CONSUMER
DATA
STANDARDS

Consumer Experience Research
Phase 3: Round 1 and 2

March 2020

Energy | 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 only verified actors can participate in and 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 the first two rounds of Phase 3 research. A qualitative approach was used with a total of 18 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.

These two rounds of research focused on the energy sector, joint accounts, and the right to delete.

A detailed research approach can be found on the Consumer Data Standards website.

Executive summary

Key research insight

Most consumers are fence-sitters but do see CDR as trustworthy and better than existing data sharing practices.

3 key factors impact a consumer's willingness to share their CDR data:

1. ADR value propositions need to be compelling
2. Past experiences heavily shape perceptions of CDR
3. CDR parties must be trustworthy

Comprehension, Trustworthiness and Propensity Insights
- There is a overall moderate to high levels of trust with the CDR process.
- Trustworthiness and the perceived benefit of the use case are connected. Compelling value propositions and increased trustworthiness will increase propensity to share.
- Propensity to share data is increased with:
  - Minimising the data requested
  - Access to more detail on CDR and ADRs
  - Strict ACCC regulation
  - Comprehensible language over industry jargon

Energy Insights
- Consumers are digital users, just not with energy retailers.
- Energy data is difficult to comprehend but are recognised as necessary for certain use cases
- Requested data needs to be relevant, and sensitive data can cause aversion
- There is concern that energy data can be used to discriminate
- There was higher trust in the ACCC and accreditation, but low confidence in Government ability to handle data.
- A variety of authentication identifiers could be used, but account number was the most familiar and scalable.

Key energy recommendations
- Consider using account numbers (or equivalents) as an authentication identifier for the energy sector.
- Separate payment, hardship, and concession details from other authorisation scopes
- Define a model that allows 'delegated access' to non-account holders for data sharing purposes. Such a model in the energy sector can be extended for other sectors that may experience similar issues.

Joint Account Insights

- The authorisation flow is a natural context for a joint account to be elected
- Comfort with joint account sharing is dependent on the account holder's relationship with the other account holder.
- Multi-party approval is expected
- Non-account holders believe they should have access to their energy data

Key joint account recommendations

- Show unavailable joint accounts in the authorisation flow with election instructions
- Allow election to occur during the authorisation flow
- Allow both joint account consumers to choose 1 or 2 to authorise in-flow

NB 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.

Right to Delete Insights:

- Active choice ensures conscious selection
- The general difference between de-identification and deletion is understood but not the risks
- The motivation to de-identify data is dependent on personal or collective gain

Key right to delete recommendations:

- Present de-identification as 'opt-in', or on an equal footing with deletion
- 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.
- 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

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

Research approach

What did we do?

What did we want to find out?

We used a qualitative approach over two rounds of research, conducting eighteen 1-on-1 sessions that ran for 90 minutes each.

For **Energy**, we wanted to understand:
- behaviours, pain points and needs
- which authentication identifiers were easy to access and comprehend

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

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](#)
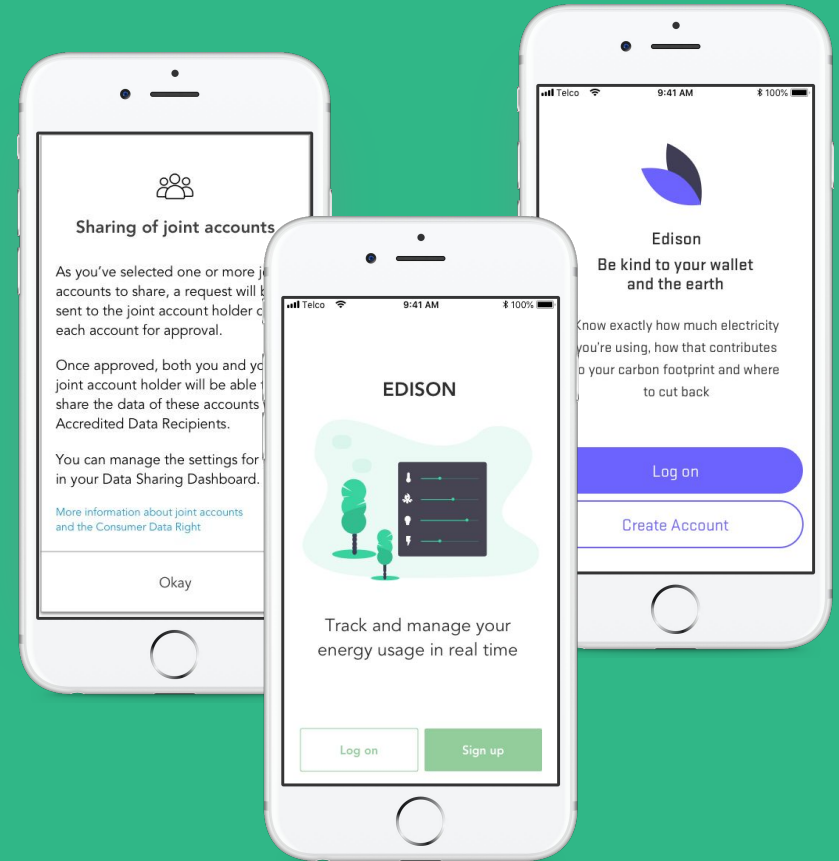
Who did we research with?

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 ↗, but will also 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

Currently our participants live in Queensland, New South Wales, Canberra, Victoria, Tasmania and South Australia.

R1P1
Female, 61-70 years
TAS - Metro

R1P4
Female, 71+ years
SA - Metro

R1P7
Female, 61-70 years
VIC - Metro

R1P2
Female, 51-60 years
VIC - Suburban

R1P5
Male, 51-60 years
SA - Suburban

R1P8
Male, 61-70 years
QLD - Metro

R1P3
Female, 51-60 years
ACT - Suburban

R1P6
Male, 31-40 years
NSW - Metro

R1P9
Male, 71+ years
VIC - Suburban

OTHER INFORMATION
Financial situation:
6 are financially comfortable
1 has experienced financial distress
2 are retired and rely on Government payments
Diversity:
1 has accessibility needs
4 are CALD
1 identifies as LGBTQI+
Level of digital literacy:
3 have low literacy
6 have high literacy
Level of energy literacy:
5 low literacy
1 medium literacy
3 high literacy

R2P1
Male, 18-30 years
NSW - Suburban

R2P4
Female, 51-60 years
SA - Suburban

R2P7
Female, 51-60 years
SA - Suburban

R2P2
Male, 71+
ACT - Metro

R2P5
Male, 51-60 years
VIC - Metro

R2P8
Male, 18-30 years
NSW - Metro

R2P3
Female, 41-50 years
NSW - Metro

R2P6
Female, 51-60 years
NSW - Metro

R2P9
Female, 31-40 years
SA - Metro

OTHER INFORMATION
Financial situation:
6 are financially comfortable
1 has experienced financial distress
3 have experienced financially instability
1 is retired and rely on Government payments
Diversity:
1 has accessibility needs
1 is CALD
1 is of Aboriginal and/or Torres Strait Islander descent
Level of digital literacy:
4 have mid literacy
5 have high literacy
Level of energy literacy:
5 low literacy
5 high literacy

Round 1 and 2
Session scenarios and prototypes

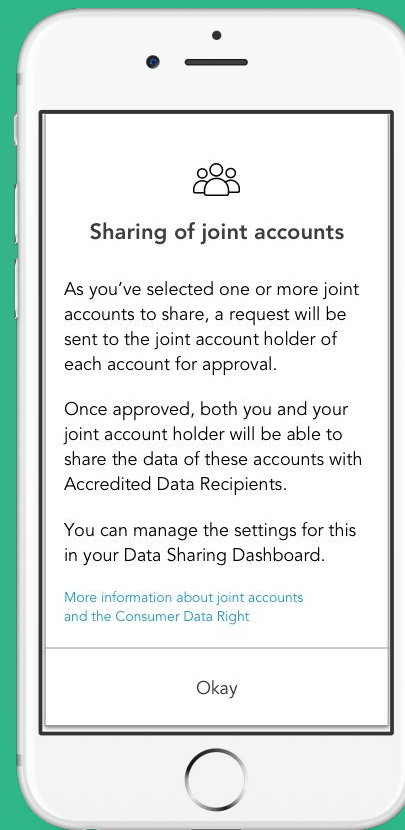# Round 1
Banking consent flow with joint account option

Prototype focus
- Joint accounts
- De-identification and deletion

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

View banking prototype

Sharing of joint accounts

As you've selected one or more joint accounts to share, a request will be sent to the joint account holder of each account for approval.

Once approved, both you and your joint account holder will be able to share the data of these accounts with Accredited Data Recipients.

You can manage the settings for this in your Data Sharing Dashboard.

