic to change)</li><li>Societal acceptance of current data sharing methods [R1,R3]</li><li>No benefit/value from ADR's product [R1,R2,R3]</li></ul>	<ul style="list-style-type: none"><li>I'm dissatisfied with current solutions</li><li>General understanding and unease around current data sharing methods [R2]</li><li>Involvement of authoritative and recognisable parties [R2,R3]</li><li>Transparency of ADR accreditation fosters trust [R2,R3]</li></ul>
CDR process	<ul style="list-style-type: none"><li>I'm averse to CDR proposition(s)</li><li>Low confidence in the Government's ability to enforce action or handle data [R1,R2,R3]</li><li>Effort and uncertainty when revoking consent</li><li>Unsolicited interactions and third party usage [R2,R3]</li><li>CDR is "new" and "unknown" [R3]</li><li>General concerns about ADR's data handling policies and practices [R2,R3]</li></ul>	<ul style="list-style-type: none"><li>I'm drawn to CDR proposition(s)</li><li>Clear benefit/value from ADR's product [R1,R2,R3]</li><li>CDR creates simple, easy and informed consent when data sharing [R2,R3]</li><li>CDR facilitates an increase in data literacy [R2,R3]</li><li>Greater control of data and its management [R2,R3]</li><li>Requested data is minimised and specific as to purpose [R2,R3]</li></ul>



# **CDR Proposition**

Understanding consumer attitudes around trust and their propensity to share CDR data.

## TRUSTWORTHINESS & PROPENSITY TO SHARE

# CDR is better.

Participants were asked:

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

*How comfortable would you be if this was the new way of doing things? Why?*

*How does this way of sharing data compare to current ways of sharing data? Why?*

While the most common Likert score for these questions was '3-Indifferent,' the accompanying open-ended 'why' revealed that **9 out of 10 participants thought that the CDR process was better than the current data sharing methods. However it's important to note that these participants also expressed some hesitance as:**

- it's "still new so would be cautious," and
- that it "depends on the use case" and benefit.

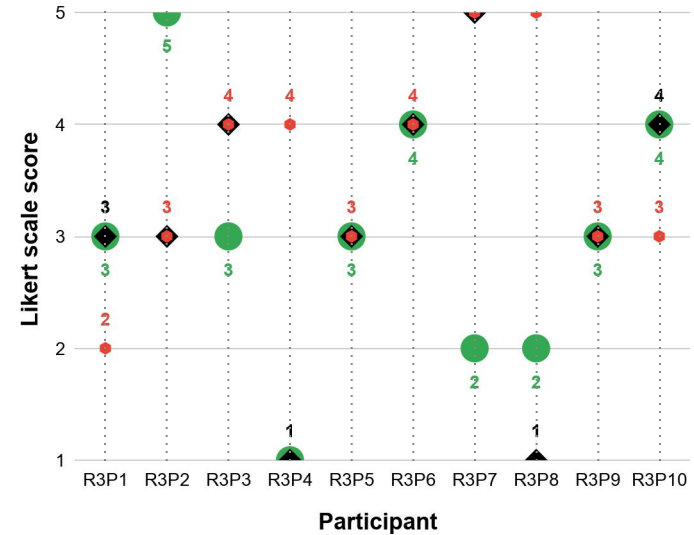
### Research objective

D2: Understand how trustworthy consumers deem the CDR.

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

## Trust and CDR adoption

- How much trust do you place in the process you've just been through?
- ◆ How comfortable would you be if this was the new way of doing things?
- How does this way of sharing data compare to current ways of sharing data?



**Note:** Responses refer to a Likert scale score of 1 to 5. '1' being a negative indicator, '3' being a neutral indicator, and '5' being a positive indicator.

# CDR is “new” and “unknown.”

Participants commended the CDR process for being “easy,” “convenient and accurate,” however in the same sentence, most participants also expressed hesitation towards the CDR process. They explained that:

- they were “uncertain because it’s new” and they “would need to make sure it is safe to share,”
- they “need more information” as they felt they had a “lack of knowledge,” and
- they felt “a bit on edge” due to “how much upfront consent there was - haven’t had to do that for any other apps” and the general mindset of “that’s not how banks work.”

---

### Research objective

D2: Understand how trustworthy consumers deem the CDR.

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

”

***Very convenient to fill in information and would be accurate. Still new so would be cautious.***

— R3P6 when asked ‘How comfortable would you be if this was the new way of doing things?’

