Department for
Business & Trade

Design Principles for Inclusive Smart Data Schemes

Research conducted by Savanta on behalf of the Department for Business and Trade

July 2023

Contents

Executive Summary **2**

Overview of consumer vulnerability and Smart Data schemes 4

Features of Smart Data schemes which could adversely impact vulnerable consumers .5

Summary of principles for designing inclusive Smart Data schemes 6

Conclusions 10

Introduction **11**

Background and policy context 11

Research objectives 12

Research methodology and definition of key concepts 12

Methodological limitations and areas for improvements 14

Consumer vulnerability and Smart Data schemes **16**

Overview 16

The impact of Smart Data schemes on different forms of consumer vulnerability 18

Potential barriers to Smart Data schemes being inclusive 21

Design principles for inclusive Smart Data schemes **27**

Overview 27

Creating trust in Smart Data schemes 28

Consent, consent management, and consent revocation 36

Choice architecture and consumer control 45

Support and redress 51

Conclusions and future considerations **54**

Appendices **56**

Appendix A – Literature review 56

Appendix B – Stakeholder workshop / interview discussion guide 57

Reference list 64

Savanta was commissioned by the Department for Business and Trade (DBT) to undertake research to inform how vulnerable consumers may interact with Smart Data schemes and identify inclusive Smart Data scheme design principles to mitigate risk of any potential harms. This report describes the research and design activities undertaken and summarises its conclusions. References to “we” in this report are to Savanta who produced this report.

Executive Summary

Smart Data is the secure sharing of customer data, upon the customer's request, with Authorised Third Parties (ATPs). ATPs then use the customer's data to provide innovative services, such as automatic switching or better account management. As the Department for Business and Trade looks to accelerate the growth of new Smart Data schemes, it is important to establish how core use cases and services can be designed in a way that ensures that they are accessible to everyone.

Accessible design means ensuring that vulnerable consumers are able to access the benefits of Smart Data schemes, as well as ensuring that they are protected from any harms which could arise as a result of their participation in the scheme. Using the Financial Conduct Authority's (FCA) definition, a vulnerable consumer is someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care.[1] The most recent FCA Financial Lives survey in May 2022 showed that 47% of UK adults showed one or more characteristics of vulnerability, namely: poor health such as cognitive impairment, life events such as new caring responsibilities, low resilience to cope with financial or emotional shocks, and low capability such as poor literacy or numeracy skills.[2]

In order to shape the design of future schemes, the Department for Business and Trade commissioned Savanta to conduct a two-stage research project to better understand the barriers to vulnerable consumers accessing scheme benefits, and how these can be mitigated. The research was guided by five main research questions:

1. What vulnerable characteristics are most likely to lead to consumers being excluded by Smart Data schemes?

2. What design features of Smart Data schemes lead to excluding vulnerable consumers?

3. What design features of Smart Data schemes promote inclusivity?

4. What do app providers and data holders believe are the barriers to Smart Data schemes being inclusive, and how can we combat these issues?

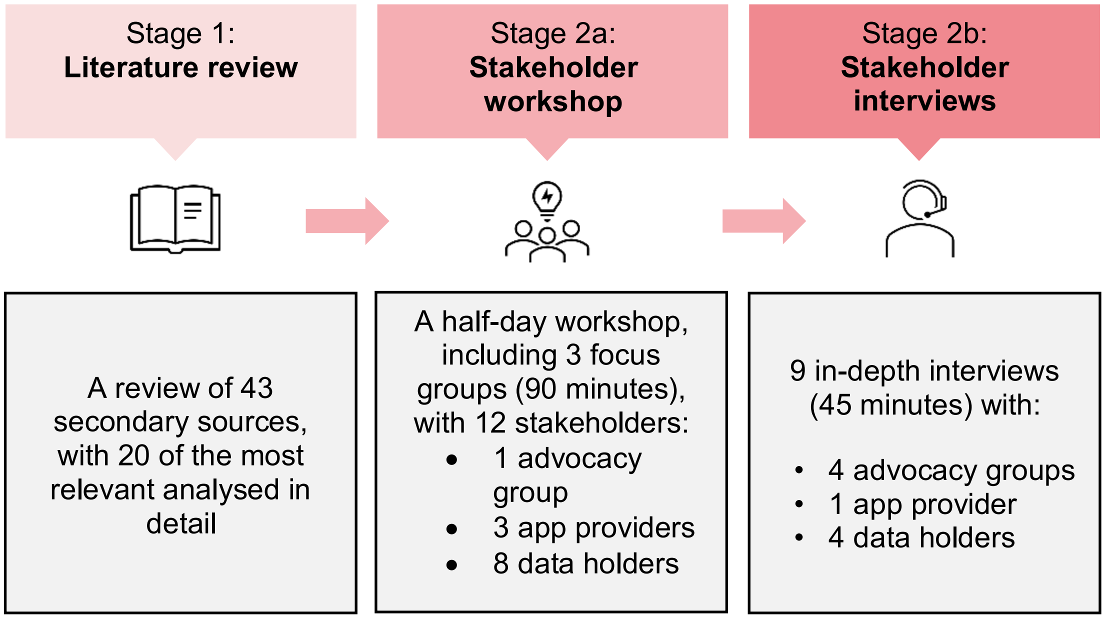
5. What practical design principles can be put in place to make Smart Data schemes more inclusive to all consumers?

This report presents the findings of a literature review, stakeholder workshop, and stakeholder interviews in line with these research questions. Figure 1 below shows the methodology in full:

[1] FCA, 2021. *Guidance for firms on the fair treatment of vulnerable customers.* Retrieved from https://www.fca.org.uk/publication/finalised-guidance/fg21-1.pdf.

[2] FCA, 2022. *Financial Lives 2022 survey: insights on vulnerability and financial resilience relevant to the rising cost of living.* Retrieved from https://www.fca.org.uk/data/financial-lives-2022-early-survey-insights-vulnerability-financial-resilience.

Figure 1 – research methodology



Stage 1:
Literature review

A review of 43 secondary sources, with 20 of the most relevant analysed in detail

Stage 2a:
Stakeholder workshop

A half-day workshop, including 3 focus groups (90 minutes), with 12 stakeholders:

- 1 advocacy group
- 3 app providers
- 8 data holders

Stage 2b:
Stakeholder interviews

9 in-depth interviews (45 minutes) with:

- 4 advocacy groups
- 1 app provider
- 4 data holders

Overall, this research aims to establish lessons and practical design principles that would need to be applied to create inclusive Smart Data schemes in key sectors.

The conclusions from this project provide an indication for government bodies and Smart Data scheme designers, to inform Smart Data policy and scheme development. This report represents research findings and does not necessarily represent government policy.

Overview of consumer vulnerability and Smart Data schemes

Smart Data schemes may be particularly beneficial for vulnerable consumers. For example, Smart Data could enable greater targeting of support in essential services (e.g., energy or telecoms) where consumers may be reluctant to proactively disclose that they identify as vulnerable, but are content with their vulnerability status being shared when prompted. More broadly, it also may make decision-making easier for some, saving time and money. However, the main challenge for future Smart Data schemes is designing core use cases and services so that they are accessible to everyone. The existing literature and stakeholder discussions found that Smart Data poses risks to each of the four forms of vulnerability, specifically:

- **Low capability:** Smart Data schemes are digital in nature and are likely to be accessed primarily via mobile and internet apps. Consumers without access to the internet will not be able to authorise data sharing and use applications developed for use cases within schemes, and therefore may be at risk of getting a worse deal than consumers who are able to engage online. As of 2020, 96% of UK households have internet access, but just 80% of households with one adult aged 65 or over living alone do.[3] Beyond digital exclusion, low numeracy, literacy, financial understanding,

[3] Office for National Statistics. (2020). *Internet access – households and individuals, Great Britain, 2020*. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2020.

or digital skills may lead a consumer to find it difficult to assess the legitimacy of use case, app or website, as well as use its interfaces. Having higher skills in these areas does not guarantee engagement but is an indicator of a person's ability to critically evaluate a platform or service[4].

- **Poor health:** Consumers with mental ill-health or addiction issues emerged as a particular concern in the context of Smart Data schemes both in existing evidence and in stakeholder discussions. These types of health conditions would make it more difficult to evaluate the risk of a particular transaction, especially if key decisions are made easier under a Smart Data scheme, in addition to there being many new entrants bringing innovations to the market. This could leave consumers at higher risk of making poor decisions about their finances, or of being a victim of a scam. Consumers with poor health may be more likely to also have low capability, and therefore may struggle to engage with the applications and use cases developed as a result of Smart Data sharing if they are not designed in an accessible way[5].

- **Low financial resilience:** those with low financial resilience may be negatively impacted by the increased access to customer data facilitated by a scheme. Low financial resilience refers to a situation where an individual or household has limited capacity to cope with financial shocks, unexpected expenses or a loss of income. Firstly, where consumer data is used to model consumer risk, Open Banking has been found to increase the likelihood that firms offer particular products, but at a cost to high-cost borrowers.[6] Secondly, under this scheme consumer data can also be used to assess consumers' willingness to pay, and therefore set different prices for different customers. Lenders charge more to the borrowers with a high willingness to pay; if especially-eager-to-borrow individuals are mainly from vulnerable sub-populations, this would worsen financial inclusion rather than improve it.

- **Negative life events:** experiencing events such as additional caring responsibilities or a relationship breakdown may lead to further vulnerability such as mental ill-health or low financial resilience. These events may lead consumers to become more time-poor, and therefore less likely to engage with and benefit from Smart Data enabled services.

Features of Smart Data schemes which could exclude vulnerable consumers

Vulnerability is extremely varied, and individuals may experience multiple vulnerabilities at the same time. Moreover, any consumer is at risk of becoming vulnerable at some point. Given this, it is important to take a needs-based approach to designing inclusive Smart Data schemes. Ultimately, four features of Smart Data schemes which could lead to vulnerable consumers being excluded, or result in harm being caused, were identified both through the literature review and stakeholder engagement (workshop and in-depth interviews):

[4] Chan, R., et al., 2022, *Towards an understanding of consumers' FinTech adoption: the case of Open Banking*. International Journal of Bank Marketing, 886-917, 40(4).

