CONSUMER
DATA
STANDARDS

GippsTech

Consumer Data Standards: Consent Flow

Phase 2 CX Stream 1 Report

June 2019

Table of Contents

Executive Summary

Stream 1: Consent Flow

Overview of this research

The Australian government is introducing a Consumer Data Right (CDR) to give consumers greater control over their data. The CX workstream aims to help organisations to provide consumers exercising their rights under the CDR with a trusted and usable consent experience.

This report is part of Phase 2 of this research. It is one of three streams of research, focusing on refining the consent flow, including authorisation of data sharing and creating an accessible and inclusive mechanism for consent, as well as investigating joint account and cross-sector use cases.

This stream's research involved a total of 31 participants. Participant selection was skewed towards younger people and early adopters, as these were likely to be the first users of the CDR. Participant selection also focused on participants from disadvantaged or marginalised groups such as people with disabilities, LGBTQI+ people, immigrants and people from non-English speaking backgrounds, and people who had experienced financial disadvantage. Participant selection include a diversity of demographics including age and gender, 6 states and territories, and participants located across metropolitan areas, large regional centres and remote/rural areas.

In Round 1, participants were asked to interact with 3 prototypes: first sharing banking data with a fictional Life Manager app, then connecting an energy account to the app, and finally sharing financial data for a joint account. Round 2 was conducted similarly, but had improvements to the prototypes arising from Round 1 feedback.

Key findings

1. **Trust and safety**: participants needed to be able to trust the process and all entities involved; to know that their data was safe; to know that sharing their data would do them no harm. Participants did not feel safe sharing financial data due to concerns about identity theft; data being used for marketing; or accessed by third parties.
2. **Transparency and accountability:** participants wanted more information about the data recipient, data security requirements, and how data recipients would be held accountable.
3. **Agency and self-directed choice:** participants strongly preferred to have control over the data sharing process, and found too much automation invasive. Automation should not be the only option.
4. **Accessibility and clarity:** participants preferred information presented on one page, with clear language and unambiguous explanations, and noted that visual accessibility was crucial.
5. **Vulnerability and disadvantage**: Participants from vulnerable backgrounds had greater concerns about possible harm arising from misuse of their data and generally wanted more control over data sharing due to those concerns.

Executive Summary

Stream 1: Consent Flow - Recommendations

Information

- Critical information should be up-front and on-screen.
- More information is better as long as it’s clearly explained, particularly information on accountability and penalties for data recipients if they break rules.
- Trust Mark accreditation should be easily verifiable by linking it to the data recipient’s specific accreditation data on a government website.
- Require data recipients to provide information about measures taken in case of security breaches.

Accessibility

- Require compliance with strong accessibility standards.
- CDR helpline or contact information should be available in multiple languages.
- CDR info site should have full translation functionality and be fully screen-reader accessible.

Joint accounts and energy consent flow

- Joint accounts should require multi-party approval; the majority of participants expressed concern about possible abuse of any process that did not require approval from joint account holders.
- Energy consent flow should ask for user input rather than automatically detecting energy providers, and should avoid jargon (eg. NMI) and use clear language.

Designing for vulnerable users

- Further consultation is needed with specific groups focused on issues faced by vulnerable users, as these users have more concerns about data misuse.
- Information on data views, including specific data held by the data holder and accessed by the data recipient should be made available to users upon request.
- Strong opt-out and manual data entry: vulnerable users were particularly concerned that their data would continue to exist in the system after revoking consent. Data recipients should be required to explain what happens to data on opt-out, and to provide a manual data entry option.

Overview

Overview

Stream 1: Consent Flow

Overview of the CDR

The Australian government is introducing a Consumer Data Right (CDR) to give consumers greater control over their personal data. Part of this right requires the creation of common technical standards that make it easier and safer for consumers to access data held about them by businesses, and – if they choose to – share this data via application programming interfaces (APIs) with trusted, accredited third parties. The Consumer Data Right is intended to apply sector by sector across the whole economy, beginning in the financial sector before expanding into the energy sector, followed by telecommunications.

Data61 has been appointed as the Consumer Data Standards (CDS) team to develop standards that enable consumers to access and direct the sharing of data about them with third parties flexibly and simply, and in ways that ensure security and trust in how that data is being accessed and used. There are several work streams currently being delivered by Data61 including the API, Information security, Engineering, and Consumer Experience (CX) workstreams.

The ultimate aim of the CX workstream is to help organisations provide consumers exercising their rights under the CDR with trusted and usable consent experience.

Phase 1 of the CX workstream was recently completed. The key objectives of this phase was to develop a foundational pattern for consent, referred to as a Consent Flow, which is part of an overall Consent Model. The first report can be found at: https://consumerdatastandards.org.au/resources/reports/reports-cx/phase-1-cx-report/

In phase 2, the CX workseam was split into 3 streams of work. They were tasked to specifically look into refining the consent flow, joint accounts, dashboards, revocation, reauthorisation, notification, authentication and cross sector applications.

This report is specifically about stream 1, which was charged with refining the consent flow, including authorisation of data sharing and creating an accessible and inclusive mechanism for consent, as well as investigating joint account and cross-sector use cases.

The recommendations do not reflect the position of the Consumer Data Standards body, and will need to be reviewed (e.g. against security implications). This process may result in different recommendations.

Methodology

Methodology

Research principles

Diversity

Our recruitment process aimed for a diverse range of participants in order to test the prototypes with a set of participants who were representative of a wide range of situations that exist in the Australian population.

Marginalisation and accessibility

We made a deliberate effort to reach out to people belonging to marginalised groups, since accessibility should be a fundamental aspect of the consent flow - not an afterthought. In addition, marginalised people are historically not considered in the design of technological and societal innovations; if they are considered, they are treated as edge cases. Our approach to the design research reflects our belief that there should be no edge cases where accessibility and usability are concerned; that is, we will design with a focus on making the consent flow as accessible, usable, and inclusive as possible - bearing in mind that there is no such thing as a final design that will perfectly encompass all so-called edge cases.

Avoiding tokenism

In our recruitment we aimed to avoid tokenising people belonging to marginalised groups, eg. a “token person with disabilities” or “token Aboriginal person”. In recruiting for people based on their disability or their ethnic or cultural identity, we always aimed to recruit several people so that the burden of being the single “representative” of that group did not fall on anyone’s shoulders.

Clear communication and respect for participants

In preparing for the research sessions we acknowledged the fact that we skewed selection of participants towards marginalised groups, and explained our principles for how we conducted the research sessions. To guide our researchers in facilitating interviews, we laid down the ground rules: “We acknowledge and respect the intersections of marginalisations: that is, people may belong to multiple marginalised groups, and our recruitment process will reflect that reality. We fully recognise that people are more than the sum of their identities, and we will conduct all interactions with participants with respect, thoughtfulness, sensitivity, and empathy.”

Methodology

Recruitment strategy

Age and technology skill level

Participant shortlists were skewed towards younger people and early adopters, as these were likely to be the first users of the Consumer Data Right. This was done by selecting more people from the 18-30 (and to a lesser extent, 31-40) age ranges. Early adopters were chosen through examination of their responses about the kind of apps they had installed on their mobile phone as well as their comfort level with technology and dependence on the internet for daily tasks. Round 1 participants were drawn mostly from responses to the screener survey, whose respondent makeup itself was skewed towards younger people and early adopters: 37.3% were in the 18-30 age range and 35.2% were in the 31-40 age range, compared to 18.8% for 41-50 and 8.7% for 51-60.

Vulnerability, disadvantage and marginalised groups

We aimed for strong representation of people belonging to marginalised groups, in particular:

1. people with disabilities
2. culturally and linguistically diverse (CALD), immigrants, non-White people, and people for whom English is a second language
3. LGBTQI+ people
4. Aboriginal and Torres Strait Islander people
5. low-income groups and people who have experienced financial distress

Diversity of demographics

We aimed to have a diverse range of demographics represented, to ensure that differences in behaviour and attitudes between different demographic groups were captured in the results. Specific aspects of demographics that we ensured had a wide range:

1. Age: from 20s to 60s, skewing towards 18-30 and 31-40 ranges
2. Geography: VIC/NSW vs other states
3. Location: metropolitan/inner city, suburban/outer city, large town, small/remote town, rural
4. Individuals and sole traders
5. People who had experience of separating from a partner with whom they had a joint bank account

Recruitment process

A screener survey was set up on Google Forms with questions designed to screen out unsuitable candidates and to enable selection of participants based on the above criteria. A call for research participants was published on Facebook, with a link to the screener survey and a note about being compensated $100 for participating in design research. Facebook ads were used to reach a wide target audience, with the $100 compensation being used as an incentive to participate. Over 300 people filled in the screener survey, which allowed a large enough sample of people in each of the above categories to be invited to participate in interviews. 69% of people invited to participate (31 out of 45) were actually interviewed - the remainder were not able to be interviewed due to time and/or scheduling constraints.

Methodology

Recruitment strategy

Participation

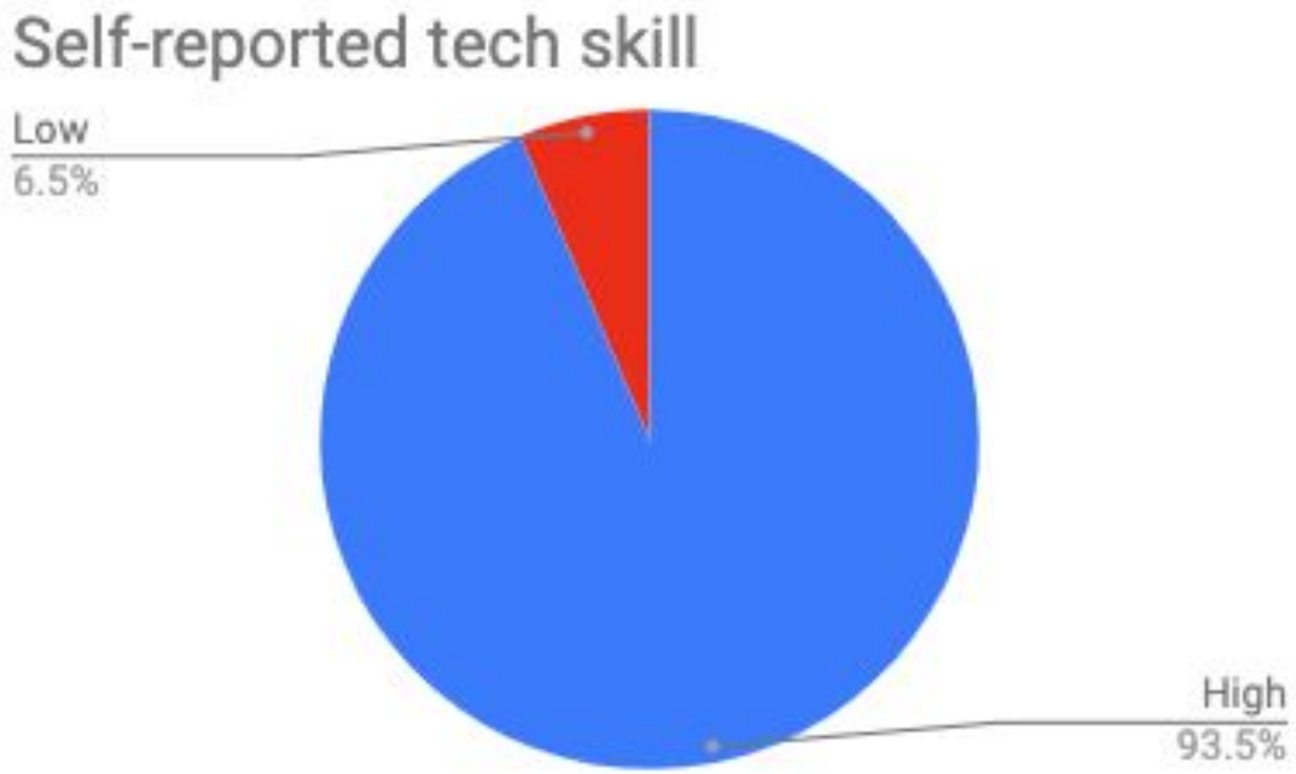
In Round 1 we interviewed 15 participants with 9 of these being in-person interviews. The remaining 6 interviews were done remotely via the internet and participants were domiciled across 4 states VIC, NSW, WA and QLD.

In Round 2 we travelled to Yeppoon Queensland representing a remote or rural community and interviewed 11 participants in-person. Round 2 was completed by interviewing an additional 5 participants remotely that represented our target demographics. Round 2 participants were drawn from QLD, SA, NSW, TAS, VIC and WA.

A total of 31 participants were interviewed for Stream 1.

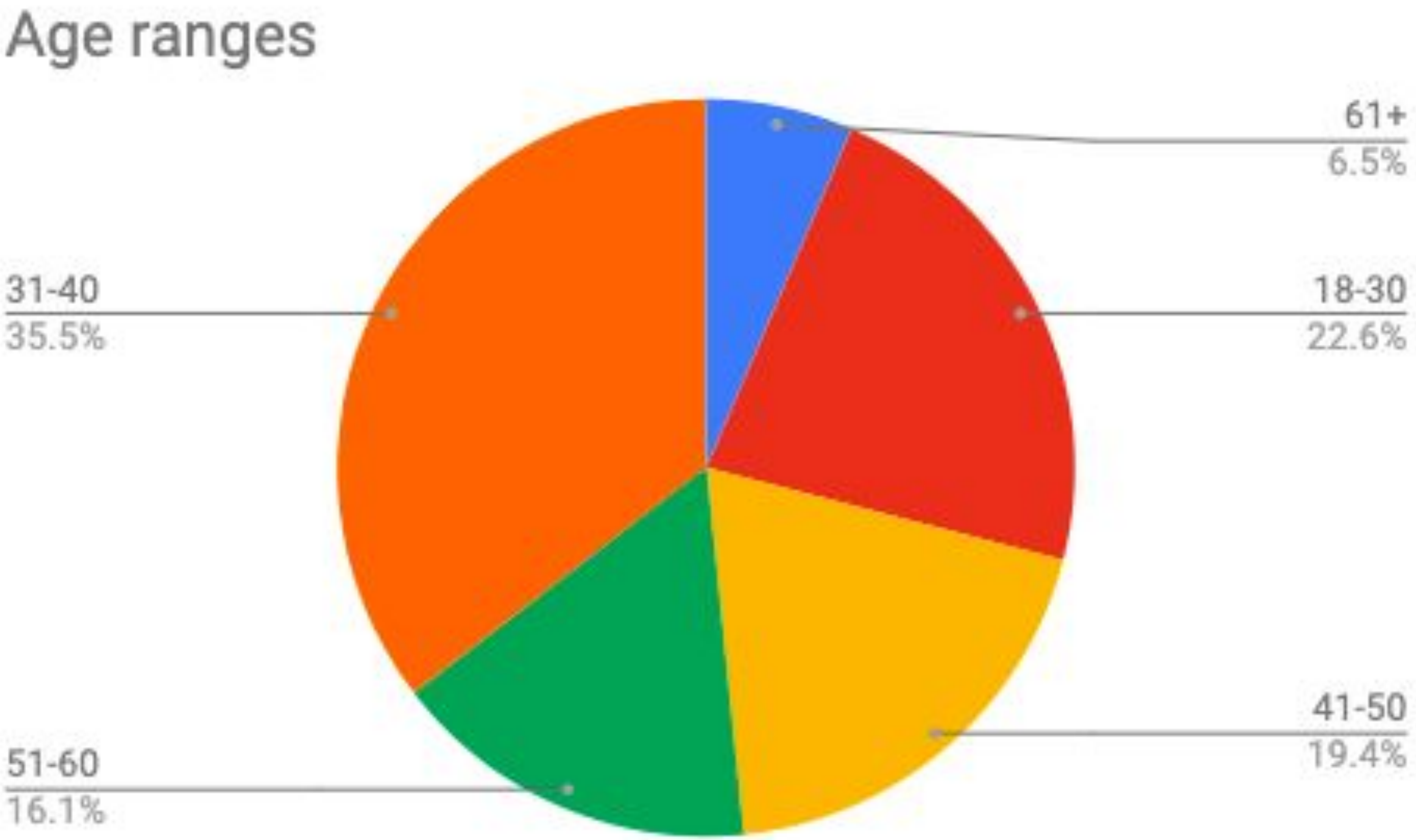
Methodology

Recruitment results / participant overview: Participant tech skill (self-reported) and level of comfort with internet technology