***The thing that I questioned is how much upfront consent there was - made me feel a bit on edge - haven't had to do that for any other apps.***

— R3P10 when asked ‘Which parts of the experience DID NOT inspire trust?’

# Comfortable with current data sharing methods.

Some participants were comfortable and “confident” with current data sharing methods. They explained that the CDR “seems similar to other data sharing processes [they] have experienced” and that it “feels like we’re already doing this in some respects.”

---

**Research objective**

D2: Understand how trustworthy consumers deem the CDR.

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

”

***A bit worse. I already feel confident with my current way of sharing data***

— R3P1 when asked ‘How does this way of sharing data compare to current ways of sharing data?’

***I don’t think I’d personally like that. Feels like we’re already doing this in some respects***

— R3P6 when asked ‘How does this way of sharing data compare to current ways of sharing data?’

## TRUSTWORTHINESS & PROPENSITY TO SHARE

# CDR is an “accurate,” “easier” and “natural” process.

Participants praised the CDR process for being “quite self-explanatory and intuitive as a system.” They explained that while they still have some reservations, their trust and comfort levels were elevated due to the following factors:

- Inclusion and familiarity with parties involved (i.e. their bank and ACCC),
- ADR accreditation,
- “Options to choose” what type of data could be shared, and
- Ability to stop sharing and control over their redundant data.

---

### Research objective

D2: Understand how trustworthy consumers deem the CDR.

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

”

***It is definitely easier but would need to make sure it is safe to share.***

— R3P6 when asked ‘How does this way of sharing data compare to current ways of sharing data?’

***The process was quite self-explanatory and intuitive as a system.***

— R3P2 when asked ‘How much trust do you place in the process you’ve just been through?’

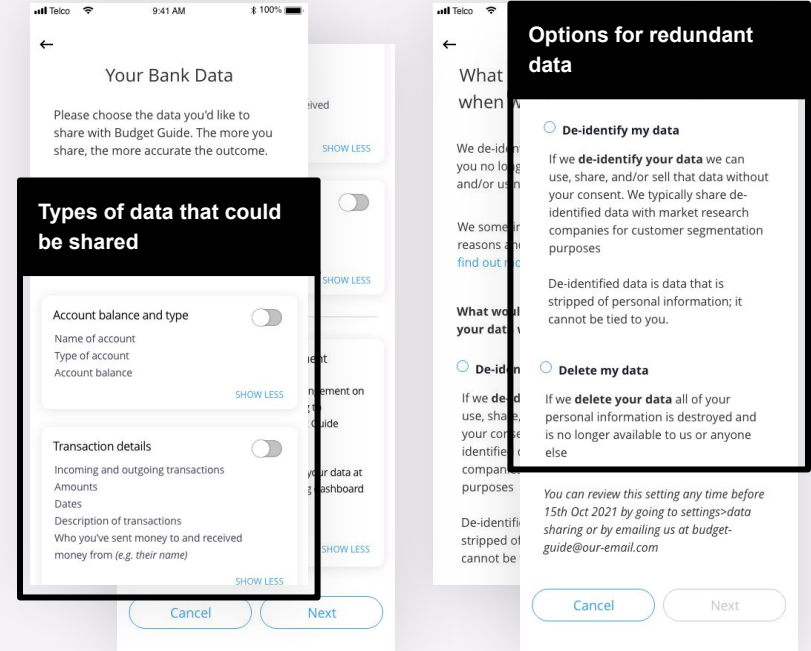
## TRUSTWORTHINESS & PROPENSITY TO SHARE

# “The parts that gave me a choice” inspired trust.

Most participants explained that trust was inspired when they were given the “options to choose:”

- what type of data could be shared,
- when to their “withdraw” data, and
- how their redundant data would be handled.

Participants also commented on the contextual and assistive information that was provided and said that it allowed them to have “informed choices.”



### Research objective

D2: Understand how trustworthy consumers deem the CDR.