[5] Consumer Policy Research Centre, 2020. *Unfair trading practices in digital markets - evidence and regulatory gaps*. Retrieved from https://cprc.org.au/wp-content/uploads/2021/11/Unfair-Trading-Practices-in-Digital-Markets.pdf.

[6] Babina, T. et al., 2022. *Customer Data Access and Fintech Entry: Early Evidence from Open Banking,* [Stanford University Graduate School of Business Research Paper, No. 19-35]. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333269. This is a review of international Open Banking Schemes, including the UK.

1. **Low consumer trust and confidence in a scheme as a key barrier to adoption, both in terms of how data is collected, stored and used, and the benefits of the scheme.** Whilst it is important to build trust among all consumers as Smart Data schemes develop, vulnerable consumers tend to show higher levels of distrust and fear around new technologies, and the encouragement to share data between providers feels counterintuitive in the context of fraud and scam prevention messaging. Stakeholders also noted that vulnerable consumers are especially sceptical about the benefits of Smart Data schemes in terms of what value they would get in return for sharing their data.

2. **Lack of transparency when securing consumer consent for data sharing, and difficulties faced by vulnerable consumers in fully comprehending information around consent.** The use of Digital Identities, complex algorithms, data storage procedures, and terms and conditions can make consent a confusing process for vulnerable consumers, particularly those with low numeracy, literacy, and/or digital capabilities. The complexity of consent means that the information is challenging to present in a transparent but accessible way. It was therefore felt that most consent processes put the burden of responsibility on the consumer, without helping them to understand the risks involved in data sharing. There are also practical difficulties with reading documents on a smart phone screen for those with certain vulnerabilities.

3. **Consumers not having appropriate control over how their data is being used, as well as personal data being used to unduly influence decision-making or determine access to products and services.** 'Legitimate interest' for data collection and storage is currently vaguely defined, allowing app providers to collect a large number of data points beyond what they need to provide a particular use case, or store historical data even after a particular service has been delivered. This data can then be utilised to design targeted marketing, behavioural 'nudges' and highly personalised pricing, allowing firms to discriminate between different consumer profiles, creating particular risks for vulnerable consumers who could be restricted in their choices (i.e., by being priced-out accessing particular products, either because personal data indicates they may be a higher-risk consumer, or that they show a higher willingness-to-pay because they need products – such as credit – more urgently).

4. **Limited support or processes for remedying issues when things go wrong within Smart Data schemes, further impacting consumers' trust.** Increased data sharing also comes with increased opportunities for fraud and other security issues. Once more comfortable sharing personal data, vulnerable consumers may be more likely to wrongly identify legitimate schemes, leaving them at risk. The current data ecosystem is complex, and lack of a clear system for remedying issues when things go wrong ('redress') may heighten vulnerable consumers fears, and lead them to withdraw from schemes.

Summary of principles for designing inclusive Smart Data schemes

Having identified four main barriers to inclusivity from the existing literature and stakeholder workshop, each barrier was reconceptualised in terms of the desired outcome schemes should look to achieve with consumers:

1. Schemes and their providers being regarded as trustworthy (**'Trust'**);

2. Consent for data sharing being easy to understand, manage and revoke (**'Consent'**);

3. Choices and decisions being presented to consumers in a manner that does not undermine their control of the process (**'Control'**); and

4. Routes for support and redress being clear and easy to access where participation in Smart Data schemes leads to confusion or issues (**'Support and redress'**). Support refers to assistance and guidance that can be provided to consumers in a Smart Data scheme, to help them understand and manage their data. Redress, on the other hand, refers to the process of addressing and resolving complaints or issues that consumers may have with how their data is being handled or used.

Primary research with scheme stakeholders primarily focused on validating that these are the priority areas for focus, and then creating practical design principles to mitigate the risks posed to vulnerable consumers in each area. Below we summarise the key principles which emerged from discussions.

These principles provide an indication for government bodies and Smart Data scheme designers to inform Smart Data policy and scheme design. These principles represent the results from research findings and does not necessarily represent government policy.

Creating trust in Smart Data schemes

A significant amount of the literature reviewed identified 'trust' as a key factor in the adoption of Smart Data schemes by consumers, and this was confirmed by stakeholders as a major barrier. Vulnerable consumers are less likely to feel confident engaging with new initiatives and prefer to stick to processes which feel familiar. They can also be sceptical of the benefits of Smart Data, as the value they will receive from sharing data is often implicit and it is difficult to understand what meaningful improvements they might see to their personal financial situation.

Embedding the following principles in scheme designs may help drive trust among all consumers, particularly vulnerable consumers:

1. Focus on bringing to life the benefits and value consumers will get from the scheme to balance concerns raised by terminology around 'openness' and 'sharing', and communicate the risk-reward of Smart Data.

2. Ensure signup mechanisms for schemes and applications allow trusted contacts in a consumer's life (e.g., a guardian, carer, friend or family member) to support vulnerable consumers in assessing trustworthiness where necessary.

3. Utilise offline community touchpoints to raise awareness of what Smart Data is, and the benefits of participation in schemes, *before* vulnerable consumers are directly contacted to ask them to participate or opt-in.

4. Be transparent about what data is held and focus on the tangible benefits and risks to consumers of participating, with detailed explanation about how schemes work from a technical standpoint shown only upon request.

5. Publish guidelines on common terms to be used in Smart Data applications, to ensure that the same terms are used within and across industries.

6. Consider establishing scheme-specific 'trustmarks', to be awarded to firms by a trusted body in the industry with whom vulnerable consumers have prior familiarity. Make the criteria for accreditation publicly accessible.

Consent, consent management, and consent revocation

The way in which consumers are required to provide consent for data sharing may create barriers for vulnerable consumers. The terminology and processes can be confusing and overwhelming, and these can be even more difficult to digest in a digital context where it is difficult to present a large amount of complex information on-screen in an informative, yet concise, way. As a result, vulnerable consumers may not accurately grasp how their data will be used, how long a provider has access to their data, if they can/what the process is for revoking their data and/or how their data is built into algorithms. This could lead to a vulnerable consumer disengaging with a scheme (and therefore missing out on important benefits), or sharing data without full understanding the implications.

There are challenges to standardising consent, as these will vary according to the risks posed by a particular use case, but overall the following principles emerged as useful considerations for building a more inclusive consent journey:

Giving consent

7. Include *minimum* standards for consent forms within scheme design, to ensure a concise explanation of which data is to be shared and how long it will be retained for, explained *in terms of* the functionality which it enables.

8. Ensure that vulnerable consumers can access schemes and consent to share their data via preferred offline, non-application-based channels, such as via telephone.

9. Allow for a ‘basic’ consent option where only the data which is absolutely necessary for a particular function or service is granted.

Managing consent

10. Consider establishing a cross-scheme Smart Data dashboard which provides consumers with a consolidated view of the data they have consented to share and the purposes for which they have consented to share it. Consumers should then be able to make changes to consent via this central dashboard.

11. Send periodic reminders to consumers through their preferred communication channel to provide them a summary of the data they have consented to share and prompt them to review it and make changes as appropriate.

12. For the most sensitive types of data (e.g., health or finance-related data) that are not critical to the specific service being provided directly to consumers, consider introducing a standard set of ‘expiry times’ for consent, to be used across schemes. These could be accompanied by prior reminders about the expiry and any impacts, possibly integrated into a cross-scheme dashboard.

Revoking consent

13. Require a clear explanation of consent revocation processes to be included whenever consent is asked for or reminders to review consent are shared, to make the process as straightforward and low effort as possible.

14. Introduce a ‘cooling off’ or grace period where consumers can withdraw consent without any adverse consequences or commitment to the services with which they shared their data.

Choice architecture and consumer control

The high volume of data collected by some application providers within schemes poses a risk to vulnerable consumers in particular, as providers may use this to manipulate consumers based on their sensitive circumstances (e.g., their mood, personality, stress levels, mental health or emotional state). These practices can reinforce existing inequalities by allowing firms to discriminate between different consumer profiles, creating particular risks for vulnerable consumers who could be restricted in their purchasing choices and therefore experience unfavourable pricing. Another concern relates to app design; namely, that user experiences may be designed to push a consumer to make a certain decision quickly when it may not be in their best interests.

The following principles were identified as strategies to ensure vulnerable consumers retain control over decision-making within Smart Data schemes:

15. Make decisions as clear and unbiased as possible, enabling consumers to make educated and uninfluenced decisions in their own favour.

16. Better deals or preferential prices should not be based on the amount of data a consumer is willing to share, and consumers who are less engaged in schemes should not pay more for the same products and services as those who are using schemes more extensively and regularly.

17. If personal data is retained and aggregated (with consumers’ permission) to inform the development and marketing of specific products, there should be clear guidelines on what is considered fair targeting and pricing to avoid vulnerable consumers being offered inappropriate products, that they still have the choice of a range of products to meet their needs and/or that they do not pay a premium for the same services compared to non-vulnerable consumers.

18. How easy or difficult transactions are within schemes (the level of ‘friction’ attached to them) should be risk-based. When high risk decisions are being made it is important that risks are clearly communicated and that cooling off periods or buffers are built into application design.

19. Ensure that design throughout applications allows trusted family, friends or other advisors to help vulnerable consumers, but also that this be implemented in a way that does not require consumers to give that advisor full control.

Support and redress

Finally, given the complex nature of Smart Data schemes, it is likely that consumers – particularly those who are vulnerable, will require support. The digital nature of schemes mean some consumers may find it difficult to access use cases. In some instances, a trusted close contact may be able to support them to engage with schemes online, but not everyone will be able to rely on these networks. More broadly, data sharing comes with a number of risks, and lack of clear system for remedying issues when things go wrong (‘redress’) may heighten vulnerable consumers fears around getting a decision ‘wrong’, and lead them to withdraw from schemes.

The final two principles suggested by this research are aimed at mitigating these issues:

20. Wider, wrap-around support and troubleshooting should be delivered by a consistent and clear point of contact (e.g., the data holder), and be accessible through multiple formats - including offline communication channels.

21. Create a system for redress, ideally by widening existing regulators' scope to include Smart Data schemes, as these institutions are often already familiar to consumers.