More information about joint accounts and the Consumer Data Right

Okay

Round 1
Energy consent flow

Prototype focus

- Exploratory energy research
- Simplification of consent flow
- Consumer understanding of sector-specific terms and data
- Authentication identifiers (Account number)

Scenario

- Edison, an ADR, is a company that helps consumers save money by tracking their energy use in real-time and using this information to find more suitable energy retailers.
- Infinite Power is the DH

View energy prototype
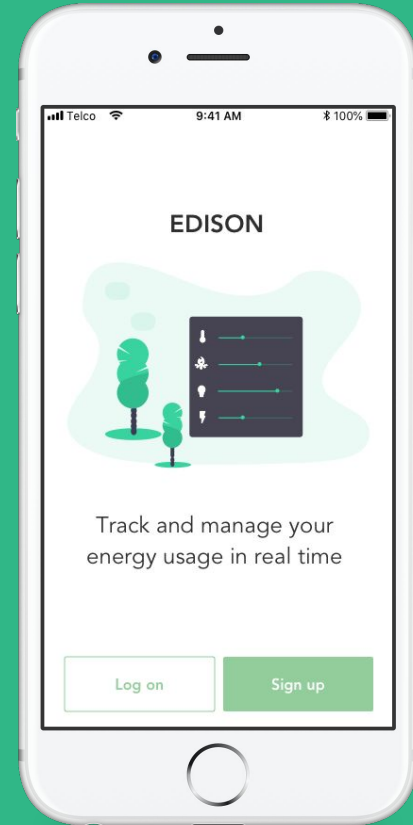
Round 2
Energy consent flow

Prototype focus

- Exploratory energy research
- Simplification of consent flow
- Consumer understanding of sector-specific terms and data
- Authentication identifiers: National Meter Identifier (NMI)

Scenario

- Edison, an ADR, is a company that helps consumers track their electricity use and carbon footprint.
- Real-world retailers were used as DHs

View energy prototype
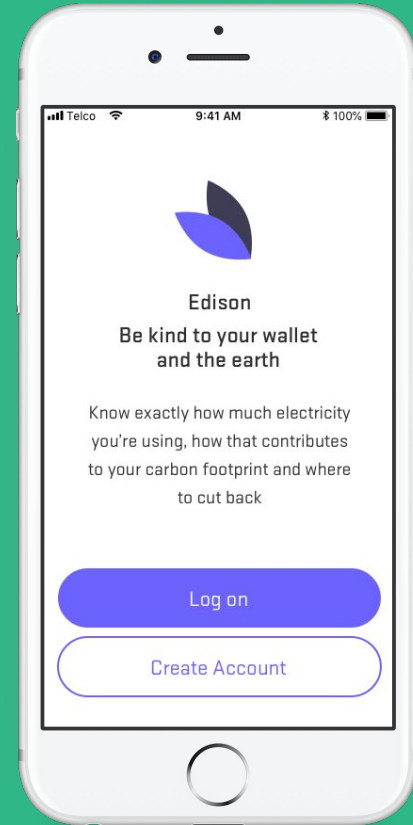
Key insights for
Energy

Understanding consumer attitudes and behaviour towards energy, with a focus on the application of CDR in the energy sector.

I want to switch, but it's too hard.

Cost is key in choosing the best provider. Most participants saw the need to look for a better deal but faced switching barriers.

Participants struggled to understand who offered the best deal because tariffs, charges, discounts, and bundled offers are not easy to understand and compare.

Other participants were faced with a lack of choice, especially in areas like Tasmania and ACT.

Research Objectives

A1: Understand current consumer behaviours, pain points and needs

A6: Understand how consumers currently interact with energy retailers, and how this shapes expectations and CDR accessibility

"Deciding which ones to go [with] was mostly trying to find which ones say [they] had the best deal. And obviously, everyone has a certain condition."

— R2P1

"In Tasmania it's very much been the hydro forever."

— R1P1

"I try not to. About once a year I ring them to ask about a cheaper price. I try to avoid talking to utility companies."

— R1P7

Expectations are shaped by existing experiences.

Cold calls and unsolicited door knocking created a negative association with switching, leading to distrust in the overall concept for some participants.

Participants were wary of being misled with sponsored results by comparison services instead of genuine comparisons.

Comparison services formed part of a broader comparison process; participants did not base their decisions on comparison services alone.

A comparison is a comparison. Some participants saw little benefit in sharing personal data to achieve what was understood to be the same outcome.

Research Objectives

A1: Understand current consumer behaviours, pain points and needs

A6: Understand how consumers currently interact with energy retailers, and how this shapes expectations and CDR accessibility

"I think they are in the market to make money. So they've probably tried to only throw up what they want you to see."

— R1P5, on comparison websites

"These door to door people had been around the area"

— R2P4

Recommendation

If CDR is used to augment existing use cases it must provide and emphasise a distinction in value. Without this the CDR use case risks being seen as equivalent to or even riskier than existing offerings.

Retailer interaction is low and transactional.

Bill payment was cited as the primary retailer interaction for all participants. However, upon probing, even this was done via bank transfer or BPAY, rather than directly with the retailer.

Participants did not trust that their retailer would put them on the best plan without prompting, so made sure to call yearly to negotiate - and phone was the most common interaction channel.

Low interaction did not mean low energy engagement. Some participants were highly engaged with their energy data but rarely engaged with their retailer.

While there was low/no digital adoption in energy, participants used digital channels elsewhere, including online banking to pay energy bills. This suggests digital adoption is sector and not consumer driven.

Research objectives

A1: Understand current consumer behaviours, pain points and needs

A6: Understand how consumers currently interact with energy retailers, and how this shapes expectations and CDR accessibility

"If I had a data source from my energy like the way I get it from my bank, I would use that. I'm interested in reducing my environmental footprint and spend."
— R1P3, who has tracked energy use over the past 3 years in a spreadsheet

"It's not really a relationship, it's just a utility…. I don't interact with them at all, but once a quarter when I pay my bill"
— R1P6

Recommendation

CDR can be used as a catalyst for digital transformation in the energy sector. Consumers are using digital channels already, but don't see a need to do so in the energy sector. Authentication, consent management, and CDR comms can be used as intervention points to catalyse digital adoption.

There is low confidence in the Government's ability to handle digital data

Although there is a view amongst some that the Government has people's best interest at heart, there is also low confidence in the Government's ability to handle digital data. Evidence for this is based on people's experiences with myHealth Record and inaccurate results received from Government energy comparison sites.

Participants are willing to share their de-identified data with Government (ie- to improve policies) but not their direct data as it could personally affect them.

"I have absolutely no trust with the Australian government handling my information and protecting me. None."

— R1P3, on deleting her My Health Record data before closing her account

Research objectives

A8: Understand how consumers expect to manage consents in the energy sector

There is a concern that energy data can be used to discriminate

Participants believed that socio-economic status can be inferred from sharing energy data. This included a concern that energy data would be used for surveillance purposes to assess eligibility for social assistance or benefits.

This contrasts with participants who felt they had 'nothing to hide,' and as such were more open to share their data.

This finding supports previous research that suggested participants from vulnerable backgrounds had a lower propensity to share, as they had greater concerns about possible harm arising from misuse of their data.

Research objectives

A2: Understand the consumer response to the sharing of energy data

A5: Understand how trustworthy and privacy-preserving the sharing of energy data is perceived to be

"I wouldn't share it. You could do all sorts of things like say, [...] if I'm on Newstart, [the government department] could say I'm at home too much."

— R1P7, on sharing energy data to track usage

Recommendation

The research has shown that it is just as important to show what *won't* happen to CDR data as what *will* happen. ADRs should clearly state what they *don't* do with CDR data, and what *won't* be allowed in general. This may include selling data for marketing purposes, or sharing CDR data without consent. Such messages should be tailored to the ADR's use case and customers.

Familiarity and comprehension of energy data is low

Energy sector and data literacy was generally limited to usage and costs.

Most participants struggled to understand more industry specific terminology such as 'Distributed Energy Resources' and 'NMI' (National Meter Identifier).

Participants were also concerned that the language used to describe the datasets was not accessible to non-native English speakers.

Research objectives
A4: Understand how comprehensible energy data and consent is

"I think if I was going through this, right now, I'd probably be just googling to find more information about this. What all these terms mean? And what it means for me, because in the context of energy, maybe the companies are like, this is everyday lingo, but for me, I'm just like, I don't know. I just pay my bills."

— R2P1

Recommendation

Data cluster language needs to be iteratively tested with a wide range of participants to achieve higher levels of comprehension. Data language should comply with WCAG 2.1 on reading experiences. Alternatives and additional clarifiers should be provided to facilitate comprehensibility, which may include more detailed descriptions and translation options.

It is believed that data sharing is required to obtain accurate results

For energy comparison/monitoring/management use cases, most participants believed that the CDR data was necessary for providing accurate results.

This insight contrasts with the low expectations and low comprehensibility findings, but suggests that most participants did see the value and relevance of CDR data for the tested use cases.

Research objectives

A2: Understand the consumer response to the sharing of energy data

5 out of 9 participants believed the requested CDR data was needed to provide accurate energy comparison and management outcomes

Recommendation

Informed consent can be facilitated when ADRs provide a clear and unambiguous reason for requesting data that meaningfully applies to all of the data being requested. The CDR Rules already require ADRs to comply with the data minimisation principle; minimising the data being requested will also reduce the extent of data that the ADR's purpose statement needs to refer to, thus facilitating informed consent.

Irrelevant or sensitive data causes aversion

Broadly clustered data caused concern, such as when payment arrangements, details about hardship and concessions, and contact details were bundled with other datasets.

Participants were comfortable sharing hardship and concession data if it would lead to discounts and support. Others were concerned it could lead to discrimination. The lack of a clear benefit caused some apprehension and concern.

Participants reacted negatively to sharing bank details as part of their energy data. It was seen as irrelevant and unsuitable for the use case, and lowered trust in the ADR.

Occupation was also seen as irrelevant data that participants were reluctant to share, though it was not as sensitive as bank details.