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

## TRUSTWORTHINESS & PROPENSITY TO SHARE

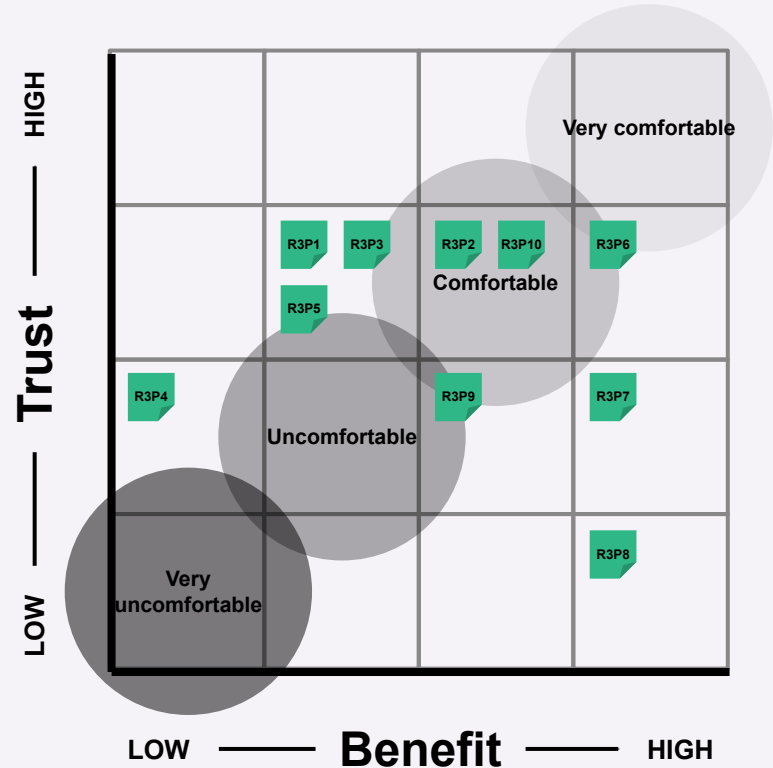
# CDR trust vs. ADR product benefit

Generally participants were hesitant to share their own financial data as they tied it to their “livelihood.”

However some participants were eager to understand “the benefit of using the data sharing and what changes it can bring to my financial habits.”

Other participants expressed an unwillingness to share data as they were “unsure” and saw “no real benefit” in the ADR’s product.

Participants explained that they were more likely to continue using their existing financial tools and features within their banking apps. Furthermore, participants explained that their willingness to share data would “depend on use case.”



### Research objective

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

# Increasing trust and propensity to share.

Participants were asked:

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

Participants explained that the following would increase their trust and propensity to share:

- Greater “awareness” and “reassurance” that the CDR and ADRs were “all above board”;
- Involvement of “an independent body with resources” and “authority”; and
- Greater consideration of vulnerable consumers

---

### Research objective

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

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

D5: Understand if consumers would seek out more information about the CDR.

”

***Giving lots of reassurance that it's all above board.***

— R3P3 when asked ‘What changes to the experience could be made to increase your levels of trust?’

***Something with no ties to private industry.***

— R3P4 when asked ‘What changes to the experience could be made to increase your levels of trust?’

***Ask consumers about level of risk and safety when it comes to sending authorisation request to a joint account holder. From a family violence perspective, this could place a victim survivor at risk.***

— R3P2 when asked ‘What changes to the experience could be made to increase your levels of trust?’



# CDR as a catalyst for behaviour change.

Participants suggested that the CDR could be a catalyst for behaviour change. They praised the CDR's ability to:

- “provide insights on data sharing,” as well as
- surface “the rules and which website to look at.”

They further suggested that the CDR, ADRs and DHs provide “more awareness” around consumer data protection. Participants explained that they would seek out more information and “look at laws and policy guidelines.”

---

### Research objective

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

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

D5: Understand if consumers would seek out more information about the CDR.

”

***If there is more awareness raised by CDR and by banks about data protection and benefits to consumers. And an industry guideline RE protection and use of data.***

— R3P9 when asked ‘What changes to the experience could be made to increase your levels of trust?’

***It looked legit - it provided insights on data sharing, it connected to my bank.***

— R3P10 when asked ‘Which parts of the experience DID inspire trust?’

# CDR Participants

Understanding consumer attitudes around trust and their propensity to share CDR data.

# Inclusion and familiarity with parties involved increases trust.

Similar to previous research rounds, participants were familiar and expressed increased levels of trust when they saw the inclusion of the ACCC and their bank.

Participants continued to explain that the “privacy accreditation body” did not necessarily have to be the ACCC, but simply one that they could trust.

Note: For some participants, the involvement of the ACCC was negatively received as they believed that the ACCC would not be able to provide adequate “oversight.”