Conclusions

As shown by this research, without careful design Smart Data schemes risk excluding those with vulnerable characteristics, or even causing further harm. Each of the twenty-one design principles discussed aims to mitigate one of the four aforementioned features of Smart Data schemes which have the potential to exclude vulnerable consumers, but it should be noted that none have been directly tested with vulnerable consumers. Principles relating to user experience design – particularly the consent journey, consent dashboards, trustmarks and support services – would benefit from further research to validate that they deliver on the needs of vulnerable consumers and do not have unintended consequences.

Across the principles highlighted, there are also four overarching considerations for the future development of inclusive Smart Data schemes. Like the principles, these considerations are also mainly based on the primary research, and can be regarded as broader themes which encapsulate the individual design principles.

1. Inclusive design is best achieved through principles which address specific needs or outcomes, rather than ones which targeted at specific types of vulnerability. Vulnerability is varied and transient, and consumers can have multiple vulnerabilities at once. Given this, and the fact that there are common risks and needs for Smart Data across vulnerabilities, making outcomes such as trust and control the focus could streamline the design process and deliver better outcomes than creating principles which are specific to each type of vulnerability.

2. Schemes should be based on a fair and transparent exchange of personal data for services, and each use case should clearly demonstrate the tangible benefit it provides to consumers. Regulatory frameworks should reflect the significant value that a consumer's data holds to them, and ensure that they maintain overall control over how it is collected and used.

3. The regulatory framework for Smart Data schemes needs to strike a balance between standardisation and innovation. Instead of stipulating a consistent template for aspects such as consent, the regulatory framework should clearly articulate certain *minimum standards* for data holders and app providers in terms of the language they use, the information they provide to consumers about risks and benefits, and how long data is held for.

4. Who is accountable when things go wrong needs to remain clear and consistent even as the landscape becomes more complex. A robust system of support and redress is especially important given that Smart Data schemes will facilitate the entry of many new and lesser-known firms into the market, making the landscape more complex for consumers to navigate. This accountability needs to be underwritten with a strong
5. regulatory presence for each scheme through new powers of existing industry regulators.

Introduction

Background and policy context

Building on the 'right to data portability' under the UK General Data Protection Regulation (GDPR), Smart Data is the secure sharing of customer data, upon the customer's request, with Authorised Third Parties (ATPs). ATPs then use the customer's data to provide innovative services, such as automatic switching or better account management. In 2017, Open Banking was established as the UK's first Smart Data scheme, with the nine largest payment services providers mandated to participate under the Competition and Markets Authority retail banking order. This scheme has continued to gain momentum, with 7 million consumers and SMEs actively using Open Banking services as of January 2023, with the annual potential benefits estimated as £12 billion for consumers and £6 billion for businesses[7].

The Department for Business and Trade (DBT) now wishes to support the growth and acceleration of new Smart Data schemes and increase cross-sector exchange of information. Smart Data offers an opportunity to empower consumers, increase competition and unlock innovation. In March 2023, the government therefore introduced Smart Data legislation into the House of Commons – as part of the DSIT Data Protection and Digital Information (DPDI) Bill (No. 2) – seeking powers to enable the Secretary of State or HM Treasury to mandate industry participation in Smart Data across the economy.

As DBT looks to support the development of potential new schemes such as Open Finance, Open Communications, and a Smart Data energy scheme, there is recognition that consumers with vulnerable characteristics will interact differently with Smart Data schemes. Specifically, DBT wants to mitigate the risk that these consumers may be unable to effectively engage with a scheme and are at higher risk of harm, if schemes are not designed appropriately. For instance, vulnerable consumers may be exposed to unfair practices, may not receive the appropriate level of protection from fraud or scams, or may find that there is not appropriate support mechanisms when things go wrong.

The most recent FCA Financial Lives survey in May 2022 showed that 47% of UK adults showed one or more characteristics of vulnerability, namely: poor health such as cognitive impairment, life events such as new caring responsibilities, low resilience to cope with financial or emotional shocks, and low capability such as poor literacy or numeracy skills.[8] As part of the delivery of new schemes, DBT will aim to encourage opportunities that ensure Smart Data is utilised by unengaged or less engaged consumers, while also looking to reducing the risk of Smart Data schemes worsening inequalities faced by vulnerable consumer groups[9]. It is DBT's ambition that Smart Data schemes are designed so they benefit the whole market.

[7] BEIS, 2021a. *Smart Data Working Group: Spring 2021 report*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/993365/smart-data-working-group-report-2021.pdf; Open Banking, 2023. *UK reaches 7 million Open Banking users milestone.* Retrieved from https://www.openbanking.org.uk/news/uk-reaches-7-million-open-banking-users-milestone.

[8] FCA, 2022. *Financial Lives 2022 survey: insights on vulnerability and financial resilience relevant to the rising cost of living.* Retrieved from https://www.fca.org.uk/data/financial-lives-2022-early-survey-insights-vulnerability-financial-resilience.

[9] BEIS, 2021b. *Regulatory Powers for Smart Data Impact Assessment (IA).* Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/915974/smart-data-impact-assessment.pdf.

Research objectives

To support DBT's ambitions to ensure the inclusivity of future Smart Data schemes, Savanta was commissioned by DBT to undertake research in this area with two core objectives:

1. To improve government understanding of what an inclusive Smart Data scheme looks like, and understand the scheme design features that lead to an inclusive scheme.

2. To establish lessons and practical design principles that would need to be applied to create inclusive Smart Data schemes in key markets.

Based on the above aims, the research sought to answer five key research questions:

1. What vulnerable characteristics are most likely to lead to consumers being excluded by Smart Data schemes?

2. What design features of Smart Data schemes lead to excluding vulnerable consumers?

3. What design features of Smart Data schemes promote inclusivity?

4. What do app providers and data holders believe are the barriers to Smart Data schemes being inclusive, and how can we combat these issues?

5. What practical design principles can be put in place to make Smart Data schemes more inclusive to all consumers?

Research methodology and definition of key concepts

To answer the research objectives and questions listed above, Savanta undertook research in two stages. Stage 1 being a literature review and stage 2 qualitative research, in the form of a workshop and interviews.

This two-stage approach was devised and considered the most appropriate as the literature review would first allow us to synthesise existing knowledge, and then map the evidence gaps. This would then be used to inform the design of the qualitative (primary) research and ensure that further research builds on existing knowledge. The qualitative research took the form of an in-person workshop, followed by individual in-depth interviews with another group of stakeholders. This format was suggested as a workshop would bring together a mixture of audiences and experts, which would allow for greater reflection, opinion and generally richer discussions. It was also felt that having an in-person workshop would maximise collaboration between stakeholders and allow Savanta to more easily facilitate both within-industry and cross-industry working, and the individual interviews taking place after the workshop allowed some of the themes and findings to be tested.

Stage 1: Literature review

Between January and February 2023, Savanta carried out a review of existing evidence to establish what inclusive Smart Data schemes could look like across a range of vulnerabilities and identify gaps in the grey and academic literature before primary qualitative research was conducted amongst key stakeholders involved in Smart Data scheme design.

Studies were initially identified through a key word search for relevant academic and grey literature, with the list of key search terms developed in collaboration with the Smart Data team. Additional sources were then added to the review from the pre-identified literature. Alongside their demonstrable relevance to the project, sources were also screened for their methodological quality, reliability and the research type (primary or secondary)[10].

In total, 43 studies were identified, with 20 of these deemed most relevant to the project reviewed in full. The sources reviewed primarily focus on one, or in some cases multiple, of the following aspects: vulnerable consumers, Smart Data schemes both within the UK and abroad, and inclusive design principles from areas outside of Smart Data. Savanta then analysed the reports in a comprehensive Excel framework which recorded types of vulnerability referenced in each source (in accordance with the FCA definition of consumer vulnerability), the suggested implications of scheme design for helping or hindering inclusion, and specific design features related to key use case(s).[11]

Stage 2: Qualitative research with app providers, data holders and advocacy groups

Following the literature review, primary evidence on practical design principles was gathered through qualitative research with key stakeholders involved in the delivery of inclusive Smart Data schemes. Stakeholders were categorised into three main sub-groups:

- **Data holders:** organisations who hold data on customers that they would be required to share securely, at the customer's request, with ATPs under Smart Data schemes. Representatives from banks and energy suppliers are examples of this kind of stakeholder. This also includes membership organisations who represent data holders.
- **App providers:** organisations aiming to develop innovative solutions using the customer data shared under Smart Data schemes.
- **Inclusion advocacy groups:** organisations who represent the interests of individuals with vulnerable characteristics.

A total of 21 stakeholders[12] participated in the qualitative research. 12 participants were convened in a 4-hour face-to-face workshop, involving:[13]

- A presentation to the group from Savanta and DBT to provide the context for the research, and an overview of the findings of the literature review. A 2-page summary of the literature review was also shared with participants before the workshop.
- Three 90-minute mini-groups each with four participants (from across the stakeholder types) to discuss issues and solutions in more detail. A discussion guide was used to guide groups through discussion and it touched upon: experts knowledge of and experience with vulnerable consumers and Smart Data; vulnerability types and the barriers faced by different vulnerable consumers; principles for designing for vulnerability (using the three pillars consent, trust and control and choice architecture as a base); and other design principle suggestions.

[10] Sources were evaluated using an analytical framework in Excel. The framework was devised to and prompted the reviewer to question the reliability and methodological quality of the source. Sources, which were deemed methodologically weak (small base size), lacking in reliability (problematic or potential author biases), irrelevant or simply not helpful to the research were excluded through the review process. If a source was deemed as low quality / not helpful to the research, it was excluded from a further in-depth review.

[11] A more detailed explanation of the literature review is included in Appendix A.

[12] Of the 21 stakeholders, 12 were data holders, 4 were app providers and 5 were from advocacy groups. This represents a small proportion of the relevant organisations across each of these groups, which would include all businesses in the relevant sectors, all potential future app providers and all advocacy groups in the area. The participants were targeted based on previous experience with vulnerable consumers and / or Smart Data and chosen to ensure a good mix across these groups in the relevant sectors.

[13] The discussion guide which formed the basis of the qualitative research, is included in Appendix B.