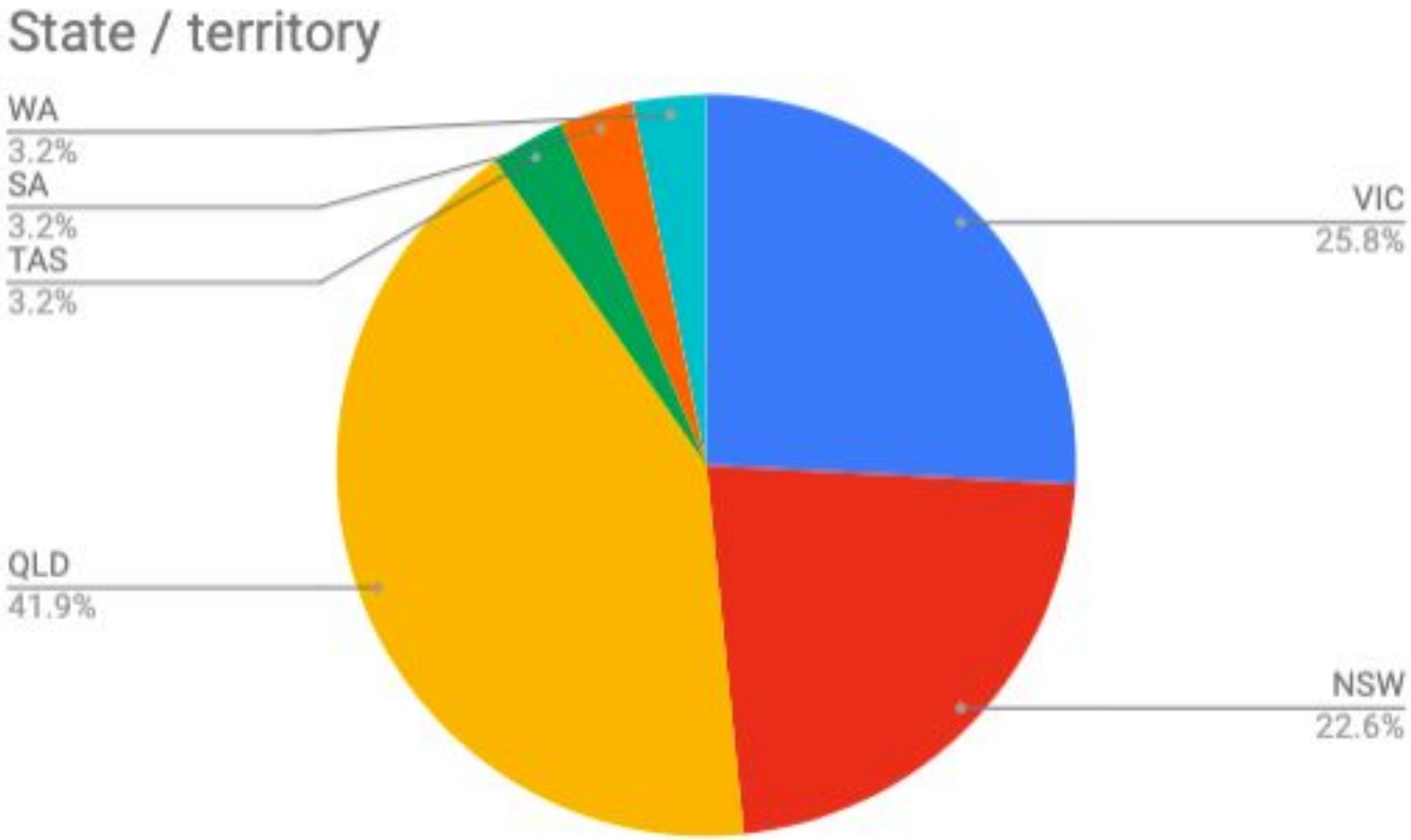
Methodology

Recruitment results / participant overview: Participant age ranges



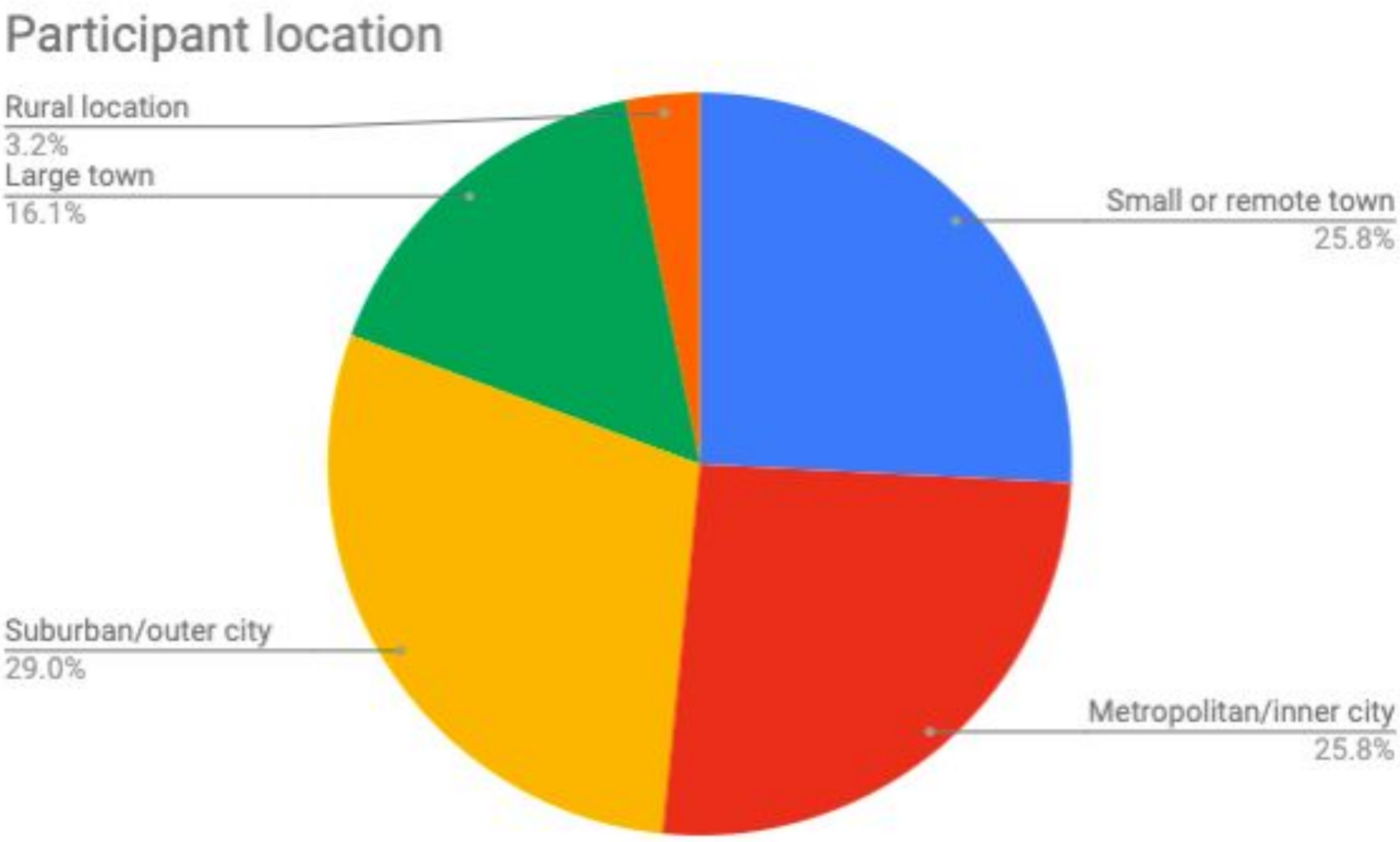
Methodology

Recruitment results / participant overview: Participant location by state



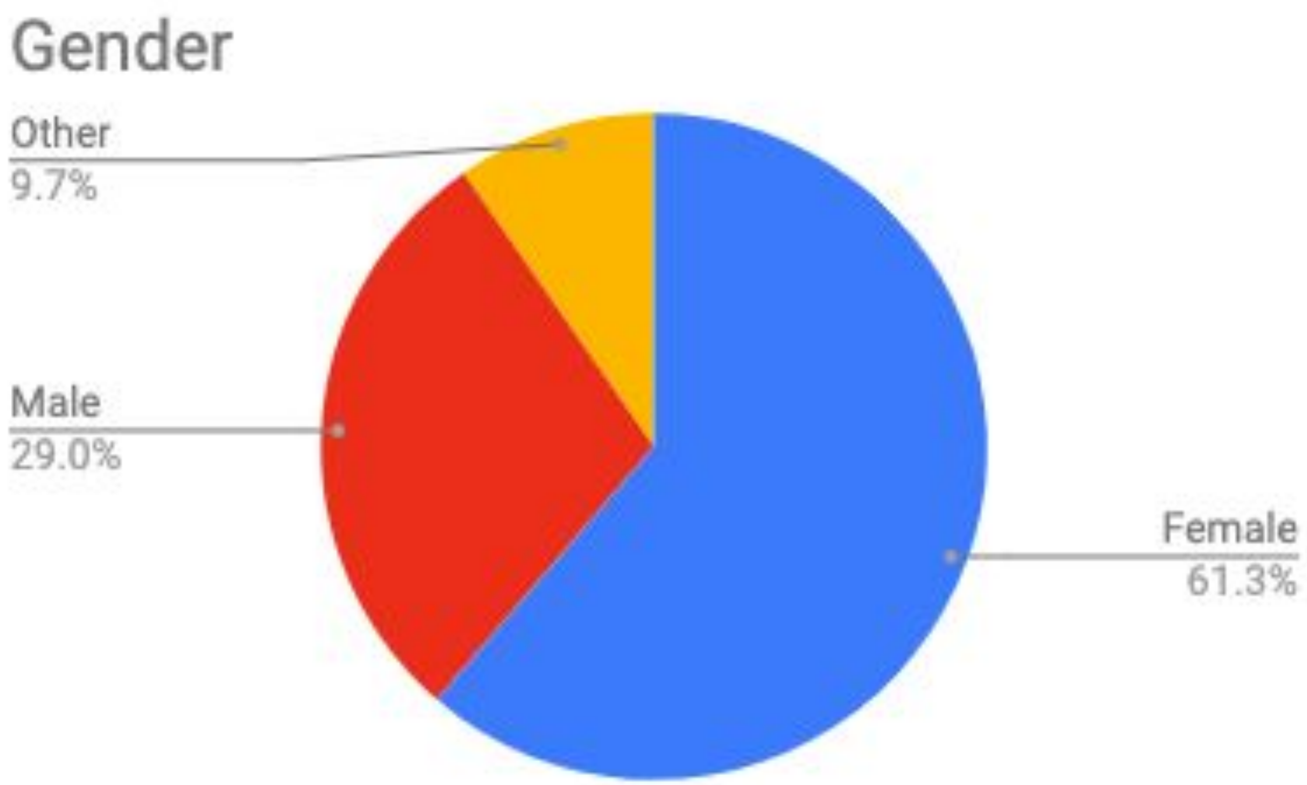
Methodology

Recruitment results / participant overview: Participant location type



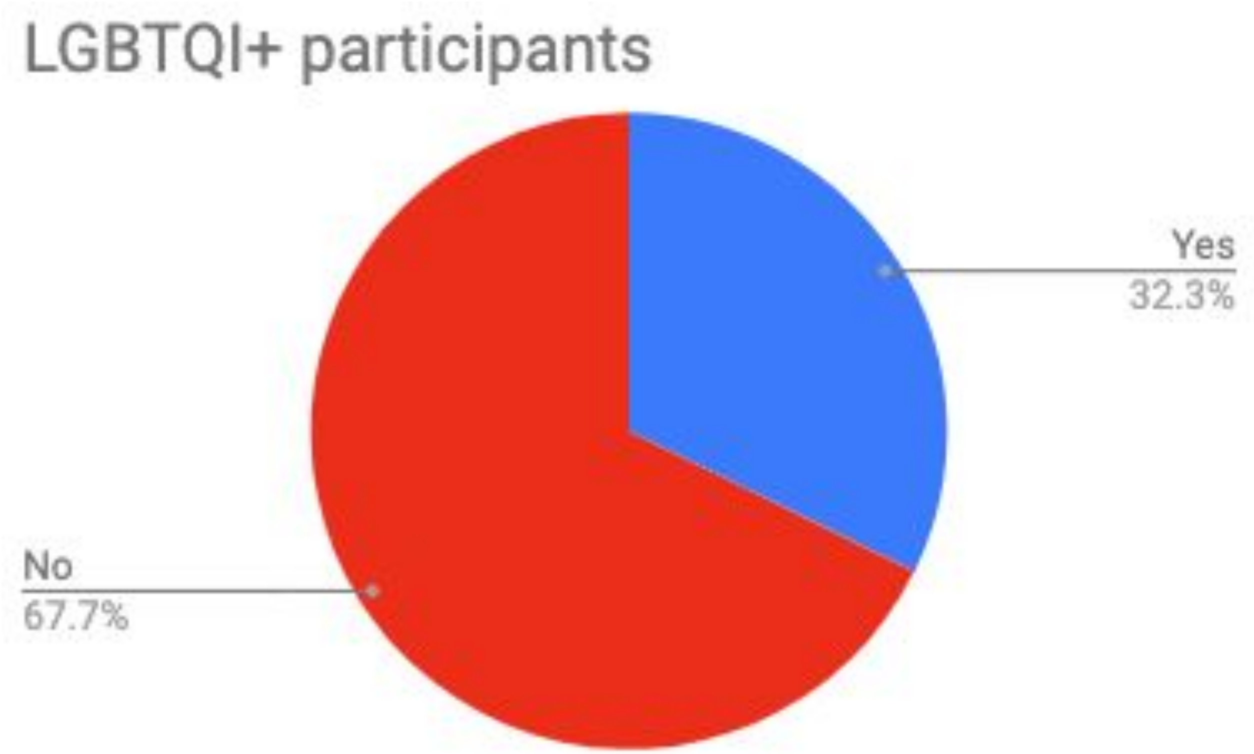
Methodology

Recruitment results / participant overview: Gender
“Other” includes asexual, nonbinary, genderqueer, and agender participants