---

### Research objective

D2: Understand how trustworthy consumers deem the CDR.

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

”

*I'm okay with connecting because [my bank] is a big bank, if this app is somehow allowed on their platform then I should be more comfortable.*

— R3P1

### ***Protection from ACCC.***

— R3P9 when asked ‘Which parts of the experience DID inspire trust?’

*It's good to see it's being checked out by someone else. By a government body. The ACCC has their issues at times. They are a bit of a toothless tiger. And at other times they come in and act really well. I'm a bit 50/50 with them.*

— R3P6

# Low confidence in Government capabilities.

The [Edelman Trust Barometer 2020](#) states that:

69% of Australians believe that “Government does not understand emerging technologies enough to regulate them effectively.”

This sentiment was echoed by some participants this round. While previous rounds showed high levels of trust in the ACCC, this round showed pronounced concerns about enforcement capabilities. Participants specifically questioned whether the ACCC had the resources and ‘teeth’ to effectively “monitor and enforce the privacy” and “ensure that the data sharing is not abused.”

Participants had low confidence in government in general. As with other rounds of research, attitudes towards data sharing were informed by past experiences and shaped by broader social attitudes.

---

### Research objective

D2: Understand how trustworthy consumers deem the CDR.

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

”

***I do not trust the oversight from the ACCC to ensure that the data sharing is not abused.***

***I would have an independent body with resources and teeth that would be the authority and could investigate any complaints and breaches.***

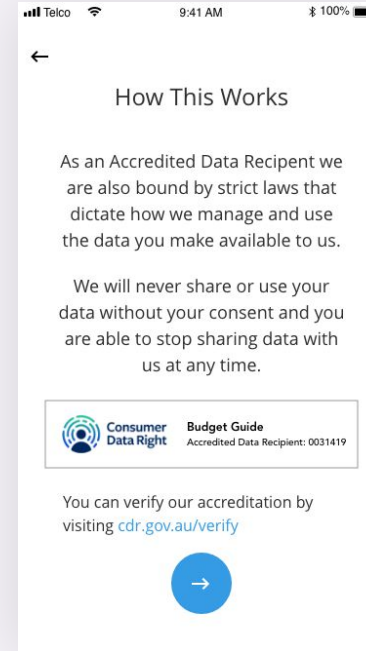
— R3P8 when asked ‘How much trust do you place in the process you’ve just been through?’ and ‘What changes to the experience could be made to increase your levels of trust?’

# Accreditation of data recipients fosters trust.

Similar to previous research rounds, participants expressed greater levels of trust and comfort once they knew that they were interacting with a company that had been accredited.

Participants explained that an accredited company would be part of a “chain of accountability” and there would be “consequences” if there was any misuse or breach of their data.

Some participants explained that they would carry out additional desk research to check the legitimacy of the accredited company, when acting as the Requester/JAH1 as well the Approver/JAH2.



”

***The fact there is accreditation it makes me feel good that there are standards that have to be adhered to. And if those are contravened there would be consequences, fines. Having that chain of accountability, they have a way of actually having compensation.***

— R3P2

---

### Research objective

D2: Understand how trustworthy consumers deem the CDR.

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

# Key insights for **Informed Consent**

Understanding consumer comprehension around their data and the CDR process.

## INFORMED CONSENT AND COMPREHENSION

# Participant recollection was over 75% accurate

Generally participants were able to accurately recall the following after completing the Consent Flow:

- Why they were sharing their data (perceived benefit),
- What types of data they elected to share,
- How they might stop sharing their data, and
- What would happen to their redundant data.

Participants could, on average, recall the terms of consent with over 76% accuracy:

- **4 out of 10** participants scored between **55-66%**
- **5 out of 10** participants scored between **77-88%**
- **1 participant** recalled with 100% accuracy

### Research objective

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

R3P2

I've shared data from my bank ✓  
with a budget planning app ✓ so that I can  
increase my financial wellbeing and address any  
recurring bad financial habits I may have and identify  
patterns of spending behaviour. ✓

I've chosen to share the following types of data All  
my account details, including transactions, balance,  
direct debit, scheduled payments. ✓

The sharing period for my data is 1 year. ✓

I might want to stop sharing my data because of  
Not wanting to have my ex-partner notified that I am  
using this app. ✓

If I want to stop sharing my data I can do this by go  
to the appropriate section of the website and follow  
the steps to revoke my authorisation. ✓