- A 1-hour plenary session, in which each group presented back a summary of their recommendations for practical design principles. After hearing from the groups, live polling was used to probe, prioritise and dig deeper into design principles. This involved 'voting' on how to prioritise the principles which were discussed in each of the focus groups, in order to prompt discussion across groups.[14]

This insight was supplemented by 9 subsequent in-depth interviews with stakeholders who did not attend the workshop, with each lasting between 45 and 60 minutes. This approach ensured that the views of those who were unable to attend were captured, and had the additional benefit of enabling the hypotheses and findings of the workshop to be tested after the event.. The interviews allowed experts to speak freely and in detail about the subject and discussions mirrored the content covered in the 90-minute focus groups with workshop attendees.

Participants were recruited via email using a list of pre-agreed contacts[15], provided by DBT, supplemented by Savanta with relevant contacts sourced through desk research. No incentive was offered for participation in either the workshop or in-depth interviews.

Methodological limitations and areas for improvements

Although the methodology was thoughtfully designed, there are a few limitations that must be acknowledged:

- The qualitative nature of the research allowed us to collect detailed information from multiple experts and delve deeply into their perspectives. However, it's important to keep in mind that the study involved a limited number of participants, which could mean that not all opinions have been adequately represented.

- Owing to the scope of the research, no vulnerable consumers were included in the study, and we did not conduct any user testing. As a result, the conclusions are based solely on the experiences and viewpoints of industry and vulnerability experts, rather than on the usage or experience of those with characteristics of vulnerability. Given the need to develop design principles which cut across multiple industries and types of vulnerability, speaking to those with expertise in designing for inclusivity was felt to be the most effective and comprehensive starting point in addressing the needs and challenges of a wide range of vulnerable consumers across multiple markets.

- It is also important to note that certain scheme-specific considerations may not be evident in these generalised discussions and they must be accounted for.

- The experts that were contacted were diverse in sector and background; however, there was a notably smaller proportion of experts from advocacy groups and so the views and knowledge of those who work closely with vulnerable consumers are limited in comparison to other experts.

- Finally, due to the tight timing of the research project, the extent and thoroughness of the literature review and qualitative research were restricted. Tight timings, not only

[14] This was conducted using the online tool by Poll Everywhere. Note that this was primarily used as a tool to facilitate discussion and debate across groups, rather than to quantitatively measure the perceived effectiveness of any of the principles discussed here. A larger sample size would be needed to robustly undertake any such quantitative research, so it is worth emphasising that this was not the purpose of this polling exercise.

[15] Out of a list of 55 contacts, 21 agreed to participate in the workshop or an interview.

added restrictions to the breadth and depth of the literature review but also could have affected expert's ability to attend given the relatively short notice. Thus if more time was allowed a literature review with a wider scope could have been developed and a larger proportion of stakeholders could have possibly been recruited.

When interpreting the findings of the study, all these limitations must be taken into account.

Consumer vulnerability and Smart Data schemes

Summary

This chapter introduces the concept of consumer vulnerability, and explores the evidence around what consumer vulnerability means in the context of Smart Data schemes, how consumers with vulnerable characteristics may interact with schemes, and the benefits, risks and challenges of schemes to vulnerable consumers.

Smart Data schemes may be particularly beneficial for vulnerable consumers in allowing for greater targeting of support in essential services (e.g., energy) where these consumers may have previously been reluctant to self-identify as vulnerable. However, the main challenge for future Smart Data schemes is designing core use cases and services so that they are accessible to everyone. The existing literature and stakeholder discussions found that Smart Data poses risks to each of the four forms of vulnerability, and in particular the digitally excluded, those with low numerical, literacy, and digital skills, and those with some health conditions that may make evaluating risk more difficult. Moreover, for low-income consumers, even if they are able to effectively evaluate the risk of a transaction, Smart Data schemes may lead to disadvantage by increasing the likelihood that firms will use personal data to offer this group higher prices for the same products and services.

Through the literature review and primary research, four features of Smart Data schemes which could potentially lead to vulnerable consumers being excluded, or result in harm being caused, were identified:

1. Low consumer trust and confidence in a scheme as a key barrier to adoption, both in terms of how data is collected, stored and used, and the benefits of the scheme.

2. Lack of transparency when securing consumer consent for data sharing, and difficulties faced by vulnerable consumers in fully comprehending information around consent.

3. Consumers not having appropriate control over how their data is being used, as well as how personal data may be used to influence decision-making or determine access to products and services.

4. Limited support or processes for remedying issues when things go wrong within Smart Data schemes, further impacting consumers' trust.

Overview

As set out by the FCA, a vulnerable consumer is someone who, due to their personal circumstances, is especially susceptible to harm in a market, particularly when an organisation is not acting with appropriate levels of care[16]. All individuals are at risk of becoming vulnerable at some point, underpinned by four key drivers of vulnerability: health, life events, resilience, or capability. Two main ways in which vulnerable consumers could come into contact with Smart Data schemes emerged from the literature review, each with their own benefits and challenges.

[16] FCA, 2021. *Guidance for firms on the fair treatment of vulnerable customers,* [Online]. Retrieved from https://www.fca.org.uk/publication/finalised-guidance/fg21-1.pdf.

Firstly, Smart Data schemes could be seen to bring significant benefits to vulnerable consumers through better data sharing between service providers to identify those eligible for additional support. For example, the process for identifying those eligible for social tariffs is currently a manual process, and requires consumers to self-identify as vulnerable and sign-up to the Priority Services Register.[17] This process can create barriers to receiving support; for example, because of a lack of awareness of the process of self-identifying as vulnerable, or because disclosing a vulnerability causes feelings of 'shame' and feels 'intrusive'[18].

Stakeholders interviewed in the qualitative research highlighted that Smart Data schemes could help tackle these problems around disclosure and facilitate better targeting of support by using customer data (e.g., sharing usage data from smart meters where the consumer has provided their consent, an individual's Universal Credit status) to identify those in need. The need for this use case was seen as particularly pressing in the context of the rising cost-of-living. This was seen to only lead to consumer betterment, with little to no risk for vulnerable consumers.

> *"In the telecommunications sector…different providers have different schemes in order to make sure that their products are affordable for vulnerable customers. And that is often on the basis of sensitive data that we receive from their part. The government is starting to intervene in order to make that easier. The Department for Work and Pensions has been working with BT and with Sky in order to develop an API that facilitates notification of whether someone is eligible to be considered vulnerable through their eligibility for Universal Credit."*

Stakeholder

> *"Thinking about something like the Warm Home Discount, for example, in the UK, or the ECO [Energy Company Obligation] Scheme where the government holds the data and the supplier just asks, basically, if they're vulnerable. And I think utilising some sort of data spine that enables service providers to make those sorts of requests reduces a lot of the concerns in this space around data sharing and ownership of data."*

Stakeholder

Secondly, and more broadly, inclusive Smart Data schemes can only be achieved if vulnerable consumers can benefit from use cases and services designed for all consumers ('whole-market' services). In this respect there are concerns that scheme designs could lead to a vulnerable consumer being unable to participate in a scheme, or receive a worse deal or service from a provider as a result of participating in a scheme. Practical design principles are therefore needed to ensure that scheme design considers the needs of vulnerable consumers, and this was the main focus of the literature review and qualitative research with stakeholders. The rest of this section sets out evidence for which forms of consumer vulnerability are most likely to be excluded from Smart Data schemes, and summarises the design features which most likely to lead to vulnerable consumers being excluded from schemes.

[17] The Priority Services Register is a free support service in the energy industry that ensures extra help is available to those who disclose that they are in vulnerable situations. In order to receive this support, vulnerable consumers must actively contact either their energy supplier(s) or network operator and disclose their needs.

[18] Elliot, K., 2022. *Know Your Customer: Balancing innovation and regulation for financial inclusion,* Data & Policy, 4, e34. Retrieved from https://www.cambridge.org/core/services/aop-cambridge-core/content/view/81ECE6589B2932FDCAD400E41EA36661/S2632324922000232a.pdf/div-class-title-know-your-customer-balancing-innovation-and-regulation-for-financial-inclusion-div.pdf

The impact of Smart Data schemes on different forms of consumer vulnerability

Previous research into vulnerability and Smart Data schemes has tended to talk about vulnerable consumers as one single group, so evidence for how specific types of vulnerability may interact with Smart Data schemes and specific use cases is inconsistent. Workshop and interview discussions therefore focused on understanding how each form of vulnerability would affect how consumers engage with Smart Data schemes. The forms of vulnerability discussed in this report are:

- Low capability:
- Poor health;
- Low financial resilience; and
- Negative life events.

The next four subsections discuss each of these forms of vulnerability in turn. It is also important to note that all consumers are at risk of becoming vulnerable, and that consumers may show more than one form of vulnerability and therefore subject to different forms of risk.

Low capability

Low capability refers to consumers who have poor skills in areas such as numeracy or literacy, have low digital skills, or are digitally excluded and therefore do not have the opportunity to engage with online services. The 2022 FCA Financial Lives Survey found that 19% of all UK adults have low capability[19].

Among participants in the focus groups and interviews, this form of vulnerability was seen as particularly likely to be excluded from the benefits of Smart Data schemes. Firstly, those without access to the internet will not be able to authorise data sharing and use applications developed for use cases within schemes, and therefore may be at risk of getting a worse deal than consumers who are able to engage online. There is also a broader concern that products will be increasingly digitised at the expense of more traditional provision – such as telephone or in-person services – which are more accessible to consumers with low capability[20]. Stakeholders highlighted that it would be a challenge to account for digital exclusion in the design of Smart Data schemes, and minimising the exclusion of this group is likely to require wider interventions such as broadening access to digital devices. For example, Singapore has looked to empower and upskill consumers through training and giving digital devices to low-income households alongside the launch of Smart Data schemes[21].

Beyond digital exclusion, low numeracy, literacy, financial understanding, or digital skills may lead a consumer to find it difficult to assess the legitimacy of scheme, app or website, as well as use its interfaces. That said, one study found that those with higher financial literacy are more likely to be wary of Open Banking, but also that those with higher levels of education and behaviour of switching are more trusting in Open Banking compared to others[22]. Therefore, financial literacy does not guarantee engagement, but is indicator of a person's ability to critically evaluate a platform or service.