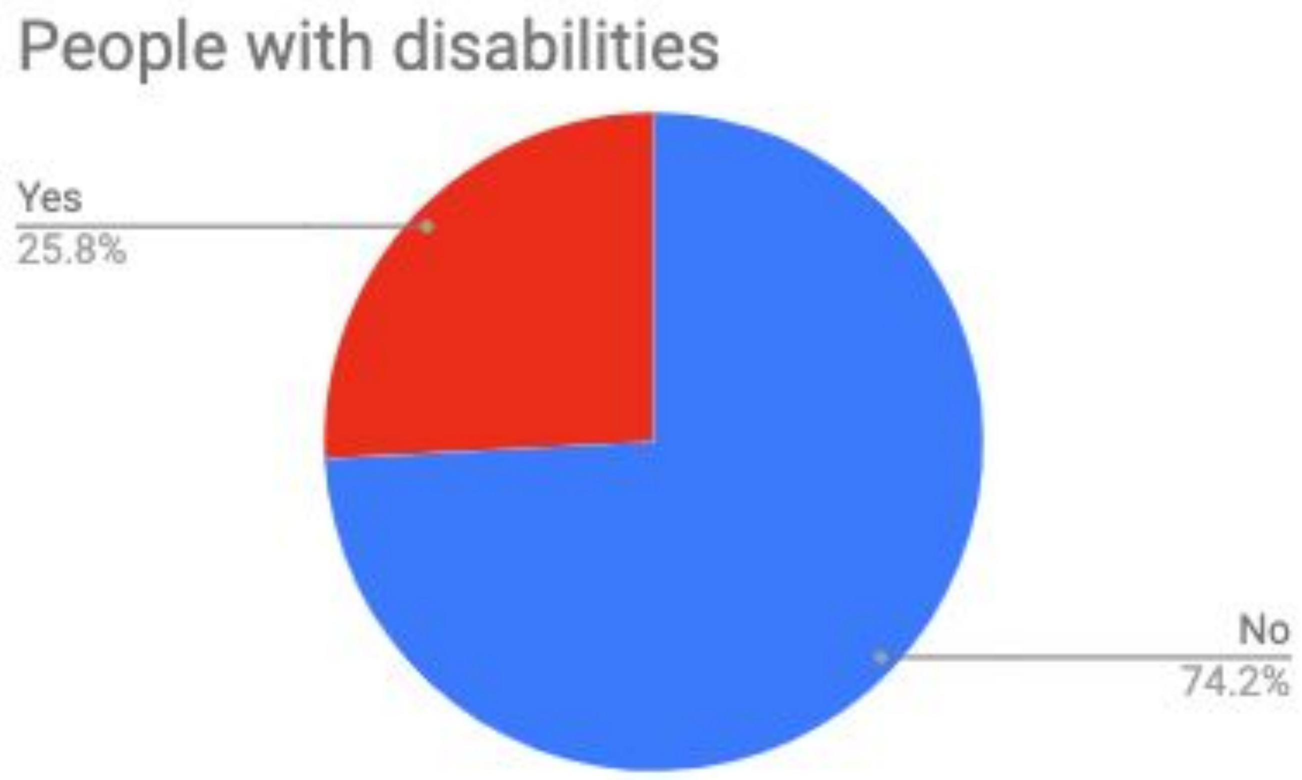
Methodology

Recruitment results / participant overview



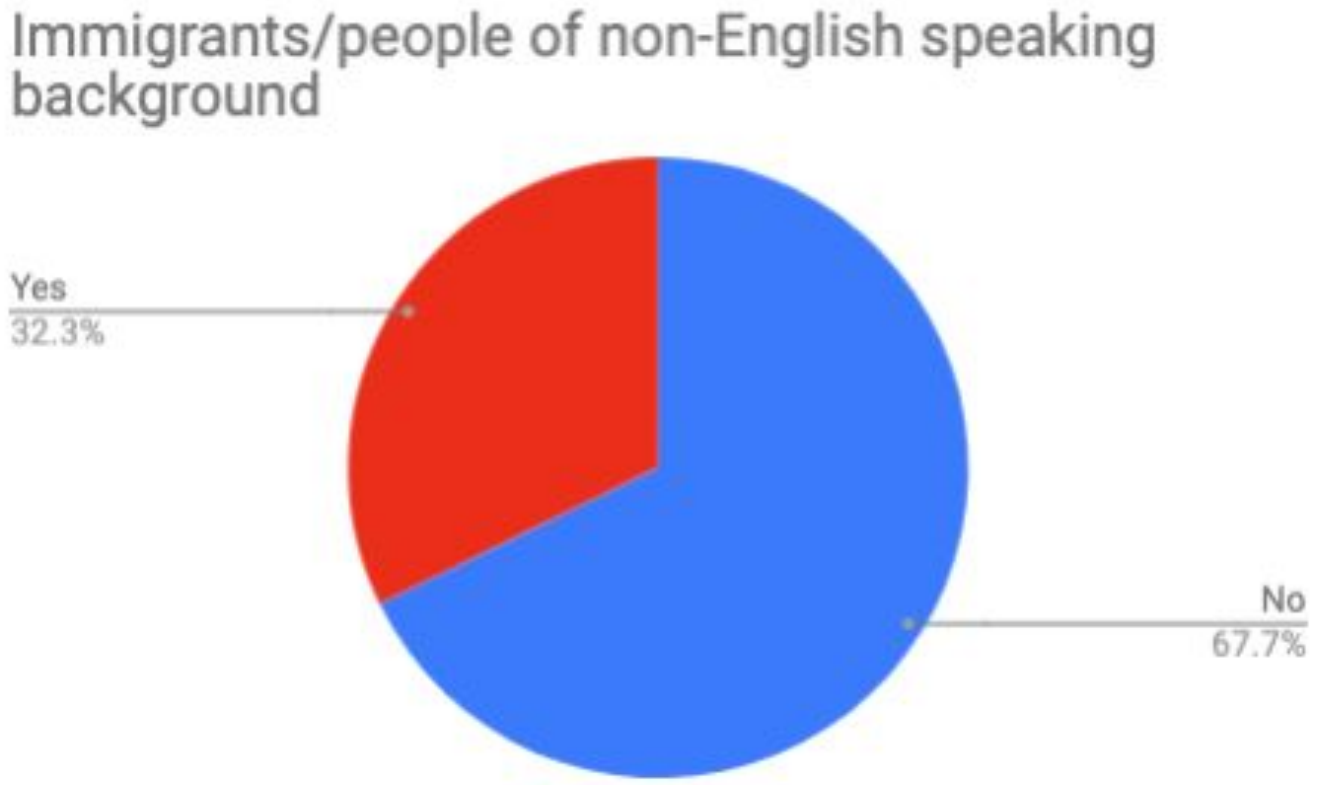
Methodology

Recruitment results / participant overview: people with disabilities



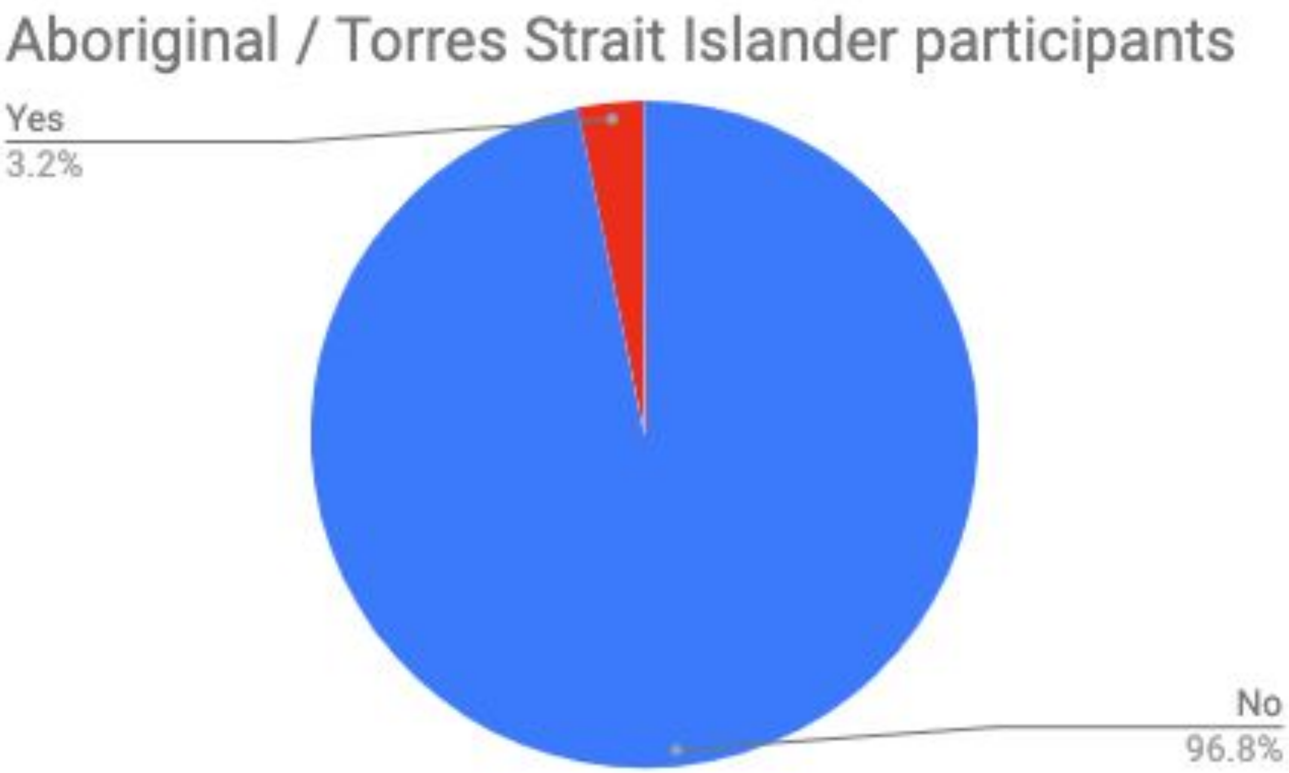
Methodology

Recruitment results / participant overview: immigrants, people of non-English speaking background



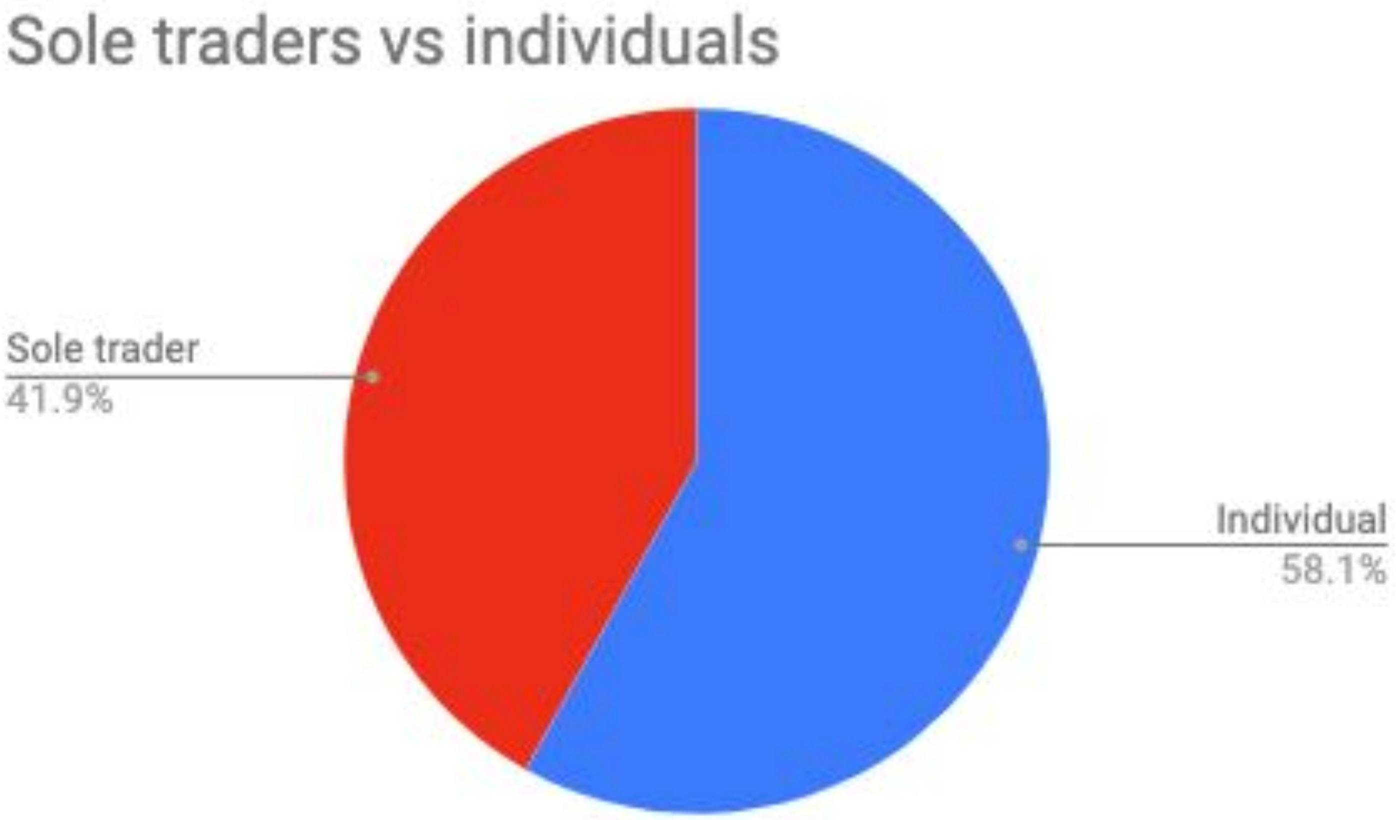
Methodology

Recruitment results / participant overview: Aboriginal and Torres Strait Islander participants