Research objectives

A2: Understand the consumer response to the sharing of energy data

A5: Understand how trustworthy and privacy-preserving the sharing of energy data is perceived to be

"I would not be happy about continuing if they were going to then suck up my bank details. It's totally irrelevant to what they're looking at."
— R2P5

"I wouldn't want hardship and concession arrangements to be passed onto anybody else... If I switch providers, I start with a clean slate."
— R2P2

Recommendation

Data clusters should be iteratively tested to find meaningful taxonomies for consumers and for ADR use cases.

Fine-grained access/control should be considered to allow flexible levels of granularity for a variety of contexts, consumers, and use cases.

Payment arrangements, hardship details, and concession details should form their own respective scopes.

This separation will allow ADRs to provide a clear purpose and benefit for requesting these more sensitive datasets.

There is reluctance to share contact details via the energy retailer

Some participants had <mark>previous experiences of being contacted repeatedly by companies</mark> and found this frustrating. These experiences affected their propensity to share their contact information.

Others <mark>believed this information should be provided separately</mark> (ie-when they sign up for the app), and did not expect their electricity retailer to share this information.

Research objectives

A2: Understand the consumer response to the sharing of energy data

A5: Understand how trustworthy and privacy-preserving the sharing of energy data is perceived to be

"I guess the contact details is always a difficult one to do because I know it is quite frustrating to have that phone call all the time while I'm at work about this."

— R1P8

Recommendation

As duplication of information request can lead to distrust in data sharing, ADRs should refrain from requesting contact details if this information has already been provided.

'Account number' was a logical unique identifier

While participants could not recall their account number, they unanimously stated that this could be retrieved from their energy bill.

When asked about other identifiers, participants questioned the use of 'customer number' as it can also relate to other utilities (such as gas or water) provided by the same retailer.

Research objectives

A7: Understand which identifiers consumers understand and can readily access for authentication purposes

*8 out of 9
found 'account number' to be a familiar and accessible identifier for authentication*

Participants did not always know what NMI was but knew where to locate it

Not all participants could define what NMI was. Some had no idea while others said they would Google this information.

Most recalled seeing their NMI on their energy bill but one participant mentioned the NMI could be found either on her house contract or on her actual meter.

Considerations for using NMI as a unique identifier include:

- It is only attached to electricity, and not other utilities (i.e. gas)
- If one account had multiple NMI, which would the consumer use?

Research objectives

A7: Understand which identifiers consumers understand and can readily access for authentication purposes

"It's either in my house contract or it should be next to the meter somewhere."

— R2P9, on where to find her NMI

One Time Passwords (OTP) are a familiar concept.

Due to previous interactions with Google and their bank, **8 out of 9 participants were familiar with the One Time Password (OTP) process.**

Most participants believed that their energy retailer had their mobile number, though **4 out of 9** participants sought the ability to elect another OTP delivery method such as:

- One Time Password sent to their email
- Automated call
- Pre-set questions

Research objectives

A7: Understand which identifiers consumers understand and can readily access for authentication purposes

8 out of 9 participants were familiar with the One Time Password process; most believed their energy retailer knew their mobile number.

Recommendation

Consider allowing the consumer to choose the OTP delivery method using the contact details the DH already has.

This should be consistent with what the DH uses for existing channels, including online channels and OTP delivery methods (if already in use).

Opportunities
Authentication

Authentication

A variety of authentication identifiers could be used, including a Customer ID, username associated with an online account; an account number; or a National Meter Identifier (NMI).

For example:

1. The consumer has five properties on one account with a single retailer
2. The consumer could use either one of the NMIs, the account number, or their Customer ID as an identifier.
3. A One Time Password would be delivered to the contact details associated with that account.
4. A consumer could then authenticate and authorise disclosure of CDR data for all 5 properties.

The possible identifiers could multiply as other sectors are designated. Sector-specific identifiers could lead to confusion if NMI, DPI (Delivery Point Identifier used for gas) etc. are advertised as authentication identifiers, versus a consistent and familiar attribute like an 'account number'. This confusion could be compounded if a customer has a plan that bundles gas, electricity, and telecommunications with the same provider.

Recommendation

*How might we provide a **familiar, accessible,** and **low-friction authentication experience**?*

*How might this design **enable CDR scalability** and **facilitate cross-sector data sharing**?*

Authentication identifiers should be familiar to consumers. Multiple identifiers could be recognised by the DH to make authentication more accessible and friction-less, such as an existing retailer login, account number (or equivalent), and sector-specific identifiers like NMI.

The research has shown that account numbers are familiar, well understood, and are relevant across organisations and sectors.

Our hypothesis is that an account number (or the DH-specific equivalent) as an identifier will reduce confusion, create consistency, be more scalable and re-usable, and facilitate cross-sector data sharing for CDR.

If a consumer does not have an online account, CDR authentication can be a catalyst for digital adoption, providing a trigger for the DH to help the customer set one up, including to provide them with a digital dashboard. Account number also doesn't *require* an online presence/account, so a consumer can still use CDR without being online with their retailer.

Key insights for
Joint Accounts

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

The authorisation flow is a natural context for joint account election

In round 1 research, we included the ability for participants to elect and authorise their joint accounts to be shared during the authorisation flow.

Participants were shown a message indicating that the other joint account holder would also be asked to authorise and were not surprised to be given the ability to request for joint account sharing at this point.

Research objectives
B1: Understand the response to the sharing of joint account data from people who have held joint accounts
B3: Understand how consumers expect joint account data sharing and management to work
B4: Understand where and how joint accounts can be made available to share in a way that is informed, intuitive, and contextual
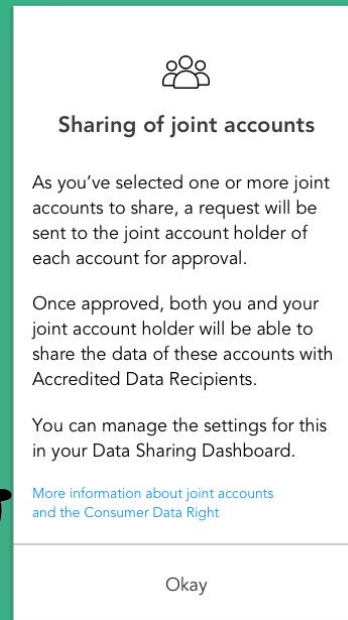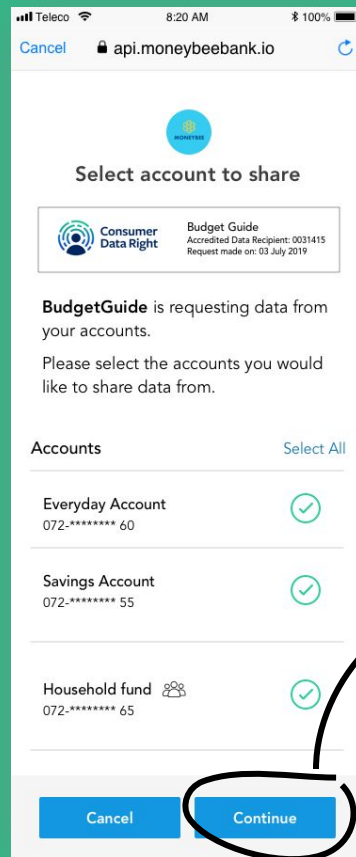
View on joint account sharing is tied to the current relationship between account holders

Most participants interviewed in round 1 seemed to have a trusting relationship with their joint account partner. This is considered a research gap as we have yet to speak with those who have had a relationship breakdown with their joint account partner.

As such, privacy risks were not heavily considered among participants, although there were concerns around sharing joint account information on the context of domestic and family violence came up.

One participant noted that there may be more risk associated with joint account sharing as more people could have their data compromised if there was a data breach.

Research objectives
B1: Understand the response to the sharing of joint account data from people who have held joint account
B5: Understand how privacy-preserving the sharing of joint account data is perceived to be

"There are two different things I have with joint accounts, [...] one where people are working on the same things together and sharing and joint is good, and equal.
[...or] one has the money and he's controlling of it with another so that they check everything that the other person might spend."

— R1P2, on the benefits and risks of joint account sharing

💡 **Recommendation**

Conduct research with consumers who may have had less positive experiences with joint accounts, including vulnerable consumers. Consider how a consumer might 'flag' that they are vulnerable to the DH so the DH can act accordingly.

Multi-party approval is expected

Although most participants in round 1 research had good relationships with their joint account holders, it was expected an alert for a 'second authorisation' would be given to the other joint account holder via email or banking app before any data sharing could occur.

However, further exploration is needed on whether both account holders are expected to authorise once or every time data sharing is requested for that account. We will explore this area further in future research.

There was also an expectation that the other joint account holder should have the right to stop or cancel sharing from that particular joint account.

Research objectives
B3: Understand how consumers expect joint account data sharing and management to work
B4: Understand where and how joint accounts can be made available to share in a way that is informed, intuitive, and contextual

" If a person I shared an account with could share all this without my consent… [they] shouldn't be able to. I've got some joint accounts with my son and that's the last thing I want."

— R1P7, who has joint accounts with her teenage son

Non-account holders believe they should have access to their energy data

There is a desire for non-account holders of a household to have access to their energy data for energy monitoring purposes. Those who are not in a close relationship with the energy account holder, for example a flatmate rather than a partner, may have less access to this information.

It may also affect those who pay their energy bills via their landlord and would like the ability to share their energy data via the CDR.

However, non-account holders cannot be authenticated by the energy company, affecting their ability to access and share their energy data.