[19] FCA, 2022, op. cit

[20] Leong, E. & Gardner, J., 2021. *Open Banking in the UK and Singapore: Open Possibilities for Enhancing Financial Inclusion,* Journal of Business Law, Issue 5 [Online], Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4194256. review of Australian Open Banking Schemes.

[21] ibid

[22] Chan, R., et al, op. cit

> *"It's a real problem…if these new tools come through that allow younger, smarter, digitally-savvy people to get better deals and switch more easily, then you've got a rump of older, non-digitally active consumers who are effectively, in the long run, going to lose out."*

Stakeholder

Poor health

Poor health refers to physical or non-physical, visible or hidden, health conditions or impairments which impact an individual's day-to-day activities. 7% of UK adults are classified by the FCA as having a health-related vulnerability[23].

Consumers with mental ill-health or addiction issues emerged as a particular concern in the context of Smart Data schemes both in existing evidence and in the workshop and interviews conducted. These types of health conditions would make it more difficult to evaluate the risk of a particular transaction, especially if key decisions are made easier under a Smart Data scheme, in addition to there being many new entrants bringing innovations to the market as a result of the scheme. This could leave consumers at higher risk of making poor decisions about their finances, or of being a victim of a scam. That said, if designed correctly Smart Data could bring new benefits to consumers who are comfortable pre-identifying themselves as having a vulnerability. For example, spending data could be used identify patterns of behaviour (e.g., multiple erratic purchases) linked with health conditions such as bipolar, and to trigger a warning for a financial services provider to proactively offer support.

Consumers with poor health may be more likely to also have low capability, and therefore may struggle to engage with the applications and use cases developed as a result of Smart Data sharing if they are not designed in an accessible way.

> *"I think there are certain types of vulnerability that actually make it very hard to discriminate between genuine and fake services, and therefore being prone to scams."*

Stakeholder

Low financial resilience

Adults are described as having low financial resilience if they have little capacity to withstand financial shocks, or because they have already missed paying domestic bills or credit commitments in 3 or more of the last 6 months. 24% of all UK adults are deemed to be of low financial resilience[24].

The use cases which could be enabled by Smart Data schemes are mainly seen to be beneficial for consumers with low financial resilience, as many are oriented towards encouraging money-saving, budgeting, and shopping around for the best – and potentially cheaper – deals on essential services. The literature review also found that Smart Data schemes could facilitate the use of non-traditional data (e.g., digital footprint providing an indication of their habits, where they shop etc.) could improve financial inclusion by, for

[23] FCA, 2022, op. cit
[24] ibid

example, enabling consumers with no credit history to obtain a loan (Autorité des Marchés Financiers Québec, 2022)[25].

However, analysis of 49 current Open Banking schemes internationally found that high-cost borrowers (who are typically on lower-incomes) may be negatively impacted by the increased access to customer data facilitated by a scheme. Firstly, where consumer data is used to model consumer risk, Open Banking increases the likelihood of firms offering particular products, but at an increased cost to high-cost borrowers. Secondly, under this scheme consumer data can also be used to assess consumers' willingness to pay for particular services offered through the scheme, and therefore set different prices for different customers. Lenders charge more to the borrowers with a high willingness to pay; if especially-eager-to-borrow individuals are mainly from vulnerable sub-populations, this would worsen financial inclusion rather than improve it [26].

> *"I [think Smart Data enables services] to help save money, things to help budgets, things to help smooth ups and downs, and when things do go wrong, ways to personalise it."*

Stakeholder

Negative life events

Experiencing a negative life event, such as new caring responsibilities, a relationship breakdown, or bereavement, may lead to further vulnerability such as mental ill-health or low financial resilience. In 2022, 20% of UK adults had experienced a negative life event[27]. Stakeholders also noted that these may lead consumers to become more time-poor, and therefore less likely to engage with the suppliers of key services. These consumers may therefore stand to benefit from Smart Data enabled services that aim to automate decision-making and therefore save time.

> *"Time-saving monitoring-type services [would be useful]. Things that spot recurring subscriptions. You don't have time to go through your bank statements but this app does, and it goes, 'Have you seen these are the things you pay every month? Do you really still need them?'"*

Stakeholder

Conclusion

Overall, through discussions with stakeholders it was clear that, within these four broad categories, vulnerabilities are extremely varied and often interdependent, introducing challenges in assessing how a vulnerable consumer may be interact with a Smart Data scheme. Further to this, stakeholder discussions also highlighted a need to consider whether the services in a particular sector are delivered directly to an individual consumer (i.e., banking services) or to a household (e.g., energy and water). For the latter, the bill payer or

[25] Autorité des Marchés Financiers Québec, 2022. *Insights into the risks and benefits of digital financial services for consumers.* [Online] Retrieved from https://lautorite.qc.ca/fileadmin/lautorite/grand_public/publications/professionnels/doc-reflexion-consos-tech_an.pdf.
[26] Babina, T. et al., op. cit. Review of international Open Banking Schemes, including the UK.
[27] FCA, 2022, op. cit

decision-maker for that household may live with a vulnerable person, but not be vulnerable themselves.

One discussion point which emerged was that it may be beneficial to pivot away from focusing on specific vulnerabilities, and towards understanding the common needs vulnerabilities give rise to. Using this lens to inform design could help mitigate the risk of the firms involved in schemes making consumers vulnerable through poor design, and also is beneficial for app providers in that it allows them to cater for a core set of needs which cut across different forms of vulnerability. Therefore, the next section will focus on identifying specific design features of Smart Data schemes which may lead vulnerable consumers to be excluded.

> *"You don't need to know their vulnerability, you need to know their need. And if you know that need, it's a whole lot less sensitive than knowing the reason for that need. I would encourage people to steer away from particular vulnerabilities, or even focusing on the vulnerability, and to focus on the need and service."*

Stakeholder

Potential barriers to Smart Data schemes being inclusive

Building upon the analysis above on how different forms of consumer vulnerability may be excluded, the literature review and discussions with stakeholders identified four features of Smart Data schemes which could potentially lead to vulnerable consumers being excluded, or result in harm being caused, if not mitigated by scheme design:

1. Low consumer trust and confidence in a scheme

2. Lack of transparency when securing consumer consent for data sharing

3. Consumers not having appropriate control over how their data is being used

4. Limited support or processes for redress

It is worth noting that the primary research conducted as part of this research did not directly test these potential barriers amongst vulnerable consumers. Rather, interviews and focus groups were conducted with experts in vulnerability and industry experts.

Low consumer trust and confidence in a scheme

A significant amount of the literature reviewed identified 'trust' as a key factor in the adoption of Smart Data schemes by consumers. Equally, lack of trust can be a more significant barrier for vulnerable consumers. This was seen in a Citizens Advice Open Banking pilot, where 14% of Citizens Advice clients declined to participate in the pilot due to security or privacy concerns, or because they would prefer to have face-to-face money or switching advice [28]. Consumers with low capability may be particularly likely to have low trust in schemes. Often feeling powerless, vulnerable consumers will stick to what they know and what keeps them

[28] Citizens Advice, 2019. *Smart data: putting consumers in control of their data and enabling innovation.* [Online]. Retrieved from https://www.citizensadvice.org.uk/Global/Public/Policy%20research/Documents/Consultation%20responses/Citizens%20Advice%20consultation%20response_%20smart%20data%20review.pdf. Review of UK Open Banking Schemes

‘safe’. Vulnerable consumers can also be increasingly distrustful of organisations and schemes and so an aversion to Smart Data schemes is not unpredictable[29].

Low trust was confirmed by stakeholders as a major barrier to the inclusiveness of schemes. They noted from their own research in the area that there is widespread distrust in organisations and institutions storing personal data securely and using it correctly. Related to this, consumers being encouraged to share their data with multiple different providers and institutions feels counterintuitive in the context of fraud and scam prevention messaging urging consumers to be vigilant when it comes to sharing personal details. Smart Data schemes will enable new, unfamiliar players to enter these markets, and vulnerable consumers may feel that increased data sharing means they would be even more likely to be targeted with scams.

Stakeholders also noted that vulnerable consumers are especially sceptical about the benefits of Smart Data schemes. The very association of the words ‘smart’ and ‘open’ with the scheme may raise concerns with consumers around security and privacy, and the value consumers will receive in return for sharing their data is often abstract and implicit, rather than tangible and specific. This can leave vulnerable consumers wondering what meaningful improvements they would see to day-to-day financial decision-making through participating in the scheme. Finally, a further worry is that if they identify themselves as vulnerable or share data which might indicate that, a provider will restrict the products and services they have access to.

> *“I think particularly up until quite recent history, we’ve always said, 'Don't share your bank account details. Don't tell anyone. Don't log into your bank account. Don't click on this link.' Now all of a sudden, we're going, 'Click on the link.'”*

Stakeholder

> *“When it is new information, vulnerable people find that, obviously, harder to process and are a bit more wary of it. So, all these new schemes and especially when technology's involved, it's kind of, overcoming that.”*

Stakeholder

Lack of transparency when securing consumer consent for data sharing

The way in which consumers provide consent for data sharing and authenticate their identity also emerged as an area which may lead to the exclusion or harm of vulnerable consumers. Previous research has found that the provision of consent – with the use of Digital Identities, complex algorithms, data storage procedures, and terms and conditions – can be a confusing process for vulnerable consumers, particularly those with low numeracy, literacy, and/or digital capabilities. In particular, a review of the risks and benefits of digital financial services in Canada noted that the digital context can make the process of gaining informed consent more challenging. There are practical difficulties with reading documents on a smartphone screen, and efforts made to shorten, simplify or compile the information in such a way as to fit a smartphone’s small screen may end up making the information difficult to understand or

[29] FinTechNZ, 2022. *Aotearoa Open Finance and Digital Equity*. [Online]. Retrieved from https://fintechnz.org.nz/wp-content/uploads/sites/5/2022/03/FinTechNZ-Report-2022_digital_03.22.pdf.

ambiguous. In addition, the over-provision of information may lead to consumers becoming overwhelmed and therefore decision-making paralysis[30].