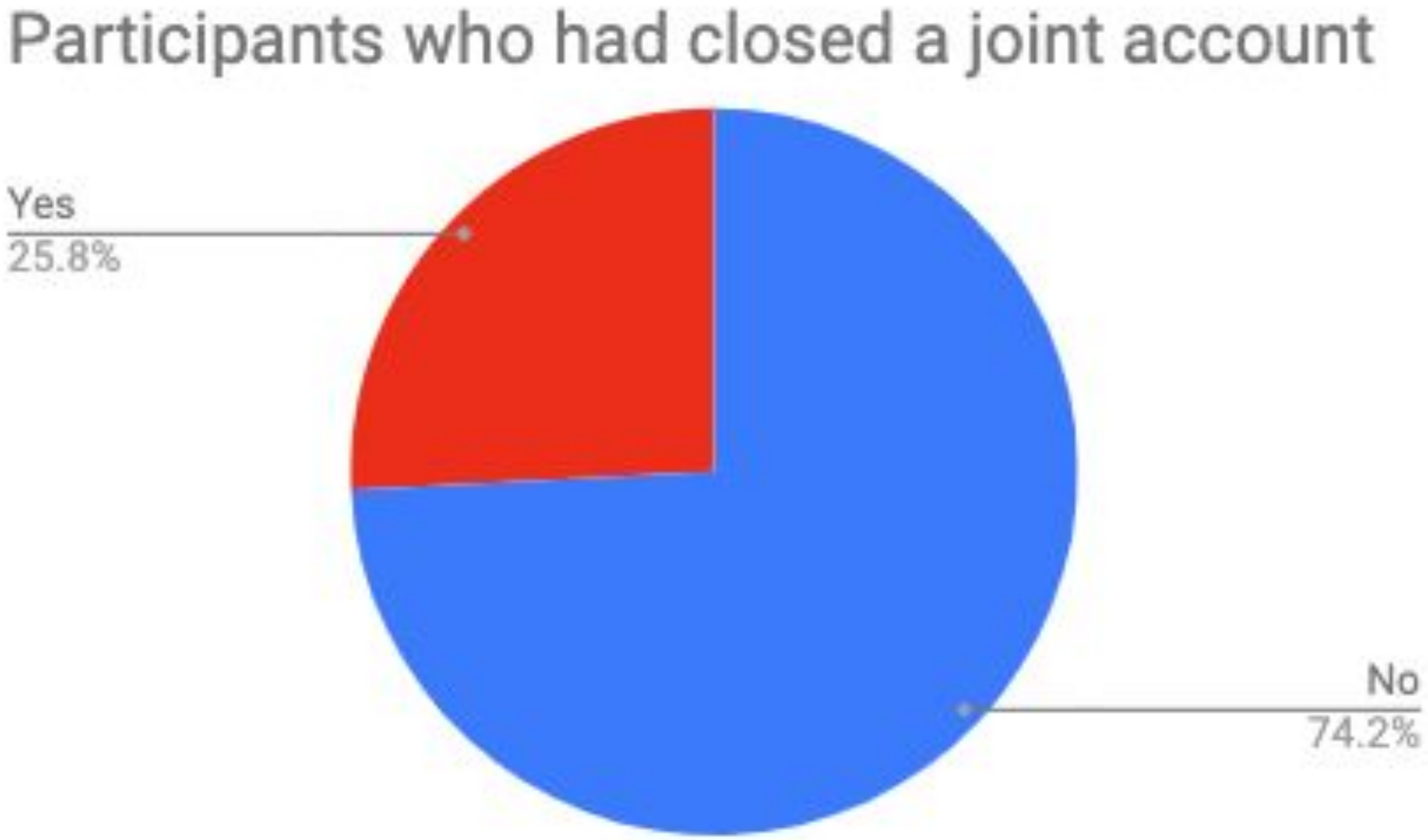
Methodology

Recruitment results / participant overview: sole traders



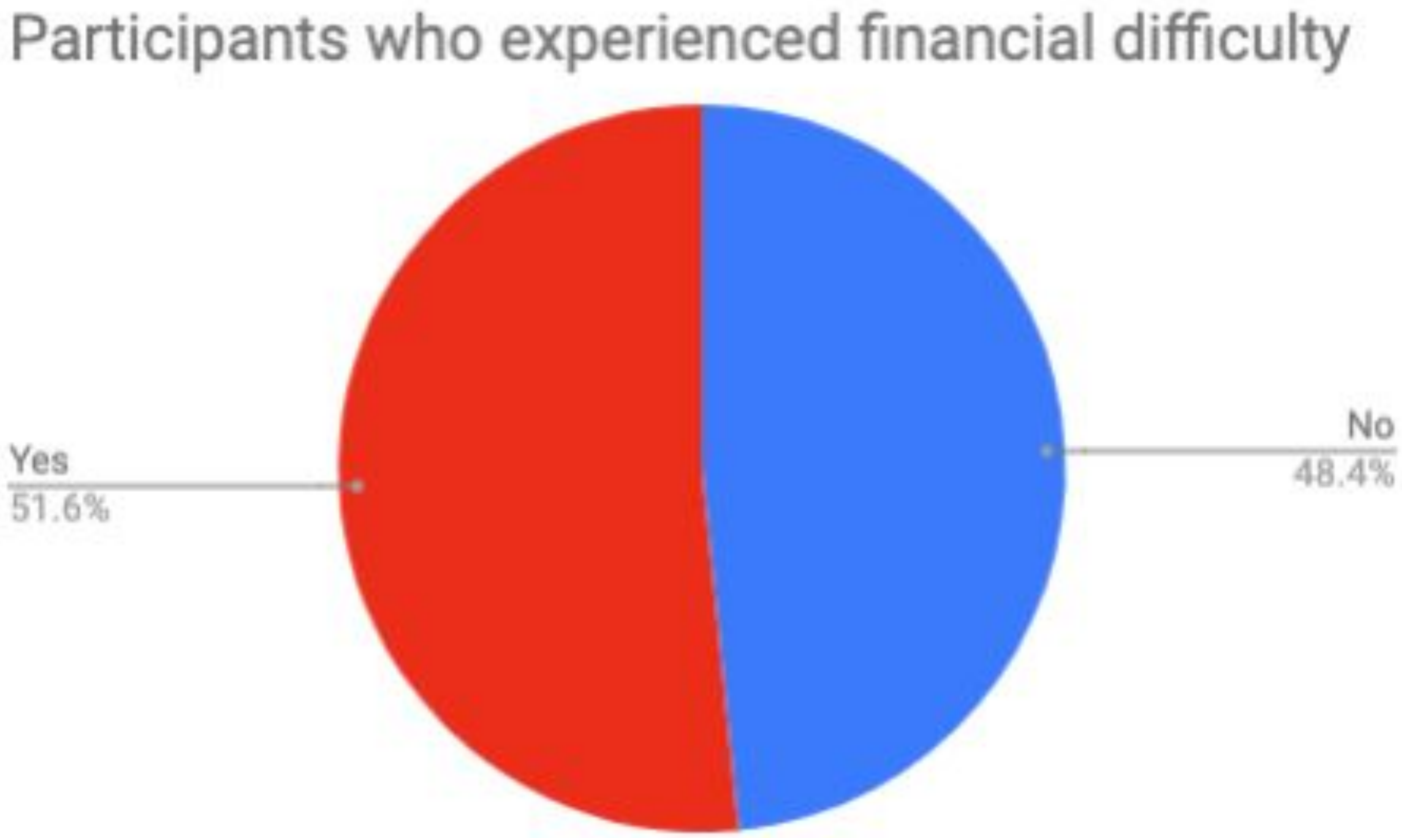
Methodology

Recruitment results / participant overview: Participants who previously held a joint account with a partner and closed it after separation from partner



Methodology

Recruitment results / participant overview: participants who have experienced financial difficulty in the past/are experiencing financial difficulty



Methodology

Session outline

Consent flow prototypes

Participants were asked to test three prototypes:

1. **Basic consent flow:** A prototype of the consent flow, asking participants to sign up for a LifeManager app that would help them manage their budget, and go through the consent flow to allow the app to access their banking data.
2. **Cross-sector energy flow:** A prototype that moved participants from the banking sector to the energy sector. Participants were asked to go through the consent flow for energy and set up data sharing for their energy account.
3. **Consent flow with joint accounts:** The banking consent flow modified by joint accounts. This was tested in two iterations over the two rounds, both as an optional notification prototype and a multi-party approval prototype.
4. **Round 2 interviews** were conducted in a similar fashion once feedback from Round 1 interviews was incorporated to improve the prototypes.

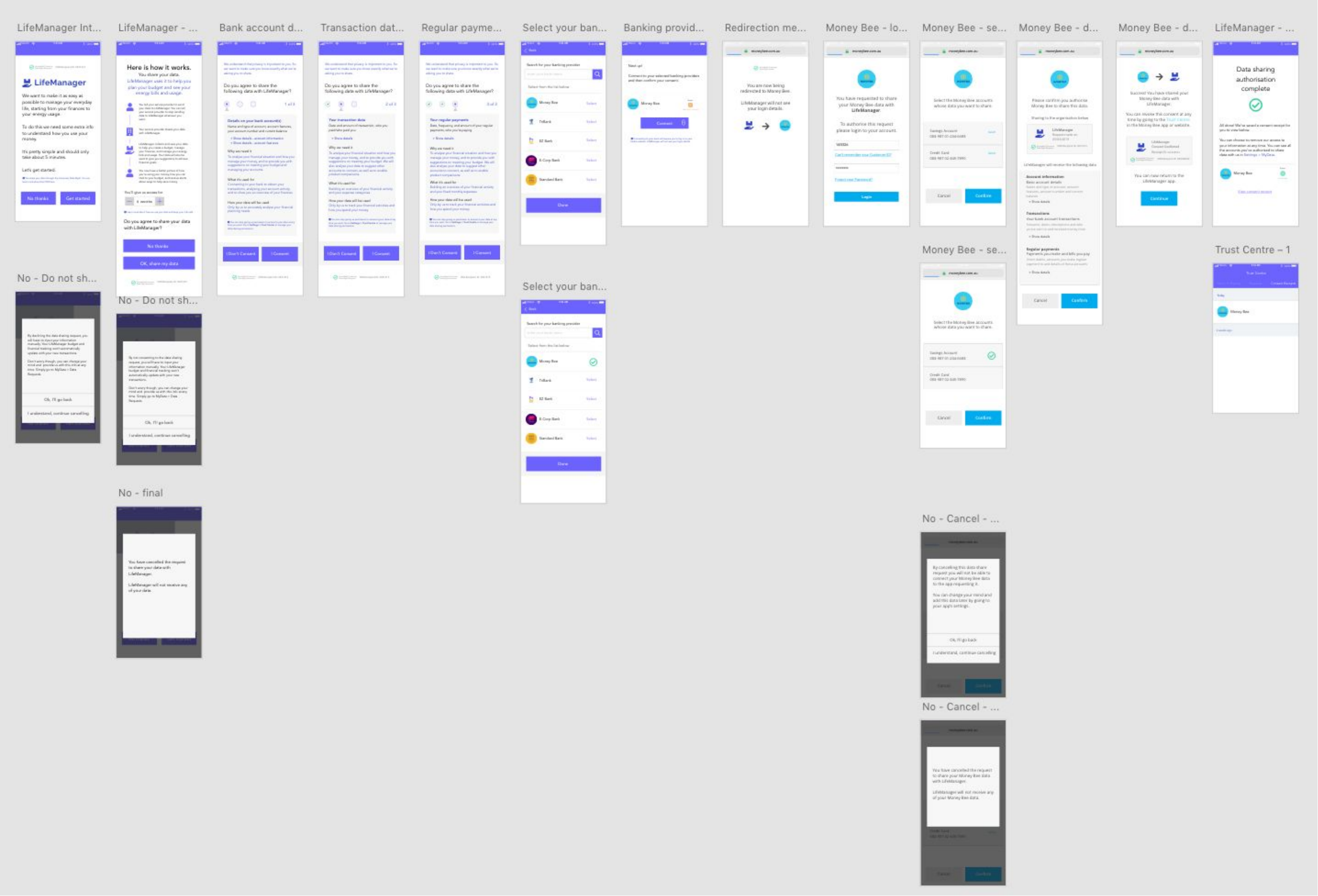
Initial thoughts vs specific questions

For the first prototype, participants were asked to go through the consent flow with minimal guidance from the interviewer and no specific questions to bias their thinking or to draw their attention to aspects they may not have noticed on their own. Interviewer comments were kept to a minimum during interaction with the first prototype in order to be able to capture the participant’s first impressions and to test their ability to understand the consent flow without external input. After participants completed the consent flow in the first prototype, the interviewer asked specific questions to test their understanding of the consent flow process, and asked more detailed questions in subsequent prototypes to get more information about specific aspects of the design.