Research objectives
B2: Understand the pre-existing barriers and needs for joint account holders that need to be considered for joint account data sharing

"Even though it's a joint account, it's still your data. And if you want to have access to it, then you should be able to have access to it. "

— R1P6, non-account holder in a sharehouse

Recommendation

Define a model that allows 'delegated access' to non-account holders for data sharing purposes.

The delegated party could access and share CDR data using a unique sharing code associated with the account.

A delegated access model could allow CDR data to remain inside the CDR ecosystem, while also allowing the account holder to maintain control over their data.

Such a model could be extended to other sectors that may experience similar issues for a range of scenarios.

Scenarios and Recommendations
Joint Accounts

Joint Accounts

Current state requires a joint account to be elected via the Joint Account Management Service (JAMS) prior to it being available for sharing.

This means it cannot appear in the authorisation flow as an account to disclose data from unless it has been pre-elected.

Issues

The Consent Flow is likely where a consumer will first encounter the concept of CDR and joint account sharing

1.   If a joint account is not available in the authorisation flow, DHs are not permitted to show 'unavailable' accounts, nor provide instructions for how to elect those accounts
2.   If a consumer only has joint accounts with a DH, this means no accounts will be presented.

Joint Accounts
Current state scenario 1

The Data Holder doesn't show 'unavailable' accounts or instructions for how to elect a joint account.

The initiating joint account holder (JAH1) cannot continue and drops off.
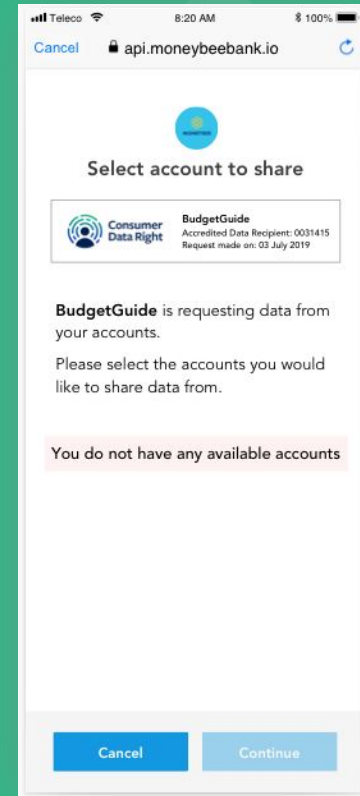
Joint Accounts
Proposed state scenario 1

The Data Holder does show 'unavailable' accounts and provides instructions for how to elect joint accounts.

JAH1 either needs to complete authorisation without selecting any available accounts, or drop off, elect the account via the Joint Accounts Management Service (JAMS), and begin the Consent Flow from scratch again.
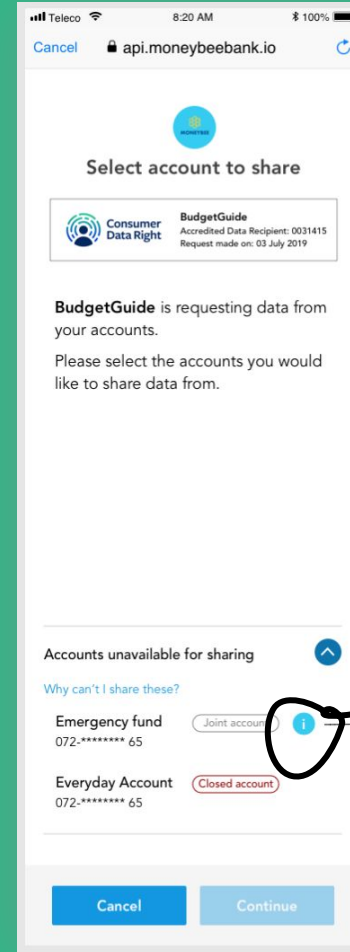
"To share information from this account, go to XXX and select 'authorise sharing'. It may require the permission of other joint account holders."

Joint Accounts
Proposed state scenario 2

The consumer is able to elect and subsequently authorise sharing from their joint account in the authorisation flow.

The Data Holder allows the consumer to choose:

- 'Always allow' (aka 1 to authorise)
- 'Allow once' (2 to authorise)
- Or 'Don't allow'

Which is confirmed by the other joint account holder (JAH2)

Alternative scenario

If the consumer still needs to pre-elect a joint account via the JAMS, the Data Holder can still allow them to choose 1 or 2 to authorise the first time they go to disclose data from that account.
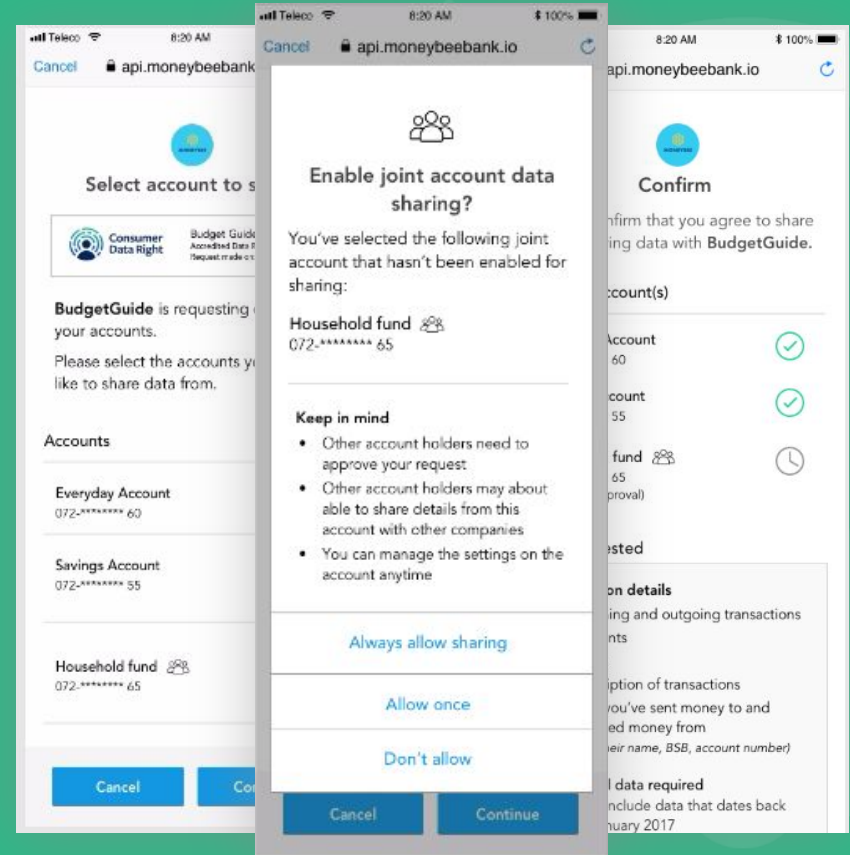
Key insights for
De-identification and Deletion

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

The general difference between de-identification and deletion is understood

All participants understood the difference between electing to have their data de-identified versus having their data deleted. They also understood the consequence of not having their data deleted before the end of their sharing arrangement.

Although there is a general understanding of the two terms, few questioned the limitations around data de-identification and deletion.

"De-identifying means making it anonymous. They wouldn't know my name or residential address. No personally identifying. [...] Delete means: remove it completely."

— R2P4

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

The re-identification risks of de-identification are not well understood

Amongst those who preferred to have their data de-identified, very few noted the limitations of data de-identification.

Some mentioned that they were happy to have their data de-identified unless this information could be tied back to them.

One participant, a financial counsellor would have her data de-identified as she understands the impact and consequences of doing so, but would advise against her clients to do the same.

"I probably advise my clients to delete the data [...] 'cause I know the impact and the consequences of [data de-identification] [...] If you're not going to spend the time to think about it [...] I'm not sure that you want your data to stay out there."

— R2P7, a financial counsellor

Research objectives
C2: Understand if consumers comprehend what de-identification/deletion means
C5: Understand how trustworthy and privacy-preserving de-identification is perceived to be

Motivation to de-identify data is dependent on personal or collective gain

Participants were more inclined to have their data de-identified if it were used for personal benefit or altruistic purposes.

Participants were also only open to sharing their de-identified data with organisations they trusted.

"Well, I suppose I'm thinking it's a service for me. But actually, it's not just a service for me is it, it's a service for somebody else […] data is quite powerful and obviously, I suppose commercial interest or government interest could be definitely interested in that de-identified data."

— R1P1

Research objectives

C5: Understand how trustworthy and privacy-preserving de-identification is perceived to be

Active choice ensures conscious selection

Round 1 tested a right to delete pattern that 'bundled' the election with other contents on a single screen. Round 2 tested a separate screen dedicated to redundant data handling which saw increased engagement and comprehension. All participants in round 2 were able to recall the choice they made as opposed to round 1 where recall was mixed.

Some participants expressed an expectation of a reminder or prompt toward to the end of the sharing period to give them the option to revise their choices.

This is not only specific to de-identifying/deletion, but rather any revisable choices previously made for the sharing arrangement.