Similar to ‘trust’, the issues around consent also relate to the power and knowledge imbalance that exists between consumers and providers of a Smart Data enabled service within a Smart Data scheme. It can be difficult for all consumers, including those with vulnerabilities, to grasp how their data will be used, how long a provider has access to their data, if they can/what the process is for revoking their data and how their data is built into algorithms. In turn, this could lead to vulnerable consumers:

1. Choosing not to share data with a scheme (which prevents them from benefitting from such APIs). This could be exacerbated by ‘binary consent’ – where a consumer must consent to their data being collected and used by a firm to use a service – which can lead to vulnerable consumers feeling like they lack control over their data[31]. Moreover, if certain data on these users are unavailable, there is the risk that providers will consider these users to be higher-risk, further exacerbating financial exclusion [32].

2. Consenting to sharing their data when they do not fully understand the scheme or the implications of data sharing, opening themselves up to other possible harms (such as excessive personalisation and targeting, which will be covered in more detail in the next section). This could be exacerbated by ‘bundling’, a process whereby a user may be asked to share multiple data points without a clear idea of what services within a scheme are using it. This may allow scheme to capture more data than consumers' use of services / the scheme actually needs[33].

In discussions with stakeholders, there was broad consensus that the consent processes widely used in digital technology are not accessible to consumers in general, let alone those with vulnerable characteristics. The complexity of consent means that the information is challenging to present in a transparent but accessible way. It was therefore felt that most consent processes put the burden of responsibility on the consumer, without helping them to understand the risks involved in data sharing.

However, stakeholders also acknowledged there are challenges to standardising the consent process across Smart Data use cases, since each use case will require a different level of consent. For example, a service which requires the sharing of high volumes of data or sensitive data would require a more complex consent journey. A use case which does not rely on sensitive data and has limited risk to the consumer (e.g., identifying whether a vulnerable consumer is eligible for a social tariff, as discussed above) could have a shorter consent journey; and an overly complex consent journey for simple, low-risk transactions could lead consumers to feel overwhelmed and therefore disengage with schemes.

[30] Autorité des Marches Financers Quebec, op. cit

[31] BEIS, 2018. *Implementing Midata in the Energy Sector: Government response to the Call for Evidence*. [Online]. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/729908/midata-energy-sector-government-response.pdf

[32] Croxson, K., Frost, J., Gambacorta, L. & Valletti, T., 2022. [Online]. *Platform-based business models and financial inclusion,* Retrived from https://www.bis.org/publ/work986.pdf

[33] BEIS, 2018, op. cit; CSIRO Data, 2018. *CDR Open Banking Workshop: Defining the UX of Consent,* [Online]. Retreived from https://consumerdatastandards.gov.au/sites/consumerdatastandards.gov.au/files/uploads/2018/12/Defining-the-UX-of-Consent-5.1-No-Appendices.pdf

> *"I think we're reaching the limit of what an average human being can comprehend and agree to. I don't know about you, but I worry about it as a tool to help consumers, I think it's increasingly just a way to allow firms to do what they want."*

Stakeholder

> *"I think we're very risk averse [as an industry] because everyone's terrified of getting a fine for doing it wrong. So, you put all the risk on the consumer by saying, 'Right here's everything. We've done our bit, it's your fault if you get it wrong now.'"*

Stakeholder

Consumers not having appropriate control over how their data is being used

In addition to securing informed consent, consumers losing appropriate control over decision-making within scheme use cases emerged as a third significant theme from the literature reviewed.

The high volume of data collected by some application providers within schemes poses a risk to vulnerable consumers in particular, as providers may use this to manipulate consumers based on their sensitive circumstances (e.g., their mood, personality, stress levels, mental health or emotional state)[34]. Stakeholders felt that 'legitimate interest' for data collection and storage is currently vaguely defined, allowing app providers to collect a large number of data points beyond what they need to provide a particular use case, or store historical data even after a particular service has been delivered.

> *"Over sharing data or data not being used in the way it was intended [could negatively impact vulnerable consumers], so, you have to be specific about the use of data; we've seen [firms] from Open Banking use data in ways that isn't probably very good, and so there needs to be some checks, controls, for that process."*

Stakeholder

This data can then be utilised to design targeted marketing and highly personalised pricing. These practices can reinforce existing inequalities by allowing firms to discriminate between different consumer profiles, creating particular risks for vulnerable consumers who could be restricted in their purchasing choices and therefore experience unfavourable pricing [35]Indeed, stakeholders had heard anecdotal examples of instances where the sharing of new types of data may even lead to vulnerable consumers being prevented from accessing products and services – for example, firms having a greater likelihood to decline consumers with certain conditions from credit products or offer more expensive premiums based on financial data shared through Smart Data schemes. That said, personalisation may also bring benefits to vulnerable consumers in allowing firms to identify and intercept negative behaviours and provide targeted support.

[34] Consumer Policy Research Centre, op. cit
[35] Ibid; Leong & Gardner, op. cit

> *"Something that I would be very concerned about, is this hyper-personalisation of data can mean that firms tailor their products to the healthy and the wealthy. They can deliver products and services to the consumers that they want to deliver to, that they know will be profitable, know will be good for their business, and they can deliberately or unintentionally exclude those consumers that are more difficult to serve."*

Stakeholder

Another concern is that app features can play on certain thought processes to influence decision-making and may even result in consumers making decisions not in their interests. This is partially achieved through how choices are presented to consumers, known collectively as the 'choice architecture' of a system.[36] Stakeholders recognised that some apps employ user experience design to 'push' consumers to make a decision quickly, creating the potential that – particularly vulnerable consumers – are unable to properly evaluate the risk of a transaction and therefore be harmed in the process. Similarly, it was also highlighted that vulnerable consumers may be more prone to potentially significant or detrimental impulse purchases late at night, and firms may engage in targeting practices aligned with this.

> *"I went to a recent panel on money and mental health, and they were saying vulnerable people were much more likely to make impulse buys in the middle of the night and if you look at targeted emails, a lot of the time they're sent at 2am. It's going to be vulnerable people…awake at that time or just having had a bad day and they're like, 'I might buy myself this, it'll make me feel much better.'"*

Stakeholder

A final consideration relevant to Smart Data scheme design is the extent to which decisions pathways have an appropriate level of 'friction' (anything makes it slower or harder for a user to accomplish a task) for vulnerable users, or conversely are presented in a way that make them appear 'easier' or less consequential than they really are. One Singapore qualitative study included in our review discusses overdrafts not connected to a current account (i.e., unbundled), an area of Open Banking in which the authors Leong and Gardner (2021) argue that "the frictionless nature of obtaining such loans may have a *detrimental* effect on the consumer's ability to exercise judgement over whether the information is really needed" [37](Leong, E. & Gardener, J., 2021). Here, the decision is presented to consumers in a way that makes it seem easy and manageable, but some providers pair this with a mechanism (Virtual Recurring Payments) where automatic repayments are taken when the consumer's bank balance increases by more than £50, with part repayment attempted if the initial attempt to reclaim the full amount is unsuccessful. Ordinarily, personal loans like overdrafts allow the consumer to maintain control over when they pay back the debt, even if a demand for repayment is made.

Limited support or processes for redress

In their study of Open Banking, Chan et al. (2022) also found that as it is a relatively new concept, people may rely more on social influence than in other areas[38]. Consumers may be reassured there are benefits if they see many other people using a scheme, thereby encouraging further uptake. However, vulnerable people may not always have close connections, such as friends and family, to support them to engage with schemes. A digital-only approach to delivering Smart Data schemes may therefore lead vulnerable consumers to

[36] For a general introduction to choice architecture see, for instance, Thaler, R. H. & Sunstein, C. R. (2008).
[37] Leong and Garner, op. cit. Review of Australian Open Banking Scheme
[38] Chan, et al. op. cit. Review of Australian Open Banking Schemes

be excluded, and vulnerable consumers themselves may be reticent to admit to a provider they do not know how to use certain features.

> *“I think, with the social proof piece, which is essential for vulnerable customers as well. They don't take advice from firms, they take advice from their neighbours, their friends, and their family.”*

Stakeholder

> *“I think, you know, groups, for example, like the elderly, would be excluded just because they won't be digitally enabled and they probably shy away from digital interaction. They'd rather go to branch and speak to people in person. So, I think it's important that we need to continue with an in-person bit, kind of, hybrid maybe of this is where you go first and then you can, you know, be handed off to a human. And an actual human, rather than a bot.”*

Stakeholder

Data sharing comes with a number of risks which the development of Smart Data schemes should be sensitive to, namely increased opportunities for fraud and other security issues. Not only does this increase fear something may go ‘wrong’, but it also increases the risks posed to vulnerable consumers - as they may wrongly identify legitimate schemes or become more comfortable sharing valuable data, leaving them at risk. Data leakage (unintended and unauthorised transfer of data from an organisation to an external source) could also results in consumers being targeted with scams or fraud, which vulnerable consumers have a higher likelihood of falling prey to [39]. Stakeholders highlighted that it is not currently clear whether data holders or Authorised Third Parties (ATP) are responsible for supporting consumers in these scenarios in a complex data ecosystem. A lack of a clear system for remedying issues when things go wrong (‘redress’) may heighten vulnerable consumers fears around getting decisions ‘wrong’, and lead them to withdraw from schemes.

> *“It's not just about interacting with your provider in a Smart Data scheme, it's about interacting with your provider and then letting them interact with your trusted third party, and I think that is a really hard bridge to cross with a lot of consumers.”*

Stakeholder

> *“You couldn't go to Open Banking and make a complaint about [a firm holding your data], saying, 'This is rubbish. It's not working. They need to fix it.' Because if you had to complain to the firm itself, it's useless. You've got to be able to complain to a higher party.”*

Stakeholder

[39] Consumer Policy Research Center, op. cit

Design principles for inclusive Smart Data schemes

Summary
This section discusses four key ‘pillars’ of inclusive design for Smart Data schemes, and how they are to be understood. Primary and secondary research suggest the need for an emphasis on trust, consent, control and redress when designing any future Smart Data schemes. Each of these outcomes is discussed in turn, with relevant scheme design principles suggested in order to ensure each outcome.