Consent flow

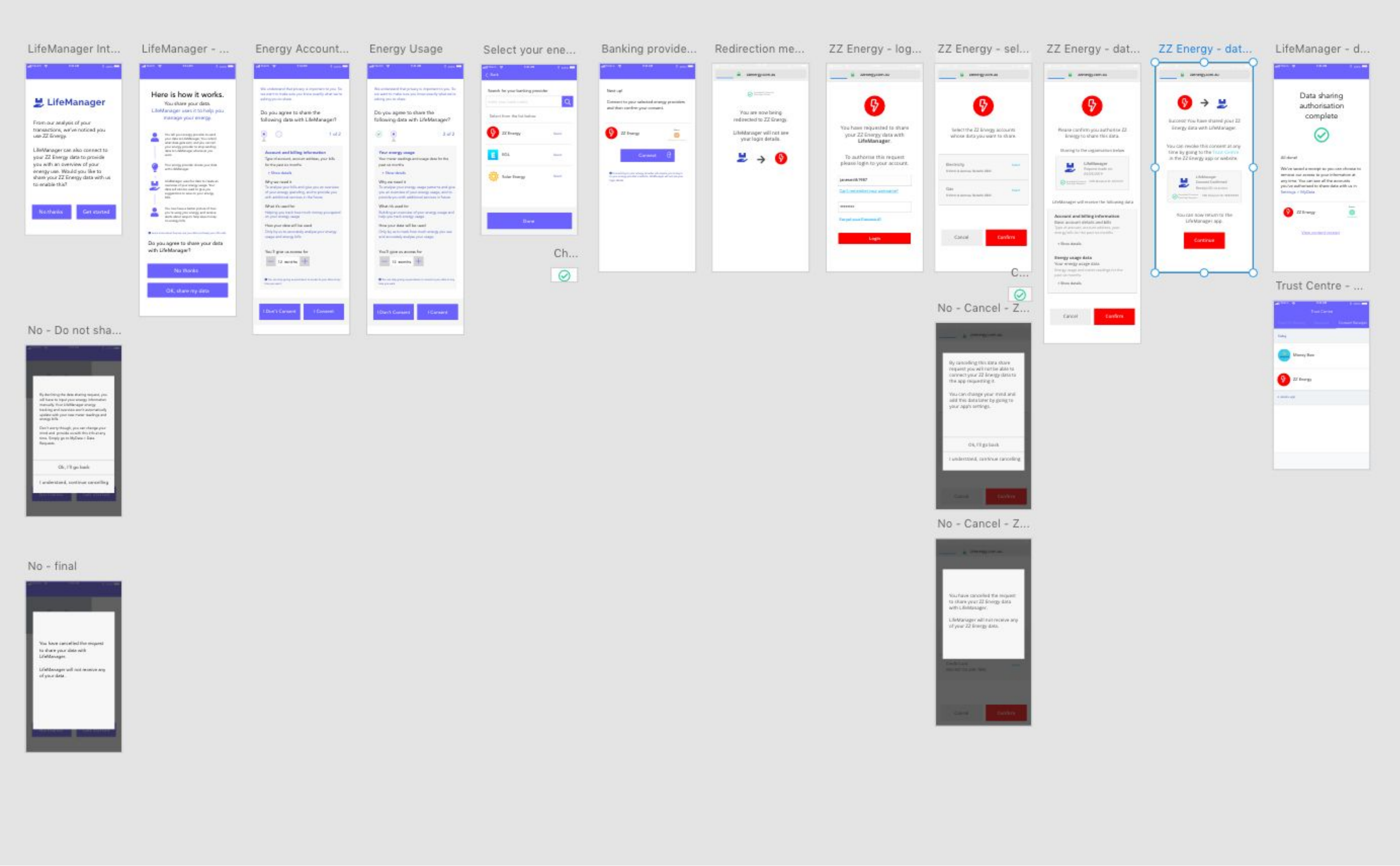
Overview

Round 1, prototype 1: basic consent flow



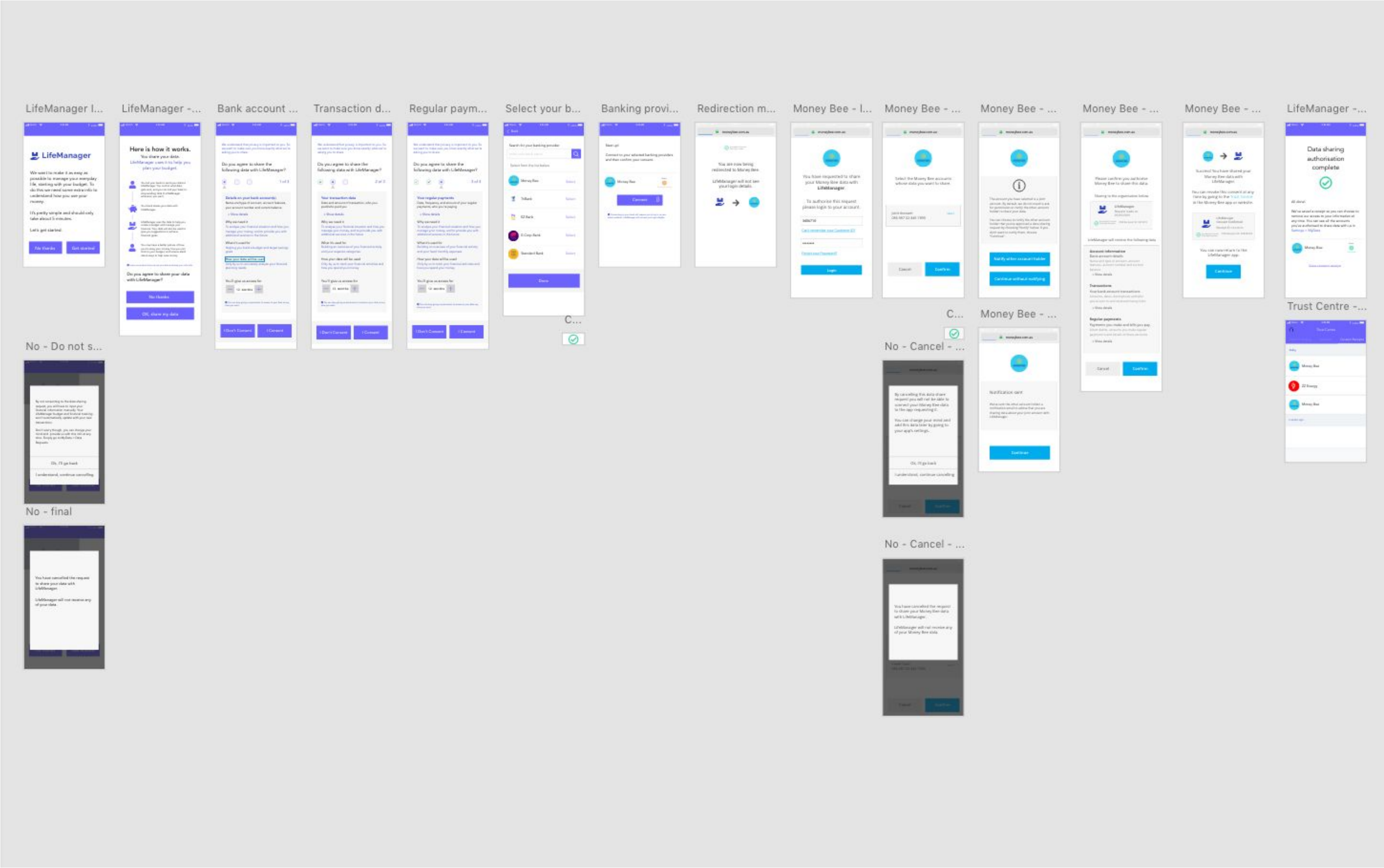
Overview

Round 1, prototype 2: cross-sector energy consent flow



Overview

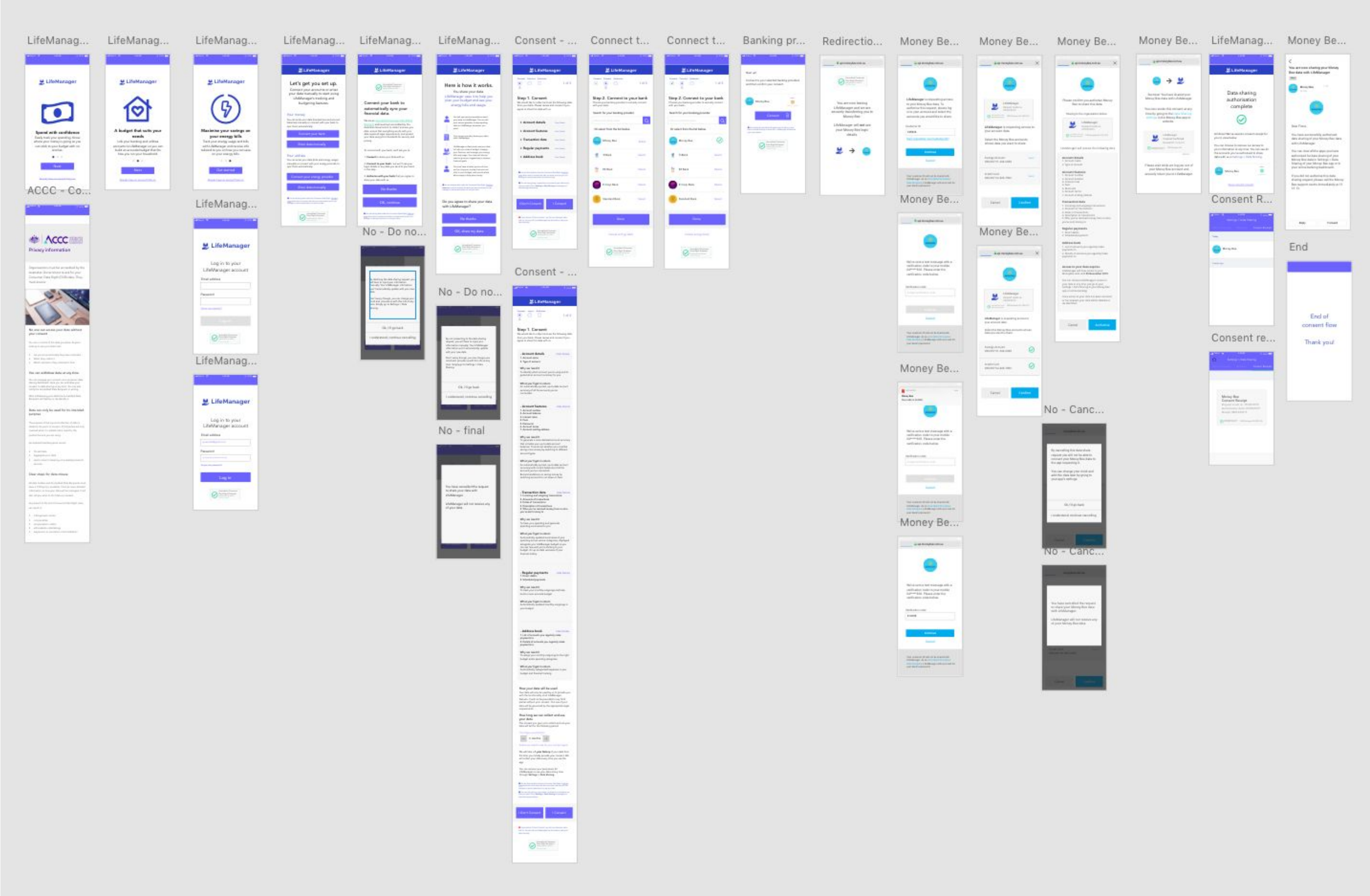
Round 1, prototype 3: banking with joint account - optional notification



Overview

Round 2, prototype 1: revised consent flow

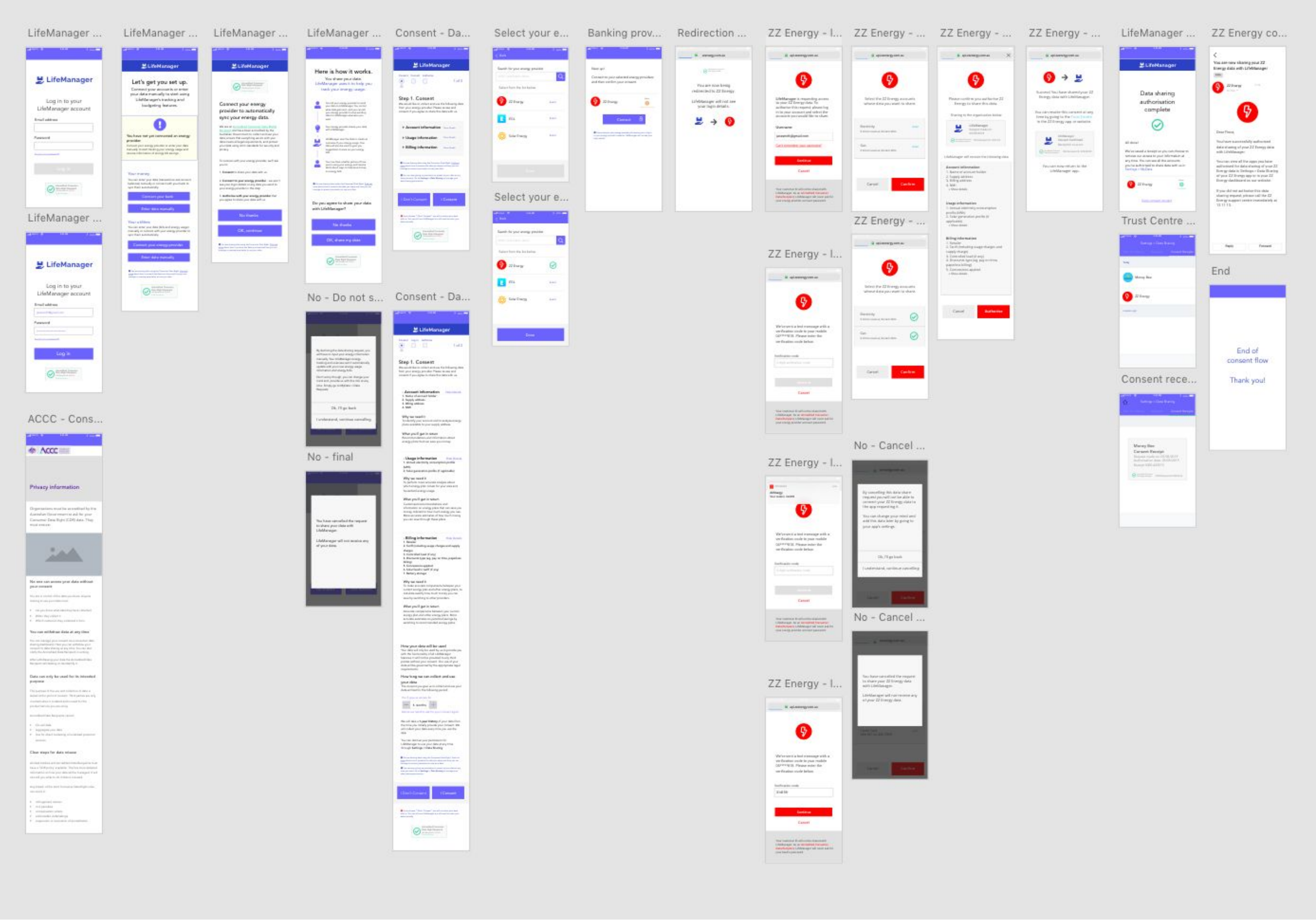
1. Expanded value proposition for data recipient app
2. ACCC one-pager
3. Basic account setup screen added
4. Three-step process explainer screen added
5. Data cluster screens changed from multi-screen consent to accordion format
6. Authorisation screens changed to conform with One-Time Password authentication



Overview

Round 2, prototype 2: revised cross-sector energy consent flow

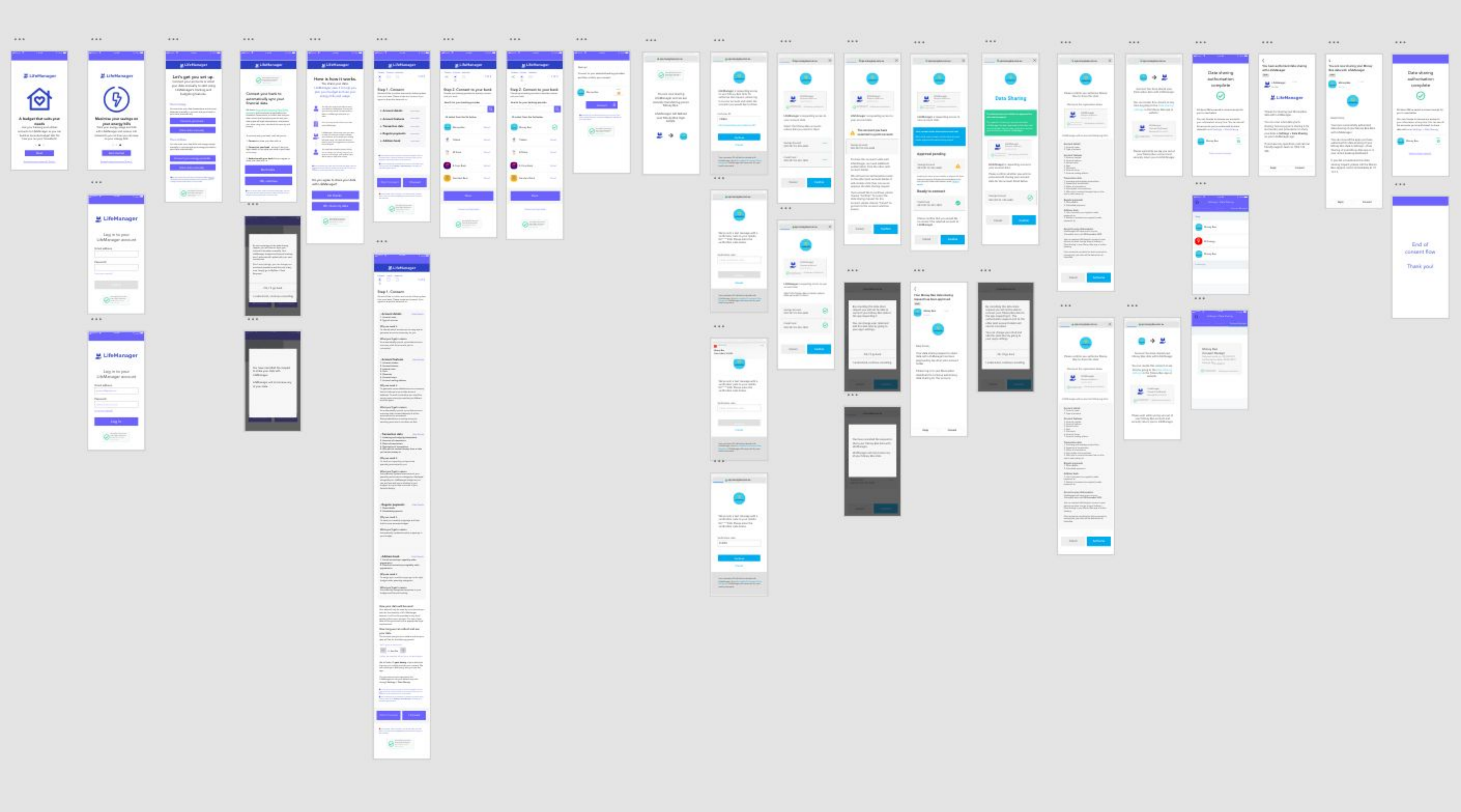
1. Expanded value proposition for data recipient app
2. ACCC one-pager
3. Basic account setup screen added
4. Three-step process explainer screen added
5. Data cluster screens changed from multi-screen consent to accordion format
6. Authorisation screens changed to conform with One-Time Password authentication
7. Cross-sector function changed: alert does not specify energy provider



Overview

Round 2, prototype 3: revised consent flow with joint account

1. Expanded value proposition for data recipient app
2. ACCC one-pager
3. Basic account setup screen added
4. Three-step process explainer screen added
5. Data cluster screens changed from multi-screen consent to accordion format
6. Authorisation screens changed to conform with One-Time Password authentication
7. Joint account alert: requires authorisation from other joint account holder, data sharing is “pending” until authorisation received



Key findings

CONSUMER
DATA
STANDARDS

Key findings

Overview

Note: These findings were gleaned from the research undertaken and specific prototypes used and may not necessarily apply to different models, mechanisms, or use-cases.