Research objectives
C1: Understand if the right to delete design pattern is an effective and contextual affordance
C3: Understand if consumers understand the implications of electing (or not) to have their redundant data deleted, including the timing of this election
C4: Understand the appropriate time and context for the right to delete election to occur
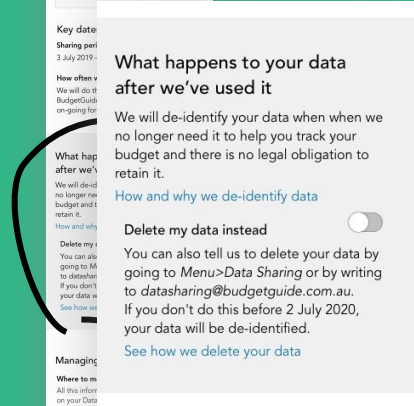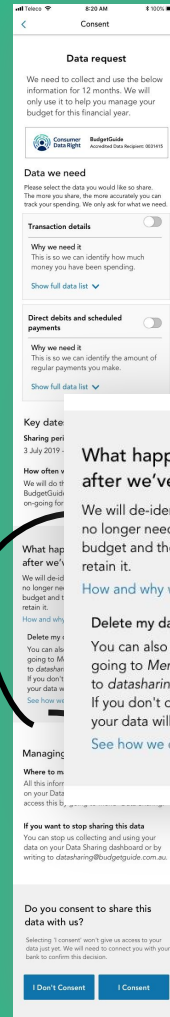
Round 1
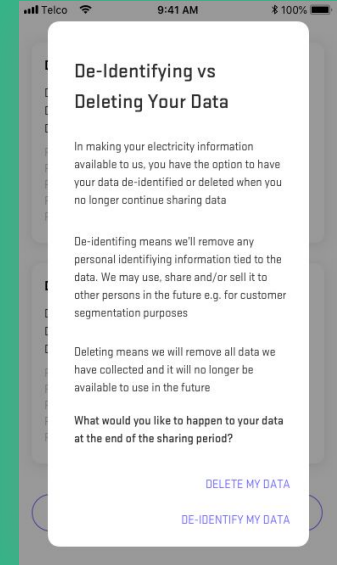
Round 2

Recommendations
Right to Delete

Right to Delete

ADRs must either de-identify or delete data that they no longer need to provide a service or good, or for legal/audit purposes.

A consumer can elect their right to delete in the Consent Flow, as part of the consent withdrawal process, or at any time prior to consent expiry.

If an ADR intends to de-identify redundant data then the consumer must 'opt-out' of this by electing their right to delete.

Research findings over the last year have shown that most participants would prefer to have their data deleted, and few participants have a good understanding of de-identification risks.

Some participants would choose to 'opt-in' to de-identification for personal benefit or altruistic purposes, but only with organisations they trust.

Recommendations

ADRs should delete redundant data by default. This approach increases trust in the process and parties involved, and can also help simplify the Consent Flow.

If an ADR seeks to de-identify CDR data this should be presented as an 'opt-in' choice for the consumer, rather than a default option that a consumer has to 'opt-out' of by electing their right to delete.

In the absence of 'opt-in' de-identification being required, ADRs should present de-identification and deletion on an equal footing (e.g. as radio buttons) so consumers can make an active choice.

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 elect that their redundant data be deleted. This could be when withdrawal occurs via a DH dashboard, when data becomes redundant at any time during the consent period, or when establishing a new consent may lead to a previous one being withdrawn.

Key insights for
Informed Consent and Comprehension

Participants generally understood the concept of sharing data

Participants broadly understood where they were sharing data from, what data they were sharing and who they were sharing that data with.

Participants were quick to point out what they did not choose to share, suggesting a greater salience for data they deem to be risky such as bank information, contact details and hardship and concession data.

Research objectives

D3: Know how informed participants are when/after they have given consent

"By consenting to share my bank data this app will be able to budget my money for me and tell me where my money is going [...] for the next 12 months."

— R1P2

"I've just shared the data I've agreed to from AGL to this accredited company Edison to get some information and and hopefully improve my energy bill."

— R2P1

"The thing that I would alter was [...] the field that contained my banking details and I think that's probably taken out a bunch of other stuff I would have been willing to share"

— R2P7

Key insights for
Trustworthiness and Propensity to share

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

Trustworthiness

D2: Understand how trustworthy participants deem the CDR.

Research Approach

The insights in this section are for general community knowledge to help facilitate trustworthy, simple, and informed data sharing experiences.

This section contains insights related to two research questions:

- How trustworthy do participants deem the CDR and its actors to be?
- What increases or decreases a participant's propensity to share CDR data?

To answer these questions, we asked participants to complete a form containing a series of questions containing 3 activities. The first two activities were adapted from >X's approach in Phase 2 research.

Activity One: Participants could answer several questions **using a Likert Scale with a score from 1 to 5.**

An answer of 1 provided a negative indicator, 3 gave a neutral indicator, and 5 gave a positive indicator.

An example question can be found below:

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

1-A lot worse, 2-A bit worse, 3-Indifferent, 4-A bit better, 5-A lot better

	1	2	3	4	5	
A lot worse	○	○	○	○	○	A lot better

Participants were also provided with **open-ended fields** to answer more subjective questions, as per below:

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

Long-answer text

Which parts of the experience DID NOT inspire trust? *

Long-answer text

Which parts of the experience DID inspire trust? *

Long-answer text

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

Long-answer text

Participants were also asked to score the use case tested in the prototype **using a Trust/Benefit scale**, adapted from New Zealand's Data Futures Partnership, to answer the following question:

'*How do you feel about sharing your data with [ADR] to help you manage usage and costs?*'
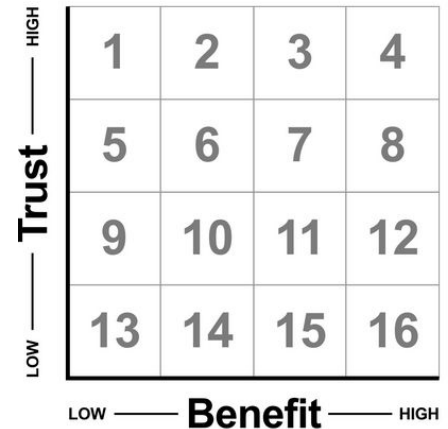
CDR is better.

Participants were asked:

"How does [CDR] compare to current ways of sharing data?"

6 out of 9 participants gave a score of 4 or higher, with an average score of 4.1, indicating that most participants felt CDR was 'better' to 'a lot better' than existing ways of sharing data.

Research objectives

D4: Understand if participants have a propensity to share their CDR data.
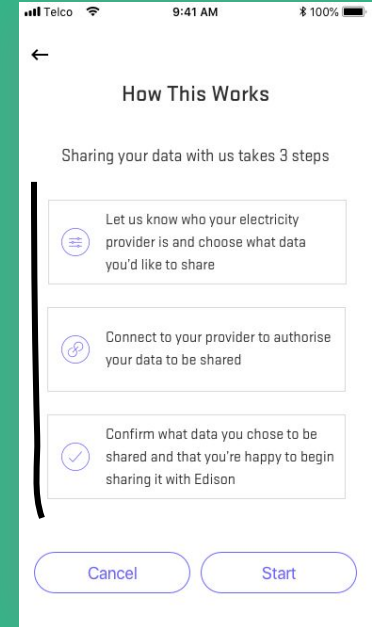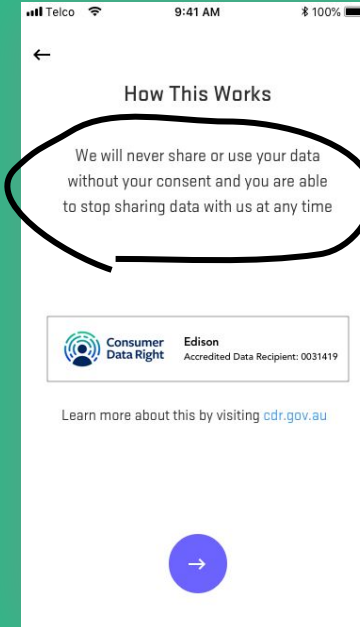
Overall "moderate" to high levels of trust with the CDR process

7 out of 9 participants expressed overall "moderate" to high levels of trust with the CDR process.

Reasons for this include:

- a greater sense of control over their data,
- familiarity with the parties involved, and
- accreditation of data recipients.
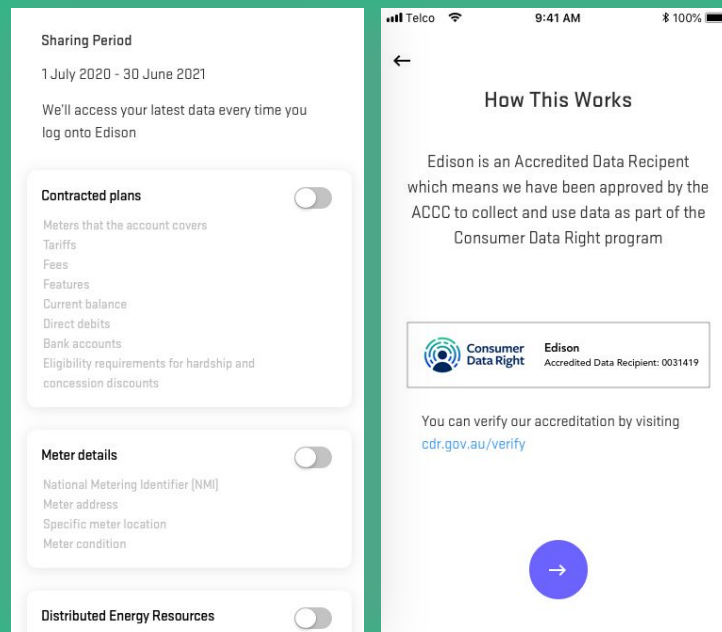
A greater sense of control over their data.

While participants struggled to understand their energy data (such as DER and NMI), **6 out of 9** participants expressed trust in the CDR process due to the greater sense of control they had over their data.