Overview

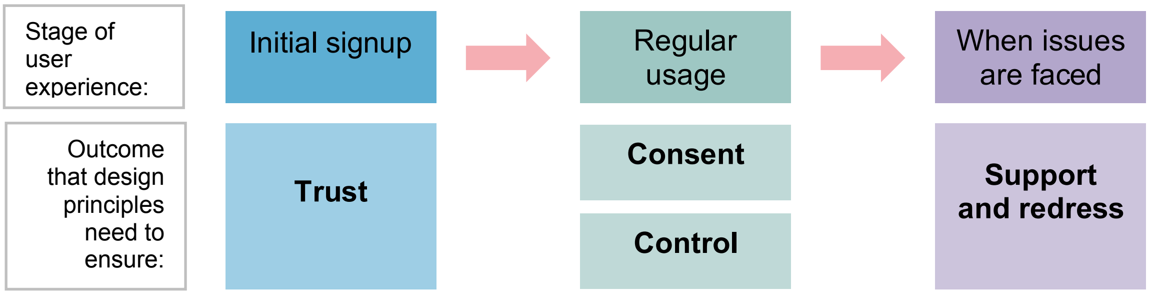
In order to develop design principles that promote inclusivity in Smart Data schemes, a clearer picture of the outcomes that would allow vulnerable consumers to access the benefits must be developed.

The outcomes, or ‘pillars’ of inclusive design, that the research identified as important are:

1. Schemes and their providers being regarded as trustworthy (**‘Trust’**);
2. Consent for data sharing being easy to understand, manage and revoke (**‘Consent’**);
3. Choices and decisions being presented to consumers in a manner that does not undermine their control of the process (**‘Control’**); and
4. Routes for support and redress being clear and easy to access where participation in Smart Data schemes leads to confusion or issues (**‘Support and redress’**). In this context, ‘support’ refers to assistance and guidance that can be provided to consumers in a Smart Data scheme, to help them understand and manage their data. ‘Redress’, on the other hand, refers to the process of addressing and resolving complaints or issues that consumers may have with how their data is being handled or used.

As can be seen in Figure 2, these pillars become more relevant at different stages of the user experience. Whilst these pillars are all relevant to all stages, the diagram shows the stage at which they become of primary importance. For instance, visible support and redress does make vulnerable consumers feel more comfortable and thereby more inclined to sign up – but trust is a bigger factor at this stage.

Figure 2 – the stages of user experience at which each design pillar becomes an essential outcome for inclusivity



Stage of user experience:	Initial signup	Regular usage	When issues are faced
Outcome that design principles need to ensure:	**Trust**	**Consent** **Control**	**Support and redress**

The remainder of this section details each of these four pillars in turn, explaining both why these are essential outcomes for a Smart Data scheme to be determined as inclusive, and what tangible steps might be taken to ensure each outcome is achieved in Smart Data schemes.

These principles provide an indication for government bodies and Smart Data scheme designers to inform Smart Data policy and scheme design. These principles represent the results from research findings and does not necessarily represent government policy.

Creating trust in Smart Data schemes

Summary of this subsection: design principles promoting trust in Smart Data schemes

1. Focus on bringing to life the benefits and value consumers will get from the scheme to balance concerns raised by terminology around 'openness' and 'sharing' and communicate the risk-reward of Smart Data.

2. Ensure signup mechanisms for schemes and applications allow trusted contacts in a consumer's life (e.g., a guardian, carer, friend or family member) to support vulnerable consumers in assessing trustworthiness where necessary.

3. Utilise offline community touchpoints to raise awareness of what Smart Data is, and the benefits of participation in schemes, *before* vulnerable consumers are directly contacted to ask them to participate or opt-in.

4. Be transparent about what data is held and focus on the tangible benefits and risks to consumers of participating, with detailed explanation about how schemes work from a technical standpoint shown only upon request.

5. Publish guidelines on common terms to be used in Smart Data applications, to ensure that the same terms are used within and across industries.

6. Consider establishing scheme-specific 'trustmarks', to be awarded to firms by a trusted body in the industry with whom vulnerable consumers have prior familiarity. Make the criteria for accreditation publicly accessible.

Every day, consumers mentally and sometimes subconsciously evaluate whether to trust a website, organisation or scheme with their personal data. A particular scheme being regarded as trustworthy is an important outcome in general, but lack of trust is a particularly significant barrier to initial adoption for vulnerable consumers specifically, as was discussed in the previous section on barriers to inclusivity.

If vulnerable consumers do not feel comfortable signing up for a Smart Data scheme in the first instance, on account of a lack of trust, then they clearly will not be able to access the benefits of that scheme. As such, developing design principles that create trust amongst vulnerable consumers is essential if Smart Data schemes are to be called inclusive.

A useful approach here is to consider the factors that are most likely to drive *distrust*, and how each might be mitigated. These factors fall into two categories: the contextual factors that make vulnerable consumers less likely to trust requests to share their data *in general*, and specific aspects of Smart Data schemes that are sources of distrust. This subsection considers each in turn, and suggests design principles that might be implemented to overcome each.

Factors that make vulnerable consumers distrust requests to share data in general

1. *Negative previous experiences with data sharing*

A common reason that vulnerable consumers are less likely to trust requests to share their data in general is that many have previously had a bad experience when sharing data or using a digital interface (which isn't a Smart Data scheme), which has caused them harm. As such, they are more likely to have negative associations with data sharing, even if the benefits are set out to them clearly.

> *"When people hear we [as data holders] have great access to [their] data and can do cool things with it,' […] it doesn't sound like something that would fill anybody with joy or promise, or cause anything other than a heightened sense of worry over what we're capable of doing. […It feels to vulnerable consumers] you hold all of the cards in an industry where consumers already believe we hold all of the cards."*

Stakeholder

Whilst overcoming this factor perhaps requires broader measures than effective Smart Data scheme design, it is valuable to discuss insofar as it further explains why trust is a particularly significant barrier to scheme adoption for vulnerable consumers specifically, over and above the general population.

Moreover, there *are* some practical implications for scheme design. This context determines the language that ought to be used when naming future schemes, or when advertising them through channels that are more likely to reach vulnerable consumers. 'Smart' and 'open' were identified in particular as terms which vulnerable consumers might associate with other instances of data sharing where they may have had a bad experience previously.

> *"If we look at this …from our customers' [perspective towards] businesses rather than businesses' [perspective towards] customers, what terms can we adopt and adapt that have encouraged them to be open and adopt new tools? What's succeeded and landed? I'd highly [recommend] go[ing] away from, 'smart' and 'open'".*

Stakeholder

In the former case, some stakeholders specialising in vulnerability expressed the concern that vulnerable consumers in the energy industry may associate the term 'smart' with smart *metering*, especially in the context of future schemes in the energy and utilities sectors. Whilst smart meters are designed to put consumers in control of energy use, some consumers in vulnerable situations may have negative associations with these meters and can be wary of them, and so this term could be avoided when naming future schemes in these industries. The concerns about the term 'open' are not industry specific, but still ought to be taken into account when naming schemes and developing communications to persuade vulnerable consumers to access the benefits of them. As such, the following design principle is supported by the research:

Recommended scheme design principle #1:

Focus on bringing to life the benefits and value consumers will get from the scheme to balance concerns raised by terminology around 'openness' and 'sharing', and communicate the risk-reward of Smart Data.

It is worth noting that the two terms given as examples here were identified by industry experts and experts on consumer vulnerability, rather than vulnerable consumers themselves. Direct research with vulnerable consumers themselves, across a range of industries, should be considered in order to accurately establish the specific list of terms to be noted for different industries.

2. *Low digital and/or financial literacy*

Another factor that makes vulnerable consumers less likely to trust requests to share their data *in general* is lower digital or financial literacy. These are markers of vulnerability, and those with lower levels of literacy in these areas find it harder to assess the trustworthiness of a scheme. This isn't necessarily to say that such consumers will be more distrusting. Rather, trust is a greater barrier for those with lower literacy levels in these areas because they are more likely to be unable to determine whether a scheme is trustworthy or not.

There are two broad strategies that scheme designers might employ to reduce the impact of this barrier. Either measures can be taken to ensure that vulnerable consumers can utilise the support of a trusted individual who is financially and digitally literate and is well placed to give trustworthy advice on scheme participation, or measures can be taken to increase the digital and financial education of those identifiable as 'vulnerable' in order to empower them to better make these judgements themselves. Attempting both at the same time is likely to be the most effective approach.

Many vulnerable consumers – often those with mental health conditions, cognitive impairments,[40] and the digitally excluded – rely upon family and friends for assistance with financial decision making, and the initial sign-up mechanism for schemes (or applications that are developed as part of schemes) should be designed to allow for their involvement. For instance, a variety of contact methods should be offered. Whilst a phone call is an appropriate alternative method of contact to offer to a digitally excluded vulnerable consumer who feels uncomfortable with app-based contact, it may in some instances be inappropriate, as the consumer will not be able to involve their trusted support in the process as readily as they might hope. This is just one example, but the more general design principle to draw from this is as follows:

Recommended scheme design principle #2:

Ensure signup mechanisms for schemes and applications allow trusted contacts in a consumer's life (e.g., a guardian, carer, friend or family member) to support vulnerable consumers in assessing trustworthiness where necessary.

Of course, not all vulnerable consumers have such support in their immediate networks or may even be isolated, so this cannot be relied upon as a sole means for overcoming this financial and digital literacy barrier, even if it can help in many instances.

[40] By 'cognitive impairment', we mean mental functions involved in thinking, planning and understanding not working as well as they should. This can have a variety of causes – see, for instance, the discussion of specifically mild cognitive impairment in Alzheimer's Research UK (n.d.), *Mild cognitive impairment* [Online]. Retrieved from https://www.alzheimersresearchuk.org/dementia-information/types-of-dementia/mild-cognitive-impairment. Note however that this discussion refers only to mild cognitive impairment, whereas we refer also to more severe cases in our point above.

It should be acknowledged that consumer advocacy organisations do sometimes play a similar role for individuals who do not have a trusted individual of this kind, but this is not appropriate in all cases. For instance, it may be a useful measure when a consumer is accessing a financial product, but may not be considered worthwhile in the case of small services. In any case, relying upon organisations to provide this service as a backstop may generate wider issues, so the involvement of this service would require careful consideration. The key implication for scheme design is again that, whilst the above principle addresses many cases of low digital and financial literacy, it cannot be assumed to address all cases.