Trust and safety

Participants needed to be able to trust the process and all entities involved; to know that their data was safe; to know that sharing their data would do them no harm. Participants were unlikely to trust the app if they felt the value proposition was weak, but the Trust Mark had a significant impact on improving trust. However, participants still did not feel safe sharing their financial data due to concerns about hacking and identity theft; their data being used for targeted marketing; or concerns around access by third parties similar to concerns around MyHealthRecord.

Transparency and accountability

Participants responded favourably to information being presented to them upfront, even at the risk of overwhelming them with too much text. They asked for more information about the data recipient and data security requirements, and wanted to know how the data recipients would be held accountable both on the government and legal levels, and on the consumer level.

Agency and self-directed choice

Even when they had understood and given consent for the data recipient to analyse their data and make suggestions of providers to connect, participants strongly preferred the option to direct this process and initiate connecting a new provider. Participants placed a high value on having control over the data sharing process, even with the trade-off of having to go through more steps.

Accessibility and clarity

Lack of accessibility throughout the process was a major barrier to consent flow completion. This included visual accessibility considerations as well as clarity both in terms of visual design and in terms of language — some participants felt that core information screens relied too heavily on jargon.

Vulnerability and disadvantage

Participants from marginalised backgrounds, who had experienced difficult circumstances, or were in vulnerable/disadvantaged situations were less likely to trust the data sharing process or the data recipient. They were more likely to assume that their data would be misused in a way that caused them harm.

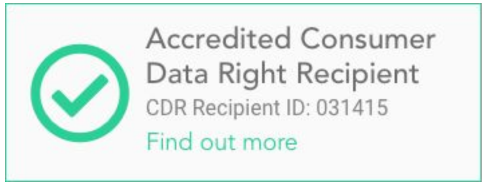
Trust and safety

Building trust

The Trust Mark

The majority of participants found the Trust Mark to be helpful in identifying the data recipient as trustworthy. For some participants, the Trust Mark drew their attention to the data holder’s Consumer Data Right Accreditation details; for others, the simple check mark symbol in itself created a positive association with trust and security.

Participants who clicked on the Trust Mark were directed to the ACCC one-pager. A common comment from these participants was that they would have wanted more information on the data recipient in addition to the information given about the Consumer Data Right.



Accredited Consumer Data Right Recipient

CDR Recipient ID: 031415

Find out more

“The tick brings my attention to what is written on the side, which is Accredited Consumer Data Right Recipient, which makes me feel more secure with sharing these details with this application.” - KB

“I saw the little green tick box and went, ‘Oh yes, they're reliable, authentic, real, honest, trustworthy people.’ I did glance at it, saw it and went, ‘Oh, that's good," and kept going.’” - EB

Trust and safety

Building trust

2. Repetition and emphasis on ability to revoke consent

Most participants felt reassured by the knowledge that they could easily revoke their consent whenever they wanted. Knowing that there were multiple options to revoke consent, including a way to revoke consent through the data recipient's app, was important to users.

The participants who found this information helpful also noted that they appreciated that this information was repeated throughout the consent flow. They noted that the repetition made them feel that the option was always available, and that they always had a choice when it came to revoking consent and ceasing to share data.

"It did tell you where to go for checking your privacy settings, it did tell you how much information was supposedly being shared, it did tell me if I wasn't happy with the Life thingy, I could go to my bank and my energy people to tell them, 'Look, tell this lot to bugger off,' and they would. So that's nice. Knowing there's a second spot where I can say, 'Go away, do not share the energy,' is useful. Like being able to turn off the gas tank at both ends." - EB

Trust and safety

Building trust

Consent receipts and the Trust Centre

The participants who finished the consent flow and ended the test at the consent receipt screen responded positively to the consent receipts. They found it helpful to have a record of the consent process they had just completed and several participants noted that the confirmation email sent to them reinforced the trustworthiness of the overall process.

However, several Round 1 participants reacted negatively to the term “Trust Centre”. While they did not object to the function of the Trust Centre, they did not like the name. When the name was changed to a more neutral term in Round 2 such as Data Sharing or Data Sharing Settings, no participants complained about the new name.

“Cool, there's another consent receipt. I think these are really great, I love these.” - SK

“That’s good to know because I'm guessing… If I had a problem I could ring them and quote that number and then yeah. Okay. So that's reassuring.” - MH

“Calling it the Trust Centre. Really? This is like when you're going into a cult and everyone's telling you to go with the flow, and the names start to get a little bit more and more corny and it's sending alarm bells.” - IK

“How it says at the top here ‘Trust Centre’… That kind of just makes me not trust them.” - BA

Trust and safety

Building trust

Detailed information, including data cluster details and effects of not giving consent

Most participants commented that the detailed information throughout the consent flow was helpful. In particular, the details of how their data was going to be used, and why this was needed in the data cluster components.

Some participants also noted that they appreciated knowing what would happen if they did not give their consent, without having to actually take that action. These people also commented that they appreciated knowing they would not be excluded from the app’s features if they did not consent to the data sharing, since they could still input data manually and try out the app.

“Oh that's good, gives me information of what I have to do if I don't consent. That makes a lot of sense.” - GB

“I like the fact that they give that prompt on what you get in return. Cause I like to know if I'm divulging everything what am I actually getting in return. That you're not just using all my information for your benefit.” - CH

“Oh, if I wanted to know more, that feels trustworthy that there is another place to go to double check.” - MS

Trust and safety

Gaps in trust

Data safety and security concerns

Many participants expressed concerns about security of their data, both in terms of risk of the data being hacked and stolen by third parties, and concerns about not knowing who would have access to their data once it was shared with the data recipient.

Some participants mentioned My Health Record as something they were concerned about due to misperceptions or misinformation about the issues, and fears of data being shared with third parties without their consent. Lack of information about any third parties the data would be shared with, how it was stored and how it was secured were cited as common concerns.

“I need a lot of information to know how the data is secured. Otherwise I would never give, if it is a random app I would never give that.” - SV

“It's always one of those things that I really get worried about. I even opted out of that Healthshare thing because I was like… I don't want that vulnerability of somebody hacking it and finding out all of our health details.” - DP

“As in, you know, who owns it? Where the data is stored? Potential breaches of security of any nature, not just hacking, but obviously internal employees, that stuff can happen. It needs secondary verification or made a stronger point, that data that's being sent between your app and what stored it's highly secure.” - KB

“I mean, this app is perfect for identity fraud. It's better than a dating app. I mean, holy shit. You could turn peoples' electricity on and off with this app.” - AW

Trust and safety

Gaps in trust

Concerns about misuse of data

A significant number of participants expressed worry about their data being stolen (identity theft), their data being used against them (eg to profile them, or analyse their situations for unfavourable outcomes such as decreasing their credit score) or for uses that they hadn’t consented to such as marketing and targeted ads.

“The masquerading online is very, very detailed these days and almost imperceptible and seems very real. There's also, it could be money laundering and I'm always aware it could be for identity theft.” - EB

“[Misuse that concerns me would be] focusing marketing campaigns and things like that. Blanket emails would annoy me more.” - SB

“It should never be that there can be an abuse of identity from the service provider. So, one of the reasons that people worry so much about MyHealthRecord, and will worry about this project, is because in MyHealthRecord, something somebody writes in your account or identifies within your account can be used against you.” - AW

“What does it do for anybody else who accesses it, because I would imagine that would be very nice for say someone who wanted to steal your identity or someone who wants to target ads at me, which I don't like.” - DC

Trust and safety

Gaps in trust

One-pager helpful, but needs more information and clearer language

The majority of participants found the page of additional information regarding the restrictions on their data use and penalties for misuse to be reassuring. In many cases, this increased the likelihood of a participant being willing to share their data, and therefore completing the consent flow.

The main concerns expressed by participants regarding this information was in its lack of clarity in some areas, as well as its lack of citation and verification. Participants expressed that they would want to verify how valid the terms in the one-pager were by doing additional research into the appropriate government and legal parameters around data sharing.

"'ACCC privacy. Must be accredited by the Australian Government to ask for your Consumer Data Right data. They must ensure no one can access your data without your consent." That's so difficult, which institution they collected it from with the sale of data. 'Only be used for its intended purpose,' that's fine, but define intended purpose." - EB

"I like it sitting under the ACCC, rather than a new internet department…. I think it makes sense that it's a consumer, that it fits within the consumer rights framework rather than anywhere else, and there's legal stuff there too… From my perspective I trust the ACCC a lot, and I know that they protect the rights of the consumer. I would rather that this is developed from a consumer point of view, than the purchaser point of view." - MS

"Civil penalties, compensation orders, enforceable undertakings. That's a very ... enforceable undertakings, what the? That's a very funny word." - LL

Trust and safety

Gaps in trust

Additional layers of distrust around data analysis

Many participants were uncomfortable with the idea of data analysis and recommendations for changes to their behaviour, and found these aspects of the app to be invasive.

Many participants noted that they've felt uncomfortable in the past when realising how much other apps know about them, for example social media apps with targeted advertising, or solar energy companies with realising that anyone can get satellite photos of their house online.

One possible reason for this level of analysis being perceived as invasive is that this analysis goes beyond what participants were expecting from the app. Participants expected the app to show them patterns of spending and help with budget, but once the app started making recommendations for changes to specific brands, this was unexpected and perceived as invasive. Clearer communication of how data will be used by the app on signup and an ability to opt out of particular data analysis may reduce perceptions of invasiveness.

"If you analyse data in a way that penalises people, they'll learn how to game the system to get benefits. Or just to stop the negative impacts." - AW

"The casual one line of fine print that tells you that it's going to compare products on the market, without saying that therefore it will be you giving information about products… Third party information, specific brands, specific companies. It doesn't tell you how far it goes with that and that's absolutely terrifying." - IK

"I expected it but shove off… It's an abuse of data." - AW

Trust and safety

Trust and institutions

Importance of data recipient reputation

For many participants, their willingness to complete the consent flow was conditional on the understanding that they would have thoroughly researched the entity they were sharing their data with to ensure they were a respectable and trusted institution. Examples of intended research methods included: app reviews, brand recognition through advertising, searching online for a company webpage and information, and endorsement by other well-known brands. In particular, participants claimed they would want to see the holder of their data (eg. their bank or financial institution) verify and endorse the app before they would feel comfortable sharing with it.

For some participants, Government certification alone was not enough to encourage trust. Many felt that it would be easy to fake certification by falsifying the trust mark and mimicking the protocols used by properly certified entities.

“I'm not comfortable with this application because it's not reputable enough for me to actually use it.” - KB

“Before I commit to anything I’d always look at reviews. Reviews would be something that would convince me to do it or otherwise.” - PS

Trust and safety

Trust and institutions

Trust in banks higher than trust in government

Trust for financial institutions was significantly greater than trust in government for the majority of participants. Many participants felt that the regulations and protections offered to consumers were more effective and easier to challenge than those offered in government (eg. Centrelink, NDIS). Many participants felt empowered knowing that if their bank betrayed their trust, they could always take their business elsewhere.

Perception of the effectiveness of government institutions was less confident. Participants frequently cited previous experience with frustrating, confusing and even dehumanising treatment when trying to seek government services. They also felt there was a lack of ownership and responsibility by government employees when it came to the individual safety of the participant.

“For example I feel the banks are safer.“ - SV

“It's weird. I just feel like the corporations have more regulations on them, more punishments, more overwatch. And obviously if something happens and a lot of people complain, it gets looked at pretty quickly. Where the government, you can complain until your voice is gone. As in for example the NDIS stuff, we've been complaining and complaining and complaining, nobody's listening. But if NDIS was a more private corporation, I'm guessing something would have been done by now, or people would have moved on and gone, ‘No. This is how they've burned us.’” - DP

Transparency and accountability

Transparency and access to information

Data recipient information

Information about who the data recipient was and how the data would be managed was a key concern of most users. Uncertainty about the identity of the data recipient was a key cause of concern about security of their data, misuse of data and data being shared with third parties.

Many participants expressed concerns that apps like LifeManager (the prototype data recipient app) could be used for identity theft or other criminal activity, or for collecting data to be sold to advertisers. Claims about valuing security, the app being accredited and data not being shared outside the company were often considered untrustworthy in the absence of information about the data recipient’s identity, data management practices and business model. Detailed information about the data recipient’s identity and their data management practices is likely to be needed for users to feel comfortable sharing their data.

“Who that stuff is underwritten by, it comes down to that. If it's a company which is outside of Australia or is it fully Australian? Because anyone can create an app and say, "We value your security, blah, blah, blah, blah," and all that. Is the security going to be there? No.” - KB

“How does Life Manager get its money? Because they get their money from something…. I'd want to know where this lot was getting their money because they don't get it from nothing you know.” - GB

“I don't know who these people are, really and what it's all about, even though it says it's private, but who really knows. They can just start sending me vendor stuff and advertisements.” - SB

Transparency and accountability

Transparency and access to information

Transparency about data use

Most participants expressed appreciation for the clear language that outlined how their data was going to be used, particularly the reinforcement of boundaries on the limitations and storage of that data (eg. would not be sold to third parties, consent would be re-affirmed periodically).

Where concerns were expressed about the usage of their data, participants cited distrust in the app (influenced by the app's lack of credibility and endorsement in the community) and in some cases felt that the scope of data being requested for sharing was too great and unnecessary for the purpose of the app, or not sufficiently explained by the app's text.

"I understand they need that money in and out, but why do they need to know who it's from and who I've sent it to? … So, are they judging what you're spending on charities or your own personal thing or whether you're a gambler?" - LL

"The difference here is that you've got that transparency and you've got that information that tells you who you're sharing it with and who you're not sharing it with. I don't have a problem with sharing my information with people I choose to share information with." - PS

Transparency and accountability

Accountability and consequences for breaches

Very high value placed on accountability of all entities involved - government (as accrediting body), data holder, data recipient

Ability to hold institutions accountable for how they manage and use the data was mentioned as very important by many participants. Concerns about a lack of accountability were one of the underlying causes of many participants' concerns about security of their data and misuse of data.

At the same time, while accountability was considered extremely important, many users expressed skepticism about accountability of institutions responsible for managing their data. A perceived lack of accountability in data sharing situations they'd previously encountered (eg. My Health Record, social media advertising) was sometimes brought up as a reason for their skepticism about accountability in this situation.

"Well I probably would share my data now knowing that, obviously they can't on-sell it, they do destroy it if you ask for it to be gone and I guess is sort of holds them more accountable. So if I did think that anyone had shared the data and stuff, they would be reprimanded for it basically. Like you could hold them accountable for what they've done, if they did do it. So you would get your money back or anything like that." - CS

"'After withdrawing your data, the accredited data recipient will destroy it or de-identify it.' I'm skeptical about that too. I understand that they'll probably have to, because of the, if they sign up to it, then they have to get rid of it, but how do we know that actually happens." - DC

Transparency and accountability

Accountability and consequences for breaches

Data recipient accreditation and penalties for violating CDR rules

Participants' strong desire for accountability and past experiences with a perceived lack of accountability meant that they were unlikely to trust data recipients to comply with the described limitations on data usage. Several participants expressed that they would need tangible evidence that organisations would be held to account and penalised for breaching the rules before they could trust that the rules would be complied with.