Specifically, participants commented on their ability to:
- elect the type of data they want to share, and
- elect what would happened to their data after use.

"It gave me plenty of opportunity to choose what I was comfortable with, and [...] it was clear how I can both see and control what data I was sharing."

— R2P6

Research objectives

D2: Understand how trustworthy participants deem the CDR.

Familiarity with the parties involved.

Participants were familiar and expressed increased levels of trust when they saw the inclusion of the ACCC and their energy provider.

2 out of 9 participants stated that CHOICE's involvement would boost their levels of confidence and trust.

"I have an implicit trust with the ACCC, I think they are an excellent organization, they do good work. So, having them involved in that is gives me an extra sense that it's, it's likely to be done well."

— R2P7

Research objectives

D2: Understand how trustworthy participants deem the CDR.

Accreditation of data recipients fosters trust.

Participants expressed greater levels to trust once they knew that they were interacting with an ADR.

They generally believed that the accreditation process to be "structured" and carried out by unbiased and "governing bodies."

7 out of 9 participants believed that any misuse or breach of their data by an ADR would lead to:

- loss of accreditation,
- legal action,
- criminal penalty,
- financial penalty, and/or
- negative exposure of the ADR in the media.

"I'd expect there to be repercussions. If there were complaints I'd expect the ACCC to revoke the accreditation. There could be compensation. It depends on the impact. Ideally the ACCC would do regular audits"

— R2P6

Research objectives

D2: Understand how trustworthy participants deem the CDR.

Requested data must be minimised and specific to purpose.

2 out of 9 participants expressed overall lower levels of trust with the CDR process. Reasons for this include:

- the "not relevant" inclusion of "financial" permissions such as bank accounts and payments, and
- the "not relevant" "duplicate data" within some datasets.

3 out of 9 participants questioned why an ADR would want/need this information, and indicated that they would be more willing to share that data if they had an "ability to segment out bank account details."

One participant explained that another reason that they were hesitant to share energy data was because of a past experience: "Door knockers" had collected minimal personal data and were able to change their energy retailer without their consent.

Research objectives

D2: Understand how trustworthy participants deem the CDR.

"Asking for data that is not relevant to energy usage (e.g. payments, bank account details), duplicate data entry, (e.g. NMI address etc.) when that information is already available from the NMI itself."

— R2P5

Propensity to share

D4: Understand if participants have a propensity to share their CDR data.

Edison product offering

Edison 3.02 value prop:

Be kind to your wallet and the earth. Know exactly how much electricity you're using, how that contributes to your carbon footprint and where to cut back. Edison can help you see exactly how much electricity your household uses in real-time, giving you instant feedback on any changes you make.

7 out of 9 participants resonated with the product offering of Edison (Phase 3, Round 2). When asked "How do you feel about sharing your data with Edison to help you manage usage and/or costs?" participants gave scores of 4 or 5, indicating an 'excited' to 'very excited' response.

Two participants were "a little sceptical but [could] see the benefits" of the product. Based on their input and the output, they were unsure how their data was being aggregated and assumed that the results were estimates. (R2P5 gave a score of '2,' R2P3 gave a score of '3')

Research objectives

D4: Understand if participants have a propensity to share their CDR data.
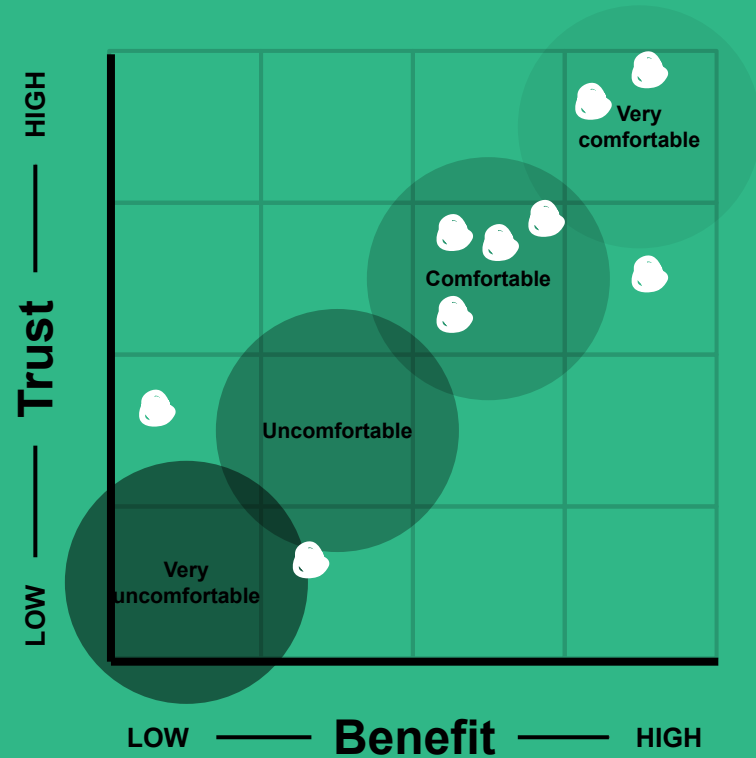
High trust + High benefit = Propensity to share

Participants coupled their trust in the CDR process (and ADRs), with the perceived benefit of the digital product when expressing how willing they were to share data.

When asked "How willing would you be to share your own energy data with Edison?" 9 Round 2 participants gave an average score of 3.4, indicating a 'neutral' to 'willing' response.
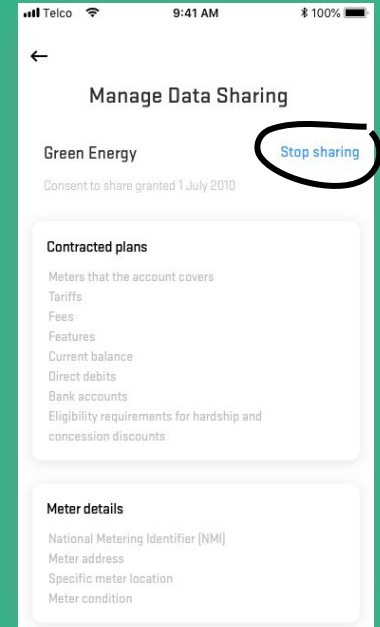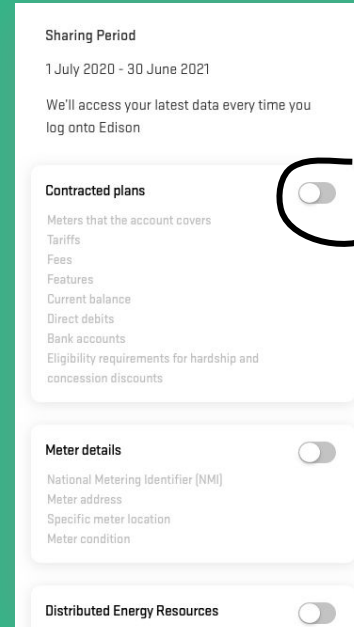
5 out of 9 participants gave a score of 4 or higher, indicating 'willing' to 'very willing' response to sharing their data. Reasons for this were:

- Clear, "well-structured and prompted consent,"
- ability to "manage my own settings," and
- the role of government and it's verification of ADRs.

Research objectives

D4: Understand if participants have a propensity to share their CDR data.
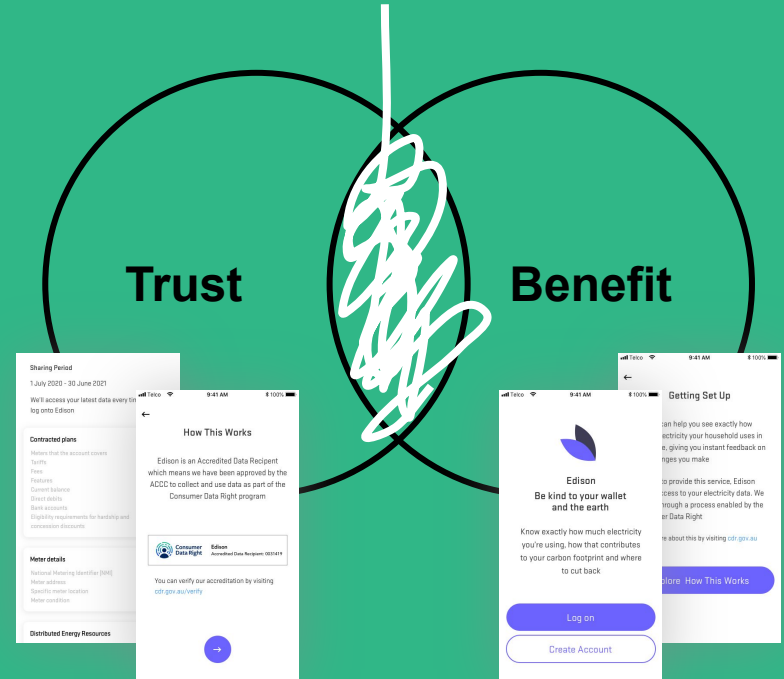
Clear, "well-structured and prompted consent"

Participants commented on the clarity and ease of sharing their data. They expressed comfort around how the concept was explained, as well as the overall process.