After I stop sharing my data, my data will be Either  
deleted or shared in a deidentified way, depending  
on which option I choose. ✓

## INFORMED CONSENT AND COMPREHENSION

# ‘Sharing period’ was difficult to recall.

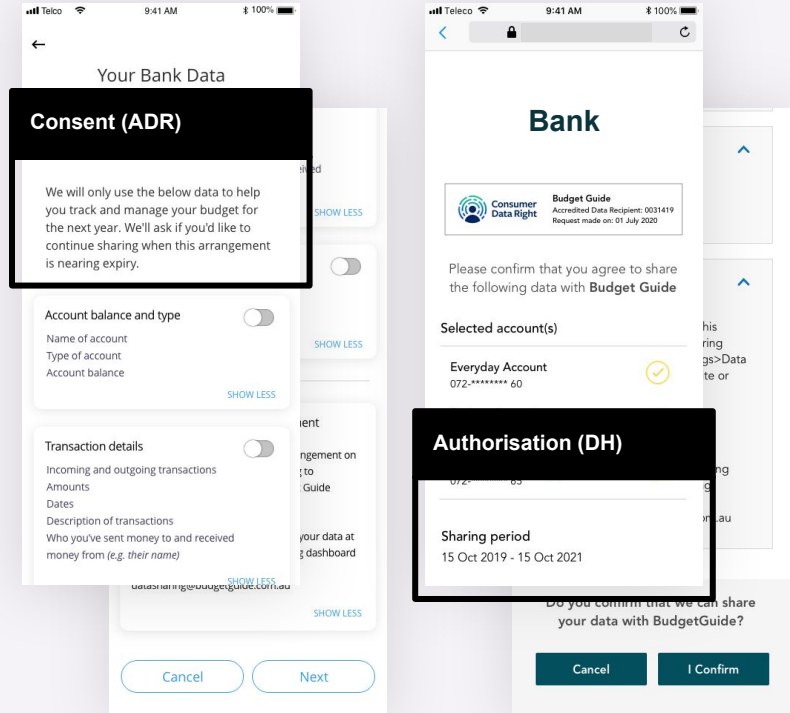
Round 3 prototypes omitted the ‘Sharing period’ component from the ADR’s consent screen to test the impact on recall. The findings suggest that simplifying consent by removing this component may negatively impact the quality of consent.

**6 out of 10** participants had trouble recalling the sharing period of 12-months. Generally participants either:

- recalled a different time-frame, or
- thought that data sharing was indefinite and that the only way to stop sharing was by contacting the ADR or “deleting the app.”

Participants may have interpreted this based on:

- how and when this information was presented in the prototype (i.e. the design pattern and context); and
- their past digital experiences.



### Research objective

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



## INFORMED CONSENT AND COMPREHENSION

# Familiarity and comprehension of financial data is high.

9 out of 10 participants were able to confidently define all banking data clusters and permissions.

Only one participant further questioned 'Name of account,' asking "Is it the name of the account holder?"

---

### Research objective

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

We will only use the below data to help you track and manage your budget for the next year. We'll ask if you'd like to continue sharing when this arrangement is nearing expiry.

**Account balance and type**

Name of account  
Type of account  
Account balance

[SHOW LESS](#)

**Transaction details**

Incoming and outgoing transactions  
Amounts  
Dates  
Description of transactions  
Who you've sent money to and received money from (e.g. their name)

[SHOW LESS](#)

**Direct debits and scheduled payments**

Direct debits  
Scheduled payments

[SHOW LESS](#)

## TRUSTWORTHINESS & PROPENSITY TO SHARE

# General hesitance to share “bank details” with “third parties.”

Participants deemed banking data as highly personal and explained that “to put that in the hands of an app. It’s unsettling.”

**8 out of 10** participants were untrustful, uncomfortable or unwilling to share their banking data. Participants were generally “cautious” when it came to their “bank details” and expressed security and “unauthorised access” concerns.

One participant further explained that “It’s relatively new where third parties can access your personal financial information. It’s unknown at this stage which companies to trust and how your data is protected.”

---

### Research objective

D2: Understand how trustworthy consumers deem the CDR.

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

”

***Untrustful, I worry about unauthorised access and losing my savings.***

— R3P7 when asked ‘How much trust do you place in the process you’ve just been through?’