Consequences for breaches by the data recipient needed to be made clear to participants, and penalties needed to actually be seen to be enforced in order for participants to trust that organisations would be held accountable for how they managed their data.

"We want tangible, practical fines and ramifications for breaching the safeguards in the system…. because the practical ramifications on people's lives are huge. People kill themselves because they can't get a loan, or people choose never to have children because they know that related costs are a fortune. People disengage with systems… These are huge ramifications that need to be with tangible accountability measures. We need more than lip service because if they're just lip service, then people, us, tune it out." - AW

Agency and self-directed choice

Choice vs too much automation

Initiating data sharing process with additional providers

An important perception of trust for participants was feeling that they had control of their data and that they had the agency to decide with whom to share. Many participants responded negatively when the prototype encouraged them to share data with other entities, feeling this was a breach of trust even if they had initially consented to this process.

Even though the process of connecting to another provider was less efficient without automation, the majority of participants preferred this method as it felt more empowering and meaningful when it was a choice rather than a path they felt pressured to undertake.

“I haven't connected an energy provider, that's very slack of me. That was because when I connected my bank it went straight on, it didn't loop back and say, "Okay now, did you want to connect your energy provider," which is probably something it should have done.” - EB

“I like that I'm involved in connecting it, it gives me a bit more sense of control, I guess, and that I'm choosing which things I want to be looked at. Like if I'm concerned about my energy, then that's why I'm doing it. If you just pop up and say, oh, energy, I hadn't really thought about energy, I'm worried about this.” - MS

Agency and self-directed choice

Choice vs too much automation

Self-directed choice

Many participants wanted to be given the choice of how much automation of the process they wanted, and how much they wanted the app to give recommendations vs just present information to allow them to make their own decisions.

Some participants found recommendations and automation useful, whereas others found them invasive and unpleasant, and likened them to an attempt by someone else to control them. Some participants liked the convenience of being able to grant direct access to their data, whereas others preferred to maintain greater control over their data and so preferred a slower process, but one that gave them more control, such as manually uploading bank statements.

In general, users need the ability to make self-directed choices about how much they value automation and convenience vs control over their data.

"That was probably one of the reasons why I wouldn't choose this LifeManager as a real app for myself. I want some autonomy from the best intentions…. It's simply the feeling that somebody tries to manage your life completely, that I find revolting, I guess." - GR

"There is nowhere in this process where I had the option of just manually putting things in or submitting six months worth of bank statements or whatever. The only option has been narrowly terrifying and that is probably where I would set my phone on fire and throw it across the room." - IK

"If it were this easy to connect my accounts to LifeManager I'd totally be in." - PS

Accessibility and clarity

Making information understandable

Multiple screens vs accordion layout

The vast majority of participants preferred the accordion layout (Round 2 prototype) to the multi-screen layout (Round 1 prototype). Having all information available on one page but segmented for readability made participants feel the process of data sharing was more transparent and easier to understand.

The multi-screen model made many participants feel as though they were not being given enough information to consent properly, as the escalating requests for further data sharing made them feel as though what they consented to at the start of the process was very different from what they consented to at the end. Many participants chose to opt out of this consent flow rather than complete the data sharing process as their trust diminished with every additional screen through which they had to progress.

“Yeah, it kind of does [feel like a lot of information to take in]… I'm kind of starting to think oh, I don't want to do this. So I'm feeling apprehensive.” - BA, Round 1 prototype

“Oh, my gosh, I feel like that a lot of people aren't going to like this amount of starting things. I think that the information it's giving is really helpful, but I think that most people, or, some people, at least, aren't going to be patient enough to go through all of it, especially because every window has a lot of information, a whole lot of words, and most people are probably going to do what I just did and just read through all of it, but the difference is, it's going to be their real information, so.” - TH, Round 1 prototype

Accessibility and clarity

Making information understandable

Presentation of information and reading

In Round 1, several participants flagged that the language used in prototypes was unclear or that information was hard to find or comprehend. Building on this feedback, the Round 2 prototypes highlighted key pieces of information and changed text for greater clarity. The majority of Round 2 participants reported that they found the wording used in the prototypes to be clear, easy to understand, and useful in helping them make the decision to share their data. When questioned, participants preferred to be presented with thorough information even if this meant a lot of text to read, asserting that this made the process feel more transparent and trustworthy.

Concise summaries and itemised lists were specifically praised for helping them absorb information. Iconography also helped draw the eye and denote the purpose of features and functions without increasing the amount of text on the screen.

"There was a lot of reading to do. Which I think might put some people off, like if reading is not a thing that you do easily, there is perhaps... And maybe because even that because it was lot of, I think I mentioned there's a lot of reading in one screen. It's a bit like when you're doing PowerPoint presentations and put one sentence on a slide. 50,000 words, sentences on the slide. Nobody reads it. " - HW

"Well, I can see the sign and read there, but I'm not going to read it, because I'm sure it's long and boring, and all I'll be saying is, "Yeah, okay," and I always yeah, okay, so my data is out there. I've got nothing to hide. I'm not reading all the small print." - MS

Accessibility and clarity

Accessibility in visual design

Visual accessibility - typography and layout

Accessibility was an important consideration brought up by many users, both to ensure that they would be able to read and understand the text, and to avoid accidentally performing unintended actions due to misclicks. This was particularly pertinent to users in the older age ranges. Several users commented that having to scroll through the lengthy data cluster screens was cumbersome; these users included participants throughout all age ranges.

At the very minimum, data recipients should use WCAG 2.0 guidelines to build their apps and websites. We recommend mandatory compliance with the WCAG 2.1 guidelines that are specifically pertinent to typography and layout, particularly guidelines 1.4, 2.1, 2.5, 3.1, and 3.3. The feasibility of requiring data recipients to have a font-magnification or zoom function in their apps should also be investigated.

"That is so small, it would maybe not be seen. I can read it, but I know some people wouldn't." - LL

"The physical length of the screen was a bit frustrating, I had to do a lot of scrolling. … One of the things I worry about sometimes, and this is ... This may sound trivial ... But when you're scrolling through every now and then when you touch to scroll it sometimes actually touches to activate or ... So yeah. You'd have to go back and make sure you didn't tick anything you didn't want to tick." - GB

Vulnerability and disadvantage

Greater concern about possible harm

Participants from vulnerable backgrounds tend to be less likely to trust, more likely to anticipate harm

Participants who had experienced vulnerability or disadvantage were more inclined to be concerned about harm arising from data sharing, both from government and institutions, and from malicious individuals such as an abusive partner. In many cases they had already experienced or were experiencing harm or struggling with systems that penalised them for their vulnerable situation, so they were more inclined to anticipate harm from greater data sharing, rather than to trust institutions to protect their data and prevent misuse.

Further consultation with people from vulnerable backgrounds is needed to identify specific cases of misuse that are of particular concern and to design the system to prevent these.

“Every Wednesday, I trundle off next door to a food bank. These people say- How is this system used to remind me of payments or how this system is used to forever lock me out of this service. How will the safeguards be overridden? How will my data be shared in a way that's not ethical, but will lead to serious consequences in my life? How will these frameworks be rigid in ways that will bear extra bullshit?” - AW

“If you think a scenario where you're experiencing family violence and somebody seems to know what you're doing and where you are and things are happening that seem... a little like, oh, Big Brother's watching. There is a sort of a... People become... And I'm not being paranoid, but it comes across as a bit of paranoia.” - HW

Vulnerability and disadvantage

Greater concern about possible harm

Concern about using people's data against them and profiling vulnerable people

Though participants from all backgrounds expressed concerns about the safety of their data, those from disadvantaged groups or marginalised identities had more explicit concerns about how their data might be used to classify or exploit them. Their concerns specifically revolved around how institutions of authority (government, banks, health services) might discriminate against them or deny them opportunities or services relevant to their needs.

Vulnerable and disadvantaged participants expressed a certain resignation to the idea that their data would be used for surveillance and exploitation, already anticipating that data sharing systems would be used to classify and exclude them. The involvement of government or authoritative institutions only exacerbated these fears.

"If the government checks how much power we used, could that be taken into account to whether you got that transitional house.... There are scenarios where you go, maybe this could be used even by government bodies against people." - HW

"I think far as LGBTQI that can sometimes use against you so I have concerns. Even though theoretically it's legal but there's those weird things that you still can't get jobs in church institutions, areas of discrimination and marginalisation. And you can't get health insurance if you've ever had a major health condition because they will use that against you to deny a claim even though it's not connected to that.... So I have concerns about information can be used against people." - HW

"This program, this analysis, will catch people, will identify people who are outside the norm." - AW

Vulnerability and disadvantage

Greater concern about possible harm

Concern about reducing people to their socioeconomic data and ignoring vulnerability and disadvantage

During the testing of data sharing and automation, participants felt more reassured knowing that their data was only going to be analysed by algorithms instead of viewed by real people, but disadvantaged and marginalised participants voiced concerns that this method might not be sensitive to individual needs. This concern was strongly voiced by participants with disability, for whom there is often no ‘choice’ in the way they use their money or energy resources.

Participants expressed a need for greater understanding and empathy in the use and analysis of their data, uncomfortable with being measured against a societal standard (of weekly budget, of energy usage) that they simply are unable to conform to.

“If it sees my life only financially, it's only gonna look at me from a financial standpoint. So they reduce me from a human being to being a consumer and to my bank account, spending account. Which then loses sight of all the things that bring quality of life.” - AW

“A person with chronic disability, who needs to turn the electricity on more, because they need extra heating, isn't worth less than a person who can stand the cold.… Half of Australians have chronic health issues. And it progresses with their age, and if we're gonna look at analysing people’s purchases, spending power, then we have to realise that they're hinging on a range of factors that are not always within their control.” - AW

Vulnerability and disadvantage

Recommendations

Further consultation with specific groups focused on issues vulnerable users face

Further consultation with people from vulnerable backgrounds is needed to identify specific cases of misuse that are of particular concern and to design the system to prevent these.

Prioritise transparency of information - including what data is viewed (what do the authorities see, what does the data recipient see)

Vulnerable participants were apprehensive about sharing their data without knowing the exact details of what the data recipient would receive or what information the data holder stored. The data holder and data recipient's views of the user's data, including the specific personal data held (for data holder) and accessed (for data recipient) for each data cluster, needs to be accessible by users upon their request.

Strong opt-out

Vulnerable participants were especially concerned that data recipients would still keep their data even if they opted out (revoked consent). The information disclosed by data recipients and the information on the CDR websites and educational materials should clearly state:

- That consumers can opt out (revoke their consent) at any time
- That opting out means consumers' data will be de-identified and/or deleted

Options for manual entry

Participants from vulnerable backgrounds especially wanted greater control over their data, even at the expense of convenience and efficiency. Providing options for manual entry, such as manually uploading bank statements, is critical for participants from vulnerable backgrounds and should be a requirement for the data recipient to implement.

Joint accounts

Participant comments

Multi-party authorisation vs optional notification

Almost all participants preferred joint accounts to require multi-party authorisation. Many participants expressed concerns about ability for one party to share access to a joint account without the other party's approval. In particular, some participants had concerns that this could be used for surveillance, or that malicious joint account holders could deliberately grant access to untrustworthy third parties.

Requiring multi-party authorisation was seen as the preferred method of accessing joint accounts by most participants, since this prevented abuse by malicious third parties by preventing access without all parties' approval.

"I would do it just to spite my ex-partner. I would drain my accounts of my money and then link it to like every single dodgy-looking app there is on the market, and completely eff up my ex. That would be awesome. …. I don't think there's any situation in there where I wouldn't find a way to liberate myself." - IK

"I think since it's a joint account, one person shouldn't do whatever they want without the other person. In my opinion. The bank acting as go-between, that's the easiest solution." - GR

"I don't like the idea of somebody's joint account being shared without their approval, without their consent." - HW

Joint accounts

Key considerations

Common patterns in situations facing vulnerable users

Vulnerable users were more likely to be concerned about situations such as domestic violence, controlling relationships, financial or emotional abuse. In particular, they had concerns about an abusive partner using apps that access data from a joint account as a method of surveillance and control. Given that smart home devices, remote monitoring equipment and family tracking apps have already been misused in such situations, these concerns are justified and requiring approval from both account holders is necessary to prevent misuse.

“I just feel like I'm being a bit silly because it's a joint account so it should be getting consent from both account holders and I'm not with him anymore, so I really should change that account situation into just my name, or split whatever's in there between my ex and I, and just alarm bells, yep. … Yeah, incredibly uncomfortable because I'm thinking of like, domestic violence situations where you could have a partner in the relationship who's taking advantage of the other partners finances and controlling them through this information.” - SK [on optional notification prototype]

“Nobody in a vulnerable situation wants to sign up to this! The only reason that somebody would do this is so that they can track their card after. Okay? It will always, always always always, come from this position of somebody who will abuse somebody else. Vulnerable isn't going to get up and get attention for using this app. All the vulnerable, what will happen to the vulnerable, is extra surveillance. How can you share somebody else's data without their permission? It's not ethically permissible.” - AW [on optional notification prototype]

Joint accounts

Key considerations

Access to authorisation

The process for authorising access to share data from a joint account will require further review, as a participant identified that the current process (an email request sent from the bank using the joint account contact information) is easy to circumvent. For example, if the joint account is also linked to a shared email address that both parties can access, it's easy for one person to complete dual authorisation without the other party being aware or consenting.

The participant also explained that the kind of credentials used to identify someone either online or via phone is information that an ex partner would often know (birthdate, passwords, security question answers) and that it would not be difficult to change a partner's email and contact details on a joint account in order to gain full control of data sharing authorisation.

"There's a certain human element that can be sucked in. So if you want a different account, I know that I could walk into my local bank account and tell them that I wanted to change the emails they were sending. It shouldn't probably do it with contacting my partner... So I could take my partners email account and a lot of this is because I'm in a small country town, bank tellers know me. We chit chat. I don't think they would be particularly suspicious of me." - HW

"I still think even if you are sending an authorization email. It can still be bypassed pretty easily. So it's not ideal and it probably works really well if everybody is in a relationship where it's all upfront and lovely. And what about people- half of the time [my partner] actually gives my email address. Or you have a joint email address." - HW

Joint accounts

Recommendations

Option 1: Multi-party approval required (strongly preferred)

Joint account data sharing will require the approval of all joint account holders. If this cannot be done in time for the v1 release, joint account functionality should be delayed until multi-party approval can be implemented.

Implications of requiring multi-party approval: Data sharing will not occur unless all parties consent, which prevents joint account data sharing that can potentially increase financial abuse of vulnerable users. It is possible that some people will opt out of data sharing due to not wanting or not being able to obtain other parties' permission.

Implications of delaying joint account functionality until multi-party approval implementation: Joint accounts will not be available to data recipients, which will impair app feature sets.

In addition, **appropriate security controls**, eg biometrics, should be implemented to ensure that the communications of vulnerable consumers (eg email, contact details) are protected.

A system of **flagging accounts belonging to vulnerable consumers** should be made highly visible and available to vulnerable consumers.

Bank staff should be trained in appropriate protocols to ensure that they do not allow changes to be made to accounts involving vulnerable consumers without the vulnerable consumers' explicit (and if possible, in-person) consent.

Option 2: Account-level consent (if multi-party approval is not feasible)

If authorisation at account level will be required for v1, we do not recommend that data sharing authorisation should 'piggy back' off existing account authorisations like making transactions from joint bank accounts. Data sharing should be introduced as a new feature of joint account management and explicit acknowledgement of both parties should be established.