One participant remarked on the "well-structured and prompted consent" process, and attributed this to their feeling of "full control over [their] data, allowing [them] to stop sharing at any point in the process." (R2P1 gave a score of '4,' R2P2 gave a score of '5')
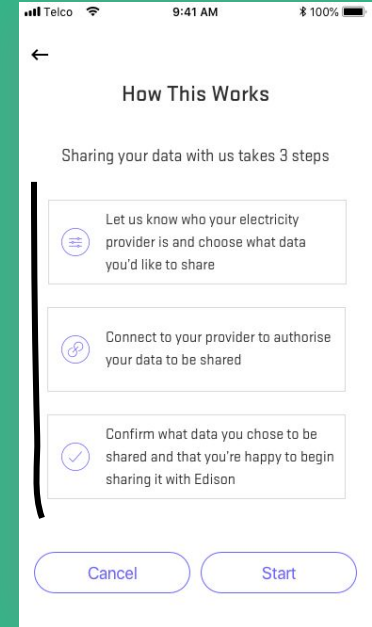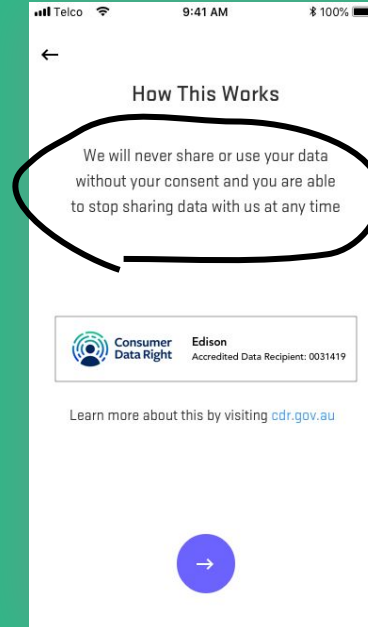
Research objectives

D4: Understand if participants have a propensity to share their CDR data.

Ability to "manage my own settings"

Two participants commented on the flexibility and self-management of their data. They felt like they were "not [...] locked in indefinitely," and appreciated the "choice" to de-identify or delete their data. (R2P8 gave a score of '4,' R2P9 gave a score of '4')

Research objectives

D4: Understand if participants have a propensity to share their CDR data.

The role of government and its verification of ADRs

Two participants commented on the involvement of government and the ability to "verify" ADRs. During the onboarding process, participants were shown a link to "verify" the ADR. Some participants appreciated this and said they would click to verify the ADR before proceeding. (R2P7 gave a score of '5,' R2P9 gave a score of '4')

Research objectives

D4: Understand if participants have a propensity to share their CDR data.
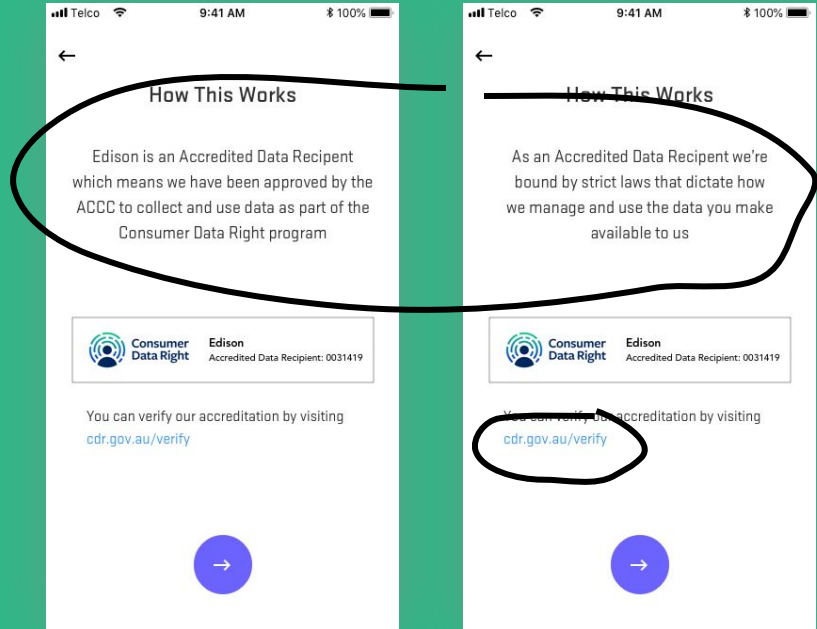
Low trust + Low benefit ≠ Propensity to share

4 out of 9 participants gave a score of 3 or lower, indicating a 'not very willing' to 'neutral' response to sharing their data. Reasons for this were around:
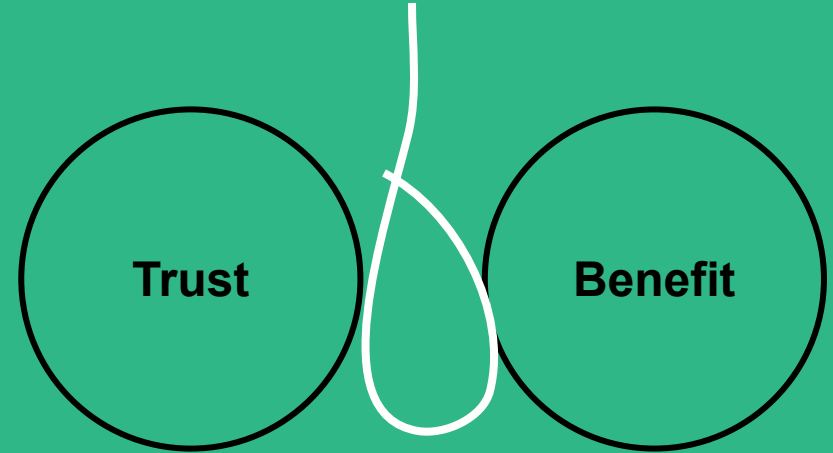
- "the benefits" of the product,
- their own past experience, and
- privacy and third party usage.

Research objectives

D4: Understand if participants have a propensity to share their CDR data.

Propensity to share?

Trust

Benefit

"The benefits" of the product

Two participants were "a little sceptical but [could] see the benefits" of the product. <mark>Based on their input and the output, they were unsure how their data was being aggregated and assumed that the results were estimates.</mark> (R2P5 gave a score of '1,' R2P3 gave a score of '3')

Research objectives

D4: Understand if participants have a propensity to share their CDR data.

64 | Insights and findings | Trustworthiness and Propensity to share
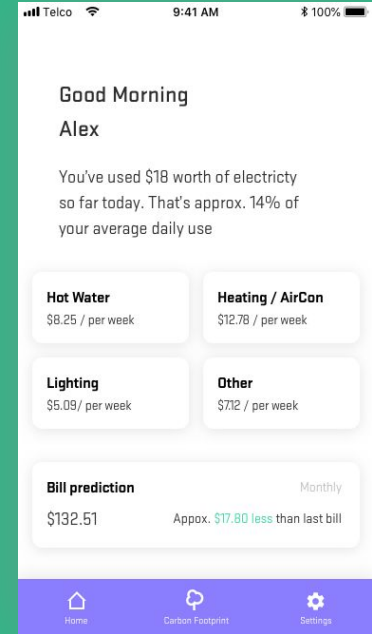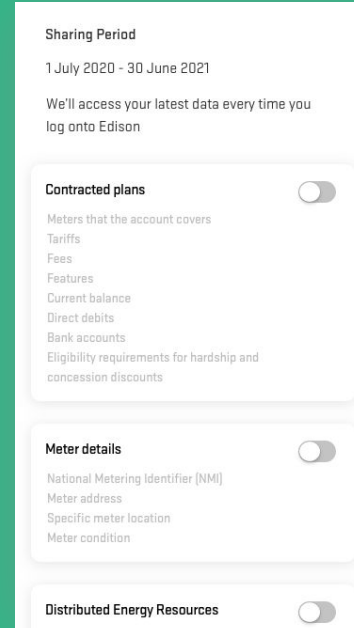
Their own past experience

One participant anecdotally explained that the reason that they were hesitant to share energy data was because of a past experience: "Door knockers" had collected minimal personal data and were able to change their energy retailer without their consent. (R2P4 gave a score of '2')

"It was just a couple of kids and they got money for number of people they signed-up. In my view, this is fraud and it was a big process for me to get back to my original provider."
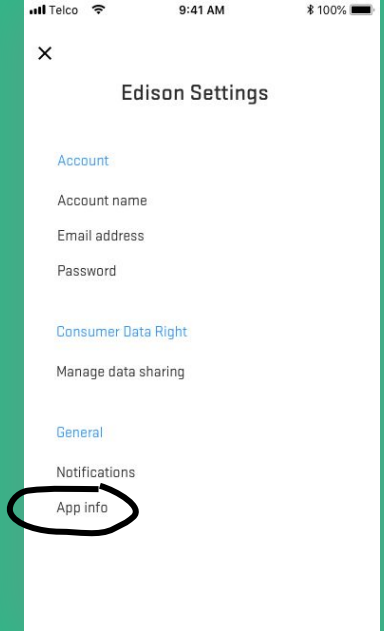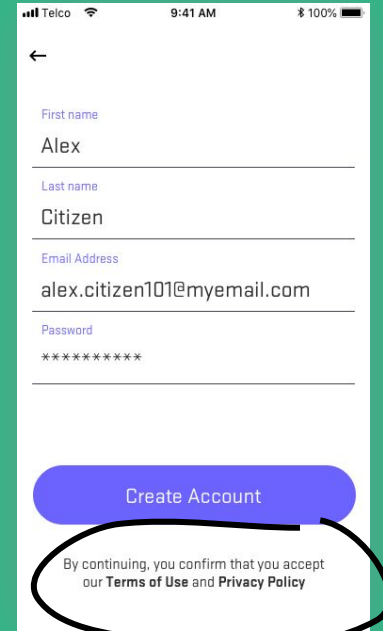
— R2P4

Research objectives

D4: Understand if participants have a propensity to share their CDR data.