***I am still cautious about data sharing bank information***

— R3P6 when asked ‘How willing would you be to share your own bank data with BudgetGuide?’

***If they have that data I just assume they can do whatever they want with it. Even if there are laws, nothing stops them from breaking it. You never know, someone hacks into the data.***

— R3P1

# Key insights for **Joint Accounts**

Understanding consumer attitudes and experience with joint accounts and data sharing.

## JOINT ACCOUNTS

# Sharing preferences are case by case

Participants were given three joint account sharing options:

1. Request to enable always (1 to authorise),
2. Request to enable only once (2 to authorise), and
3. Don't allow.

Participants assumed that these options would apply solely to this consent, and only for BudgetGuide (the ADR). 'Request to enable once' was conflated with 'once-off' data sharing, and 'Request to enable always' was conflated with 'ongoing' data sharing.

Most participants had no prior knowledge of how the CDR worked and conceptualised data sharing on a case by case basis, with one ADR at a time.

The framing of '1 to authorise' is critical given the limited understanding of the CDR, and misunderstanding this preference may increase confusion and distrust.

### Research objective

B4: Understand where and how joint accounts can be made available to share in a way that is intuitive, contextual.

D2: Understand how trustworthy consumers deem the CDR.

**Sharing options (DH)**

How would you like to proceed?

**Request to enable always**  
Always allow data sharing from this account with Accredited Data Recipients. Future approvals are not required from both account holders.

**Request to enable only once**  
Permission will always be required from both account holders when either party agrees to share data with an Accredited Data Recipient.

**Don't allow**  
This will remove the joint account(s) from the list of accounts to be shared.

Cancel Continue

”

*I assume that Accredited Data Recipients was just BudgetGuide at this stage, because I'm not giving access to anyone else.*

— R3P9

*Sharing with other parties in the future even though they may be accredited.*

— R3P6 when asked 'Which parts of the experience DID NOT inspire trust?'

### Preliminary Recommendation

DHs are required to implement '1 to authorise'; '2 to authorise' is optional. The research suggests that '2 to authorise' aligns more strongly to mental models of how joint account sharing should work.

The presentation of '1 to authorise' should be researched and consulted on further, including the election of a '1 to authorise' preference via a joint account management service.

## JOINT ACCOUNTS

# Approval by JAH2 is expected - but approval controls may differ

All participants **expected some level of authorisation** to occur and were not surprised to see information regarding the joint approval process.

For some joint account relationships, there is a role of **'designated finance decision maker'** that has implications for the approval process. People in these roles **see themselves as the primary decision maker and therefore approval as a given.**

---

### Research objective

B3: Understand how consumers expect joint account data sharing and management to work.

B6. Understand what information needs to be communicated to consumers as requesters and as approvers of joint account elections.

”

*My brother knows that I'm the one in charge of the finance. I'm in control so at the end of the day I just know I make that decision so I'll approve of it after it's done so I'll just tell him after.*

— R3P1

*In our case, all the contact points come to me so if I was doing this I would be asked to authorise my own actions.*

— R3P8

## JOINT ACCOUNTS

# Different expectations when roles are reversed

When participants were put in the role of the ‘approver,’ their expectations over communication and information were much stricter.

When the participant was not the initiator of the sharing process (JAH1), they expected more details around the ADR involved and other measures to assure them of the legitimacy and security of the process.

Receiving more information about JAH1’s data request may help JAH2 be better informed of the risks of approving/authorising a joint account.

### Research objective

B3: Understand how consumers expect joint account data sharing and management to work.

B6. Understand what information needs to be communicated to consumers as requesters and as approvers of joint account elections.

”

*I want to know what the app was like, look up the company make sure that they were an accredited data rights company.*

— R3P8 as the Approver/JAH2

*I would like to think that my partner has already spoken to me about this. If they haven’t, I wouldn’t do anything.*

— R3P7 as the Approver/JAH2

*First of all I would message like straight away and I’d ask her what this is. I wouldn’t even touch it until I’ve heard back from her.*

— R3P1 as the Approver/JAH2

### Recommendation

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.

## JOINT ACCOUNTS

# Knowing the ADR is important before JAH2 approves election

Knowing the identity of the ADR is important for the joint account 'approver' when making their decision and following through. How this occurs for 'approval' compared to '2 to authorise' may differ.

Although it's expected that a conversation or other form of communication would take place between the initiator and approver *before* coming to this screen, participants expected the content in these screens to be tailored to the specific request, not merely broad communication of sharing enablement in general.