Implications: This option opens up more risk for vulnerable users,

Make data sharing terms and conditions explicit: data holders should make the terms of data sharing clear to all joint account holders, and require them to re-consent to this feature being activated on their account.

Communicate all data sharing activity: Data sharing should always notify other account holders of the activity, and always allow account holders to immediately revoke consent if desired.

Review individual circumstances to protect vulnerable consumers: Where vulnerable account holders may have concerns that their data may be shared or accessed by a partner without consent, restrictions should be in place to prevent any data sharing without authorisation, such as a system of flagging accounts belonging to vulnerable consumers.

Implement appropriate security controls: Consider measures such as biometric security where possible to avoid scenarios where the partners of vulnerable consumers have access identifying information and to their accounts (email addresses, phones, passwords).

Energy-specific findings

Automation vs control

Cross-sector flow

In Round 1, we tested a flow that had a popup notification screen alerting participants that the data recipient had analysed their data and found that they were with a specific energy provider, and asked if they wanted to connect their energy account with said energy provider. For the most part, participants reacted negatively to this. They either did not realise that they had consented to this use of their data, or if they did know, they were unhappy about it, commenting that they would have preferred to set up the link with their energy provider both 1) on their own initiative, and 2) manually by choosing their energy provider from a list.

We incorporated this feedback into the Round 2 prototype, testing a flow that alerted participants that they had not yet connected an energy provider and asking them if they wanted to connect their account. This resulted in a much more positive response. Some participants noted they would also appreciate an alert email to remind them to do this setup.

“I didn't know it was going to be a thing. I didn't know it was a feature and it maybe just got stronger in the fine print, in that one little tiny line. Not comfortable at all with it.” - IK [on round 1 cross-sector energy prototype]

Energy-specific findings

Trust and safety: energy vs financial data

Preference for sharing energy data over financial data

Most participants were less concerned about sharing energy data compared to financial data. Financial data was considered more risky due to perceptions that it was at higher risk of being used for identity theft or fraud, and due to banks educating consumers about the sensitivity of their financial data.

Some participants conflated access to financial transaction data with access to withdraw money from the account, and thus were very worried about granting access to their bank account, which was not the case for energy data. Participants were also more willing to have energy data analysed in order to save on energy bills, whereas analysis of financial data was more likely to be seen as invasive or judgemental.

“That one is okay [compared to banking] because I like to save more energy.” - SV

“That's what this app is doing. Looking at my utilities. I would give it my utilities password before I give it my bank password.” - IK

Energy-specific findings

Trust and safety: energy vs financial data

Government agency as data storage

Participants were generally more comfortable with their energy data being stored by a government agency rather than by energy providers, since energy providers were perceived as having more incentive to misuse the data.

This is in contrast to the result for banks, where participants were more inclined to trust banks over government agencies with financial data. This may be because banks already clearly have access to this data, or because banks are considered to have higher security standards than government, which in turn are considered to have higher security standards than energy companies. Another possible reason for this difference may be that energy companies were perceived as having a greater incentive to misuse energy data for marketing purposes, whereas government agencies were considered to have higher likelihood to misuse financial data via policies that discriminate against people in financial distress.

“On the one hand I prefer [energy data to be stored] by government than an energy provider because I think they're less likely to sell it. They're likely, less likely to ... well it's on my back because I have already have all my other data so they could merge it. But my bigger concern is that the government is probably a bigger target for hacking and it's actually, it's probably easier to target to hack them, than a big commercial organization.” - DC

“Doesn't worry me, as long as they're getting results. No, I mean, as long as they're accountable for what they do. As long as they're, like I said, not sucking information that's irrelevant to what they need.“ - LL

“A government organization seems more ... seems like there's more accountability or there's more ... Yeah. I feel as though they'd be more responsible with my data.” - MH

Energy-specific findings

Understanding reasons for sharing

Importance of value proposition

Participants needed clarity around the value proposition of sharing their data for them as consumers, as well as a clear understanding of the motivations of the data recipient for wanting access to that data. Participants were suspicious of data recipient motives, and wanted assurance that their purpose for gaining access to that data was not just to advertise their services or sell their data to advertisers. The value proposition of being able to save money and get a better deal was viewed with suspicion due to that often being used as a marketing tactic to sell services.

One value proposition that had a greater appeal to consumers was improving consumer access to industry data in order to increase consumer negotiating power against large corporations. Greater transparency on typical energy bills giving everyone more information to enable others to get a better deal was considered a stronger value proposition than simply getting a better deal themselves, which was often viewed as just a marketing tactic.

“I'm afraid I am incredibly skeptical of things like energy companies and things like that contacting me to say, "Hey we've got this great new deal and it might treat you better." I have to be really persuaded with those. So yeah, having an app that does it for you would not be a bad idea, especially if the app is run by a third party. But as I said, I'd want to know what they're getting out of it.” - GB

"Like, that shock thing of our poor neighbors that got this ridiculous bill. And that helps sharing within the community. If people ... I can't believe that people might actually go ahead and pay an exorbitant bill, not realizing there's an issue with their supplier or the reads." - LL

Energy-specific findings

Understanding reasons for sharing

Preference for data sharing periods that sync with billing cycles

Participants preferred to share enough data to enable them to find useful insights, but not their full transaction history. This generally aligned with the duration of billing cycles, or duration of seasonal changes in behaviour.

For example, with electricity usage, participants preferred to share either 6 or 12 months since that allowed enough data to be shared to enable useful insights to be provided, and for changes to be genuine changes in behaviour rather than seasonal variations.

“Six months sounds pretty fair because you've got to give the budget some time to roll out. And when people budget then they go back to bad habits. They cut back, go back and forth a little bit. I think six months is a fair amount of time to build new habits and build new budgeting techniques. That being said, because obviously I've never used this app before. I wouldn't give it too long.” - IK

“It should be long enough to give you a gauge of energy usage. Six months probably not, but a year is about right.” - PS

Energy-specific findings

Understanding reasons for sharing

More information needed on energy data clusters

Many participants readily admitted a lack of understanding about energy data and the way it might be used to either benefit them or disadvantage them. Discussion regarding the energy sector as an industry revealed that most participants find information about energy usage and account plans to be complex and opaque.

This lack of comprehension often made participants more inclined to share their data, hoping that the interpretation of a third party could help them improve their energy consumption and costs since they didn't feel confident about reviewing and analysing this data themselves.

"This looks similar to the other one. It's a complete blast on talking about the account information. Name of the account. Supply billing address. I don't know what NMI means. Never heard of that." - CH

"It says it's sending my data but I don't actually know what data my energy provider actually collects. I don't actually know what they collect so I'm not totally sure what I'm agreeing so... Like do I want somebody knowing that I run my power 24 hours a day, seven days a week because maybe I'm growing marijuana actually?" - HW

Energy-specific findings

Mechanisms for sharing and giving consent

4. Multiple means of contact

Participants preferred to have a range of ways to contact data recipients and data holders, since different contact methods had different pros and cons which were prioritised differently in different situations. Sometimes participants preferred to use an app, email or website for speed and convenience; other times they preferred paper for record-keeping purposes or phone in order to be able to get errors or problems resolved more quickly by speaking to a customer service person in real time.

Specifically for Energy account holders, many participants still rely on paper billing instead of accessing their energy accounts online. Some users expressed uncertainty that they would even know how to access their online energy account, so any data sharing processes should also have a pathway that does not involve app or web-app consent.

"I don't usually log into my energy provider. I get paper bills and I chat with them on the phone. One of the reasons I like the paper bills it's because it's there and you can refer back to it, and I mean I know online stuff can do that as well, but I've also heard things where the sites have died and you can't get back to them. Or the company's folded and you can't get back so I do like having the paper in front of me…. I'll get the bill, open it up and realize the bastards haven't given us our rebate again so I can get straight on the phone and everything. If I had to do it online, I'd have to write all that down anyway and then call them." - GB

Common perceptions and questions

Themes commonly brought up by participants

The feeling of being watched

“I just don't want someone to see how much money I spend on Ebay.” - TH

Thinking that the data recipient also has access to their accounts and not just their data

“I really don't know that I understand enough about how detailed their access to my account is. … Okay, Life Manager will not see my details. Life Manager said they will not see it, but they're requesting access to my data. How do those two sentences work?” - LL

Equating data analysis with accessing more data

“I'm not entirely comfortable about it. I'm fairly savvy when it comes to budgeting and stuff like that. So being analysed for it is not going to help a great deal, unless it's like, "Oh there's this special deal you should go for." Yeah, it's a bit more than I'd be willing to share.” - GB

Assuming data recipient will break rules

“When you say, phone a company and they say, "This call will be recorded for quality assurance reasons." And you opt out, they're still going to record you. It's still there. They might not access it. They might deny having it. But they're still going to record you.” - IK

“‘After withdrawing your data, the accredited data recipient will destroy it or de-identify it.’ I'm skeptical about that too. I understand that they'll probably have to, because of the, if they sign up to it, then they have to get rid of it, but how do we know that actually happens.” - DC

Common perceptions and questions

Themes commonly brought up by participants

Can’t be bothered to read ‘fine print’ combined with nonchalance about data

"Well, I can see the sign and read there, but I'm not going to read it, because I'm sure it's long and boring, and all I'll be saying is, "Yeah, okay," and I always yeah, okay, so my data is out there." - MS

Usefulness of technology vs worries about financial data

“I mean, I want to trust it. Like, there's so much stuff about technology that's so useful. I love the immediacy and the handiness of it all. But yeah, financially wise. Yeah, I'm just a bit wary.” - LL

Lack of clarity about what happens to data when consent is removed

“But if it were to a previously connected organization who got it legitimately, that consent would not be removed. So again that remains out there. Does that party, company A, LifeManager is also partially owned by DeathManager, and they separate as life and death will do. After LifeManager has shared my data with DeathManager, I remove consent from LifeManager, but DeathManager still has that and they can still market, etc. to it because they got it legitimately at the time.” - EB

Recommendations

Recommendations

Information

Critical information should be up-front and on-screen

Consumers should be given all relevant information, summarised and itemised for readability, before affirming any form of ‘Consent’ action. Critical information such as consequences of not consenting and ability to revoke consent should be highlighted on-screen and should not require additional clicks to access. Where including additional information is not feasible, it should be clearly hyperlinked and easy to find.

Additional one-pager information, including more information on penalties faced by data recipient if they break rules

The accreditation process should be explained in the one-pager. Consumers want to be informed of all restrictions and consequences for data recipients who do not protect their data or who misuse it for a purpose other than to what was explicitly consented. In addition, the one-pager should explicitly state what uses of data are not allowed under the CDR rules.

Trust Mark should be strengthened by linking it to the data recipient’s specific accreditation data

Accreditation must be easily verified with a government source or site. The data recipient's accreditation information should be linked and easily accessible to consumers, and should be validated with matching data on the website of the accreditation body.

Require data recipients to provide info about measures taken in case of security breaches

Data recipients should clearly state, in an accessible and highly visible section of the app, the security measures they are taking in order to secure any data being shared with them. They should also outline what will occur in the event of a data breach, including any notification protocols for consumers and steps taken to re-secure their data. These consequences should take into account the sensitivity of the data being stored, and the scope and consequences of the breach.

Recommendations

Accessibility

Require compliance with strong accessibility standards

Consumers had concerns about difficulty reading the information due to inaccessible text, or accidentally agreeing to things they did not intend to do due to misclicking interactive elements. Some consumers also had difficulty with the vertical length of the screens and the amount of scrolling required. Data recipients should be required to comply with WCAG 2.0 standards for accessibility, particularly Guidelines 1.4, 2.1, 2.5, 3.1, and 3.3.

CDR helpline or contact information, in multiple languages

All relevant information regarding the CDR and its accreditation should be available in multiple languages common to the primary cultural demographics of Australia. This should be available as both written information, and a helpline with interpreter services for those with low literacy or a preference for receiving more personalised assistance.

CDR info site should have full translation functionality and be fully screen-reader accessible

All information for the CDR should be provided in the most accessible format possible. This should include the ability to translate the information into multiple languages on all areas of the CDR website(s) and optimisation for a wide range of devices using responsive design principles. In addition, the CDR website(s) should be fully keyboard navigable and should be tested for full compatibility with screen reader technology and other assistive devices.

Recommendations

Joint accounts and energy consent flow

Joint accounts: require multi-party approval

Multi-party approval for sharing of information from joint accounts should either be fully implemented in v1 or should be entirely deferred until a fully functioning, tested and secure system can be implemented that fully protects both parties, and particularly more vulnerable consumers in joint account situations. This is due to the high potential for abuse of this feature of the system.

The joint account consent flow should not allow exploitation or unwanted sharing of data for either participant regardless of the terms under which their joint account was formed. Due to the potential for misuse and the added risk for vulnerable users, joint account holders should not be asked to engage with a system where sharing of their data without their consent or knowledge is possible.

We strongly do not recommend any alternative to Options 1 and 2 presented in this report, though we have explored the possibility of such a system in the research sessions.

Energy consent flow: ask for user input and provide more information for energy data clusters

The original consent flow model used automatic suggestions by the data recipient app to initiate the cross-sector component of the energy consent flow. We recommend that the cross-sector component of the flow take the form of new account setup (“We notice you haven’t connected an energy provider yet”) instead of specifically using recommendations constructed via data analysis (“We notice you’re with ZZ Energy”) as participants overall strongly preferred the former option since they felt they had more control over their input and the overall data sharing process.

The majority of participants expressed confusion or lack of comprehension over the data in the energy data clusters and did not know what the NMI meant. We recommend providing more specific information on the meaning of terms for this sector as information modals. The Rules should have more stringent requirements on data recipients to explain what these data clusters are being used for in open clear language.

Recommendations

Designing for vulnerable users

Further consultation with specific groups focused on issues faced by vulnerable users

Further consultation with people from vulnerable backgrounds is needed to identify specific cases of misuse that are of particular concern, and to design the system to prevent these. In particular, it is important to seek feedback from community groups and institutions, as well as individuals who have lived experience with: domestic abuse situations, mental health issues, physical disability, mental disability, chronic illness, low English literacy, socioeconomic disadvantage and technological disadvantage.

Prioritise transparency of information: disclose data views

Vulnerable participants were apprehensive about sharing their data without knowing the exact details of what the data recipient would receive or what information the data holder stored. The data holder and data recipient's views of the user's data, including the specific personal data held (for data holder) and accessed (for data recipient) for each data cluster, should be made available to users upon their request. The Rules should mandate that this level of information be made available by data recipients.

Strong opt-out and manual data entry

This consent flow model should not make consumers feel that access to their data and the security risks therein is the 'cost' of receiving services or benefits. We strongly recommend that the Rules should mandate that the option to manually enter data be made available by data recipients through their apps.

The information disclosed by data recipients and the information on the CDR websites and educational materials should clearly state:

- That consumers can choose not to participate in the automated system instead manually inputting their information
- That consumers can opt out (revoke their consent) at any time
- That opting out means consumers' data will be de-identified and/or deleted (dependent on the parameters of the Rules)

Parameters for what happens to the data of users who opt out the system should be examined to see whether they can be strengthened, as some vulnerable users were particularly concerned that even after they revoked their consent for data sharing, their data would continue to exist in the system and it wouldn't be a "real opt-out".

CONSUMER
DATA
STANDARDS

THANK YOU

Consumer Data Standards | Consumer Experience Workstream

t +61 2 9490 5722
e cdr-data61@csiro.au
w consumerdatastandards.org.au