Privacy and third party usage

One participant expressed an uncertainty around privacy and third party usage: <mark>"I would need better understanding of what the data is and also what third parties (if any) would have access to the data,"</mark> however they also stated that "overall process better and clearer than expected." (R2P6 gave a score of '3')

Research objectives

D4: Understand if participants have a propensity to share their CDR data.

Increasing propensity to share

D4: Understand if participants have a propensity to share their CDR data

Increasing propensity to share

Participants that gave a score of 3 or lower (indicating a 'not very willing' to 'neutral' response to sharing their data) expressed that the following would increase their propensity to share:

- further control around what data is shared,
- links to additional information, and
- "strict" ACCC oversight.

Participants that gave a score of 4 or higher (indicating 'willing' to 'very willing' response to sharing their data) expressed that the following would further increase their propensity to share:
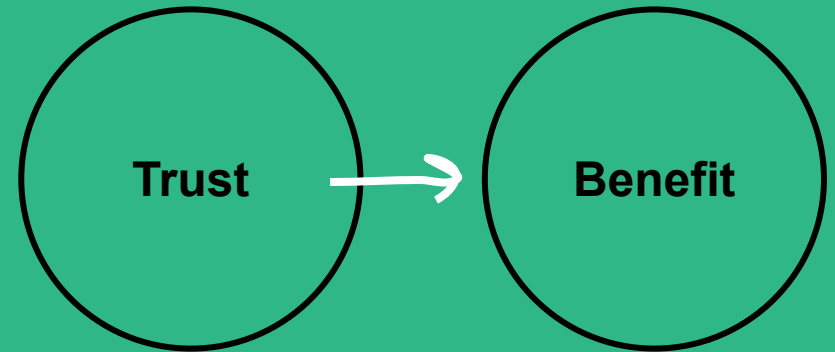
- explanation of industry language and jargon, and
- reassurance that the CDR is "really secure."

Research objectives

D4: Understand if participants have a propensity to share their CDR data.

Further control around what data is shared

Two participants that gave a score of 3 or lower (indicating a 'not very willing' to 'neutral' response to sharing their data) wanted to access the following <u>before</u> consenting to share their data:

- "more information about where and who is using the information,"
- "earlier explanation of Edison's usage of my data," and
- information around the choice to de-identify or delete.

"Do not ask for personal information that is not relevant to energy usage (payment, bank details, any further than a checkbox for concessions). Not continuing to collect data after I choose to opt out of the program."

— R2P5

Research objectives

D4: Understand if participants have a propensity to share their CDR data.

Links to additional information

Two participants that gave a score of 3 or lower (indicating a 'not very willing' to 'neutral' response to sharing their data) commented on the "little information" surrounding the "where and who is using the information" and their "need to be quite informed."

Furthermore, **5 out of 9** participants said they would seek out more information while going through the CDR process. They were interested in:

- verify the ADR (via the surfaced link: cdr.gov.au/verify),
- substantiate the CDR and that it's "Australian legislation," and
- review the "privacy rules" specifically in relation to "sharing with 3rd parties."

"There wasn't much, my own curiosity, more information about where and who is using the information and have the choice the of where you want information to be shared."

— R2P3

Research objectives

D4: Understand if participants have a propensity to share their CDR data.

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

"Strict" ACCC oversight

Participants who responded 'unwilling,' 'neutral' and 'very willing' to sharing their data expressed "a lot more confidence" after finding out about the ACCC's involvement with CDR. They expected that the ACCC would carry out "very strict management / monitoring" of ADRs and that they would enforce any "[criminal] penalties related to the legislation."

2 out of 9 participants anecdotally stated that CHOICE's involvement would also boost their levels of confidence and trust.

"[Being able to verify] does give me more confidence... [The ACCC] are for the consumers so they're usually on our side. I'll have a lot more confidence if the ACCC have approved it, definitely."

— R2P4

Research objectives

D4: Understand if participants have a propensity to share their CDR data.

Reassurance that the CDR is "really secure"

One participant, who works with CALD and immigrant communities, suggested the inclusion of plain language reminders indicating "that this [CDR process] is really secure." They went on to explain that the use of industry jargon made it hard for them to understand what they had consented/authorised to share. Knowing this, they explained that "for some people, who English is not the first language, it's hard, so the information has to be there all the time for them so they know […] 'Yes, this is confidential.'"

"Because you asked me the question "What did you agree to?" I wouldn't remember what I agree to. [...] For some people, who English is not the first language, it's hard, [...] [so they know] 'is this what I agreed to, is this safer?'"

— R2P9

Research objectives

D4: Understand if participants have a propensity to share their CDR data.

Explanation of industry language and jargon

Two participants that gave a score of 4 (indicating a 'willing' response to sharing their data) wanted an explanation of "the jargon that an every-day consumer won't understand." They explained that without context, they were "not sure what sharing that information implies for [them]. If an explanation is provided [they] can make an educated decision whether [they] want to share that data."

"Explain the jargon that an every-day consumer won't understand. [...] I am not sure what sharing that information implies for me. If an explanation is provided I can make an educated decision whether I want to share that data"

— R2P1

Research objectives

D4: Understand if participants have a propensity to share their CDR data.

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

Consent/authorisation management

Understand consent management expectations for the energy sector

Managing consent

8 out of 9 participants understood that they would "self-manage" their previously consented/authorised data through the 'Settings' in Edison. Participants also mentioned that they could "send an email" to stop sharing their data.

When asked "How capable did you feel to stop sharing your data with Edison?" 9 Round 2 participants gave an average score of 4.4, indicating a 'capable' to 'very capable' response. 5 out of 9 participants gave a score of 5 (indicating a 'very capable' response to their ability to stop sharing their data).

Research objectives

D4: Understand if participants have a propensity to share their CDR data.
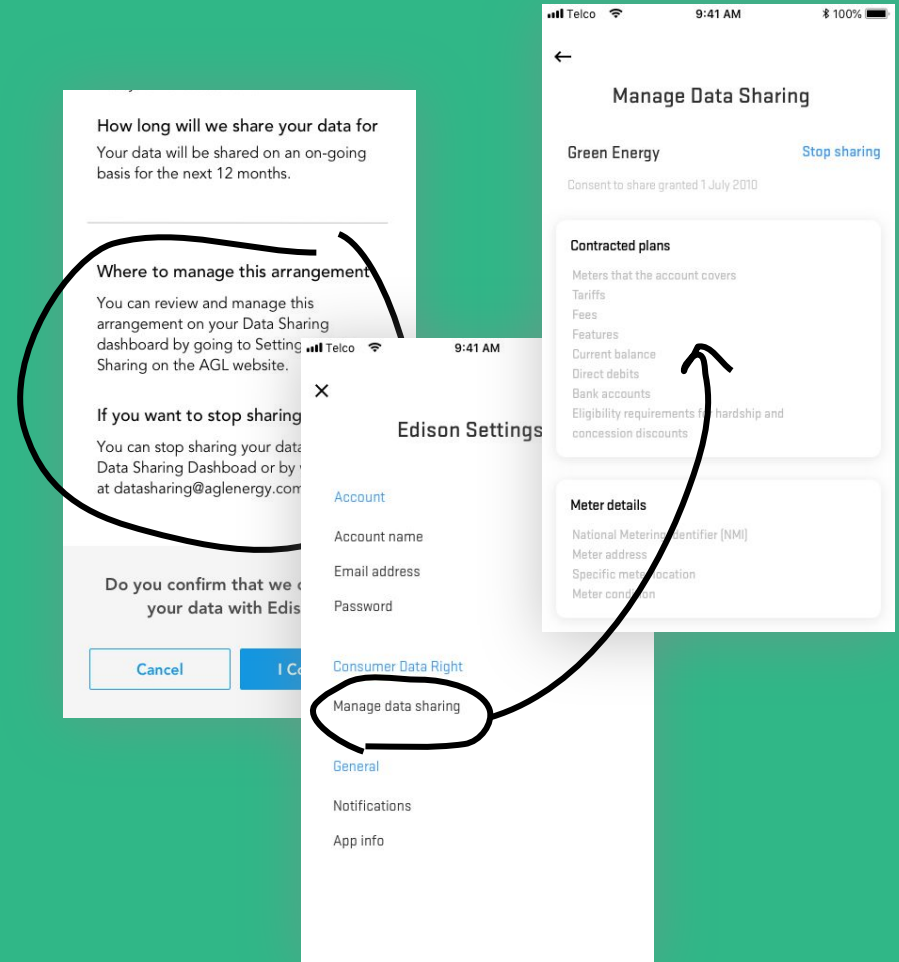
Reasons to stop sharing data

8 out of 9 participants explained that they would stop sharing their data if the company's reputation was tarnished in any of the following ways:

- "poor data handling practices" resulting in "privacy breach" and "leaks,"
- 'Terms of Use' breach such as "sharing information with other companies,"
- "identity theft" and "fraudulent activities,"
- "bad publicity," or
- the company "goes bust."

4 out of 9 participants also said that they would like to stop sharing their data if they were "no longer interested in the service" or found it "useful."

Research objectives

D4: Understand if participants have a propensity to share their CDR data.

"[I would stop sharing] if I was no longer interested in the service the company was providing by using my data. I would also decide to stop sharing my data if the company was caught using poor data handling practices (data leaks, etc.)"

— R2P1

Data Standards Body | Consumer Experience Workstream

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