In terms of security, participants are also expecting to verify what's being asked of them with what their joint account holder has told them, which includes information regarding the ADR.


### Research objective

B3: Understand how consumers expect joint account data sharing and management to work.

B6: Understand what information needs to be communicated to consumers as requesters and as approvers of joint account elections.

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

Enable sharing on your joint account

 Consumer Data Right

**Requested account** Household Fund  
072-123 4567-8965

**Requested by** JAMIE CIVILIAN

**Approvers** You

**Request created** March 25, 2020, 07:18 AM

**Request expires** April 1, 2020, 07:18 AM

**What does this mean?**

- Consumer Data Right will give you greater access and control over the data we keep for you. This is a legislation that has been passed by the Australian government.
- Consumer data sharing allows you to authorise specific banking data to be sent to accredited companies so they can provide you with services based on this information. This is often referred to as Open Banking in the finance industry.
- Before these companies can request access to your data, they'll need to be accredited by the Australian Competition and Consumer Commission (ACCC).
- You'll be in control of your data and can request for Bank61 to stop sharing the data with other companies.

every data sharing request that comes through.

Approve requests once  
This means you only have to approve requests this one time, all other other requests for this account will be automatically approved.

Decline request  
This means you do not allow data from this account to be shared.

Submit response

”

*I want to know what the app was. I'd look up the company to make sure that they were an accredited data rights company. I would go through that process of checking everything.*

— R3P8

*Going through a messy breakup, divorce, domestic violence.*

— R3P3 when asked 'What situations might trigger you to stop sharing data?'

### Recommendation

Relying on communications between joint account holders alone is not enough to ensure informed consent from both parties. At a minimum, knowing the identity of the ADR provides 'approvers' with an opportunity to fact check removing a key barrier to them completing this process.

## JOINT ACCOUNTS

# Vulnerability creates different needs

Participants expressed concerns regarding vulnerable customers - particularly those in situations of domestic violence and other strained relationships.

This included concerns about information being shared with JAH2 leading to negative repercussions, including a perception that personal information (e.g. phone, email, location) would be shared via this process. Conversely, receiving more information about JAH1's data request may help vulnerable consumers (as JAH2) be better informed of the risks of approving/authorising a joint account (Ref. [Slide 38](#))

Participants also noted that the term 'vulnerable customer' would benefit from a clearer definition to draw attention to how it might apply to them.

### Research objective

B1: Understand the response to the sharing of joint account data from people who have held joint accounts.

B5: Understand how privacy-preserving the sharing of joint account data is perceived to be.

”

*If we're not together, I would not want him to see my details. Definitely not. I would want to keep it private.*

— R3P3

*I think I would need to see the improvements made around checking in on someone's safety levels- re: disclosing to joint account holders.*

— R3P2

*This authorisation gets sent to the person who's been the perpetrator. Now all the sudden, you might be back on that person's radar again and that could actually instigate them going on a fresh campaign of stalking, harassment.*

— R3P2

### Recommendation

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.

DHs should clarify that JAH2 will not see JAH1's actual data (For example, 'Saved payees' and 'Name, occupation, contact details' data). Alternatively, these data clusters could be omitted from JAH2's dashboard to avoid confusion.



# Key insights for **De-identification and Deletion**

Understanding consumer attitudes and behaviours relating to de-identification and deletion of their shared data.

## DE-IDENTIFICATION AND DELETION

# Generally higher levels of engagement with content in this cohort

Compared to rounds 1 and 2 of research, participants in this cohort took a greater interest in information around de-identifying data and deletion.

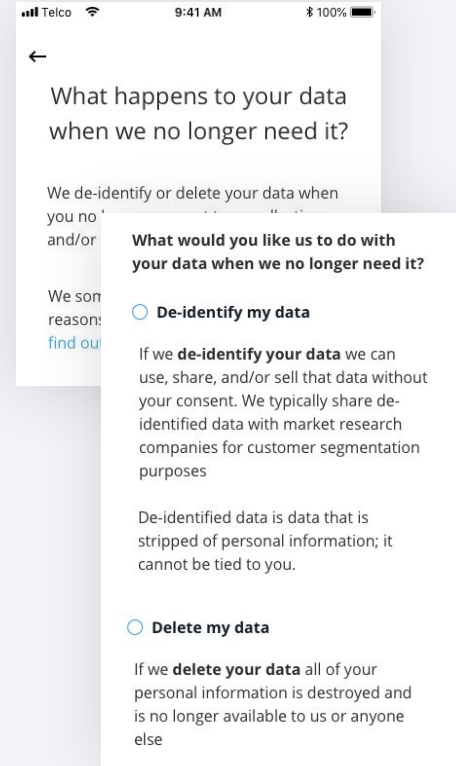
All participants expressed a preference for deleting and variables influencing this response may include:

- the nature of the information, with financial data seen as particularly sensitive,
- the design pattern, encouraging extra scrutiny, or
- the participants being particularly privacy conscious.

### Research objective

C1: Understand if the right to delete design pattern is an effective and contextual affordance.

C4: Understand the appropriate time and context for the right to delete election to occur.



### Recommendation

If the ADR does not have a general policy of deleting redundant data by default, consumers should be able to actively choose how they want their data handled when it is no longer needed.

## DE-IDENTIFICATION AND DELETION

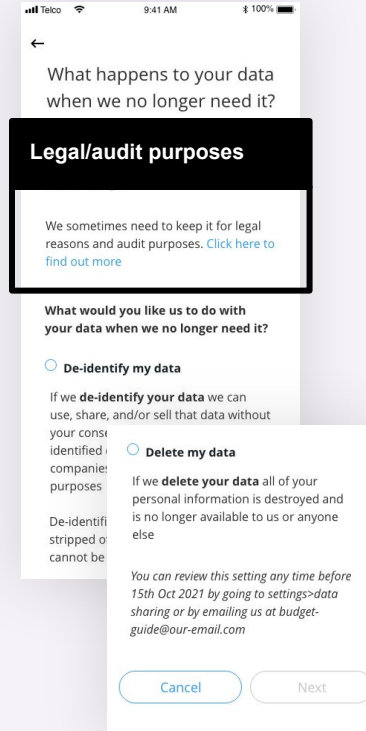
# The difference between de-identification & deletion was broadly understood

Participants broadly grasped the concept of de-identifying vs deletion, ranging from having deep knowledge over how the process of de-identifying or permanently deleting data could be achieved to a more basic understanding of ‘removing one’s name.’

Without prompting, most participants had questions around what constitutes ‘legal/audit purposes’, with participants keen to understand what may trigger such a situation.

### Research objective

C2: Understand if consumers comprehend what de-identification/deletion means.



”

*It just takes my name and address off it, my date of birth and put me into brackets.*

— R3P9

*Because I am still suspicious of this technology I'd want to know the legal reasons.*

— R3P6

### Recommendation

Clearer information explaining what constitutes an ADR’s obligation in retaining information for legal, audit or other regulatory reasons is needed to ensure consumers have a sound understanding of what may happen to their data once shared.

## DE-IDENTIFICATION AND DELETION

# Neither is “foolproof”; deletion is “safer”

Most participants expressed cynicism over the guarantees of de-identifying or deleting data, noting that no process is infallible.

There was a strong sentiment of discomfort and distrust towards de-identifying financial information. Participants felt that by de-identifying their data “there’s too much tied to a commercial interest” and a “lack of control.”

Some participants saw deletion as ending a relationship with an app/provider. For these participants, there was a strong attitude that deletion should be the default preference.

### Research objective

- C3: Understand if consumers understand the implications of electing (or not) to have their redundant data deleted, including the timing of this election.
- C5: Understand how trustworthy and privacy-preserving de-identification is perceived to be.
- D2: Understand how trustworthy consumers deem the CDR.

”

*If I’m no longer using the app I believe that they should automatically delete my data.*

— R3P1

*Even de-identified data can still be re-identified... sufficiently large companies, when they glomerate all their de-identified data, it all comes together.*

— R3P6

*I also wasn’t happy with the current lack of control with the “de-identified information” being shared without a number of options being provided.*

— R3P2

### Recommendation

To reduce cognitive load, simplify consent, and increase consumer trust and confidence, ADRs should delete redundant CDR data by default.

The de-identification of CDR data (redundant or otherwise) should always be an opt-in choice.

**Data Standards Body | Consumer Experience Workstream**

t +61 2 9490 5722

e [CDR-Data61-CX@csiro.au](mailto:CDR-Data61-CX@csiro.au)

w [consumerdatastandards.org.au](http://consumerdatastandards.org.au)