As such, it remains important to take measures to increase the digital and financial education of those identifiable as ‘vulnerable’ in order to empower them to better make these judgements themselves. The previous section on ‘consumer vulnerability’ discussed how this latter strategy has been attempted in Singapore - attempting to upskill and thereby empower such consumers through training schemes and distributing access to digital devices for low-income households as a ‘wrap around’ to launching Smart Data schemes[41]. Whilst this is likely to be a relatively expensive measure, it may be the only way to enable those vulnerable consumers with low levels of financial and digital literacy and no trusted contacts who can help them to make judgements about the trustworthiness of schemes, and thereby incline them to participate where there are benefits for them. Again, this is too broad a measure to be considered a principle of scheme design, but it is an important step for inclusivity that should be considered alongside any future schemes.

Having considered the contextual factors that make vulnerable consumers less likely to trust requests to share their data *in general*, attention can now be turned to how the particular elements of Smart Data schemes themselves might lead to distrust amongst vulnerable consumers and how schemes can be designed to overcome this.

Specific elements of Smart Data schemes that could drive distrust

1. Limited public awareness and understanding of Smart Data schemes

The relatively poor public understanding of what Smart Data is, and what its applications are, drives distrust in schemes. Whilst this is likely to be a driver of distrust in schemes amongst consumers in general, the ways in which this distrust might be overcome differ for certain types of vulnerable consumer, and so specific design features are required to ensure inclusion.

Those with low digital literacy or limited access to digital devices are less likely to encounter Smart Data schemes and associated applications online, so other avenues of contact may be required in order to make them aware of Smart Data schemes initially, and thereby enable their participation. These offline points of first awareness must be chosen carefully; a stakeholder with expertise on the specific needs of elderly vulnerable consumers stressed the need to consider the points of consumers’ first awareness of Smart Data schemes in general and how these impact upon trust.

The need to use non-digital, community-based channels of advertising was emphasised, as was the need to have this public information campaign be visible to these consumers in advance of anyone directly contacting them to invite them to participate in a scheme or share their data for a particular use case. Direct contact without this prior step was regarded as being likely to be dismissed as a scam by many vulnerable consumers.

[41] Leong & Gardner, op. cit

> *“Advertise the fact that you're us[ing] Smart Data, and explain what it is, and use community touchpoints like, for instance, charity sector locations, voluntary groups, coffee places. GP surgeries are always quite a good one. Use physical posters rather than using texts or emails. Run a television, radio, and newspaper advertising campaign explaining the advantages in a succinct way as you can, and then at some point in it say, 'Watch out for whatever it is for your opt-in opportunity for this scheme'”.*
>
> **Stakeholder**

These kinds of channels were regarded as being ones that these consumers would be more likely to interact with, and it was also felt that such consumers would be more likely to be receptive to information received via these channels compared to others (such as direct contact). As such, these would be the most effective channels to build basic familiarity with Smart Data and its uses for certain consumers, and thereby be an effective way to start to build trust in schemes in general prior to sign up. Again, research amongst vulnerable consumers is likely to most effective way to establish exactly what the most trusted and widely accessed community touchpoints are amongst these consumers, but the following general principle is nonetheless supported by the research:

✓ **Recommended scheme design principle #3:**

Utilise offline community touchpoints to raise awareness of what Smart Data is, and the benefits of participation in schemes, *before* vulnerable consumers are directly contacted to ask them to participate or opt-in.

Even with this measure taken, however, there will remain a relative lack of familiarity at the point of sign-up for a service concerning the specifics of what data is going to be asked for and how it will be used. Lack of understanding or familiarity here can drive distrust in schemes too, so is important to address. In this context, stakeholders stressed the need for transparency from data holders on how data is used to build trust amongst vulnerable consumers. There is a balance to be struck between this transparency and avoiding overwhelming vulnerable consumers with large amounts of technical detail.

It was suggested that one way to achieve both of these things might be to adopt a ‘consumer centred design’ which reflects how consumers would actually engage with the market, whilst providing the *option* to view more details if consumers would like to do so. Consumers engage with schemes in terms of concrete benefits and risks, rather than thinking primarily about the technical workings of schemes, so information should be presented to them in these terms. These more technical details or ‘back end’ workings of the scheme could be readily available for those wanting to read it, but only upon request – to avoid consumers being greeted with long and unwieldly technical details at the point of sign-up. This level of transparency is regarded as being likely to build trust in schemes without having the negative effect of overwhelming consumers and leading to decision-paralysis.

✓ **Recommended scheme design principle #4:**

Be transparent about what data is held and focus on the tangible benefits and risks to consumers of participating, with detailed explanation about how schemes work from a technical standpoint shown only upon request.

In addition to transparency, ensuring consistency of Smart-Data-specific terminology across different applications and communications was regarded as important for building this familiarity with schemes amongst consumers, and thereby building trust. Stakeholders mentioned that different ways of asking for the same pieces of data across different applications can negatively impact understanding and lead to distrust in schemes. Requiring this consistency of terminology is therefore a straightforward way to respond to this concern. The specific terminology that this ought to apply to will depend on the scheme and industry, and so should be decided within schemes or industries.

However, stakeholders were less in favour of requiring consistency of look, feel and format of the core functions of scheme applications, expressing concern that a templated approach to format or interface has the potential to limit innovation and prevent core functions from ever being advanced or improved upon. Relatedly, it was felt that a lack of opportunity to innovate processes may limit the appeal for potential new entrants to actually enter the market, as there would be less scope to differentiate themselves from competitors by offering a superior user experience. As such, this stronger suggestion should be avoided, and the following principle is supported by the research:

✓ **Recommended scheme design principle #5:**

Publish guidelines on common terms to be used in Smart Data applications, to ensure that the same terms are used within and across industries.

2. Lack of familiarity with firms in the market

Whilst transparency and clarity are important to drive understanding of and thereby trust in schemes, it is also important to promote these in a way that does not put too undue pressure on vulnerable consumers to determine whether participating in a particular instance of data sharing is in their best interests. Being transparent about risks and benefits is not enough to ensure that anything suggested to vulnerable consumers is appropriate for them, and demonstrating to vulnerable consumers that the necessary safeguards are in place to protect them from being taken advantage of (or inadvertently harmed) by firms in the market is an essential step for creating trust.

This need for visible safeguarding and protection is particularly strong given another feature of Smart Data schemes that drives distrust – schemes typically encourage a number of new entrants to the market, application providers with whom consumers are not likely to have prior familiarity. Given Chan et al. (2022)'s suggestion that recognisable brand names are important in the adoption of schemes[42], steps must clearly be taken to assure vulnerable consumers that these unknown firms in the market can be relied upon to not take advantage of them (or inadvertently cause them harm through, for instance, lack of due diligence), if trust is to be built in schemes.

Our suggestion here is one made by the OBIE: introducing a 'trustmark', which would suggest to consumers that a firm participating in a scheme is 'legitimate' and trustworthy. When tested with consumers, the mark led to a 50% uplift in likelihood to adopt Open Banking services (tested in the UK) [43], though it is important to note these observations were not specific to vulnerable customers. The reception to this idea among stakeholders was generally positive, though with two concerns that ought to be addressed.

[42] Chan et al., op. cit. Review of Australian Open Banking Schemes.

[43] Reynolds, F. & Chidley, M., 2018. *Consumer Priorities for Open Banking*, [Online]. Retrieved from https://www.openbanking.org.uk/wp-content/uploads/2021/04/Consumer-Priorities-for-Open-Banking-report-June-2019.pdf. Review of UK Open Banking Schemes.

The first concern related to the question of who should decide which organisations are trustworthy, and whether that body they can be relied upon to only award accreditation to genuinely trustworthy firms. Examples of accreditation being afforded too readily to firms were cited in other contexts, and this is clearly something that must be taken seriously if a trustmark is to function as intended. Vulnerable consumers must believe that the necessary due diligence and background checks have been completed on accredited firms if trustmarks are to actually build trust. Transparency about the criteria used for accreditation would go some way towards ensuring this, as would clear and public consequences and redress where harms are experienced by consumers, to demonstrate that they will be protected if and when things do go wrong. One stakeholder even suggested that, where there any cases of things going wrong, regulators should deliberately make these cases high profile in order to demonstrate to consumers and to the market that any such firms will be fined and that consumers will be appropriately compensated.

A second, related concern was raised that consumers would be unfamiliar with any new body or institution formed to accredit firms, and so they would not particularly inclined to 'trust its trustmark'. Both of these concerns strengthen the case for any such trustmark being managed by an *existing* body or bodies, with whom consumers are already familiar with and trust, rather than a brand new body. Existing industry regulators were the main suggestion from stakeholders, but this would require further consideration and research. There are also some industries which do not have an industry regulator, which went undiscussed in our workshop and interviews. That being the case, the following measure is supported by the research:

✓ **Recommended scheme design principle #6:**

Consider establishing scheme-specific 'trustmarks', to be awarded to firms by a trusted body in the industry with whom vulnerable consumers have prior familiarity. Make the criteria for accreditation publicly accessible.

3. *Lack of visible Smart Data regulatory presence*

Strong and visible regulation is another important measure for assuring vulnerable consumers that the necessary safeguards are in place to protect them from potential harms. The lack of an overarching Smart Data regulator was mentioned by stakeholders as something that could drive distrust, but there was not unanimous for support for setting up such a body. It was agreed that strong regulatory presence was needed across schemes, but some felt that existing industry regulators are better placed to do this, on account of both their knowledge and the trust they already have amongst consumers:

> *"What the [Smart Data] legislation will empower the Secretary of State to do is to appoint some sort of overseer for each Smart Data scheme. Our industry is regulated by Ofcom and …the nature of our industry, it's very complex, it's to do with individual prices and packages that are offered, so it would probably need to have to have remained that institution [overseeing the Smart Data scheme within that industry'. And I don't know in [energy], Ofgem would have to be involved at some level. You wouldn't want a third stakeholder necessarily emerging".*

Stakeholder

As such, the key insight from the research on this point is the more general one that it is important to have a strong and visible regulatory presence within each scheme to ensure that vulnerable consumers trust that they are protected.

4. *Concern about privacy and security*

Another major driver of distrust in Smart Data schemes amongst vulnerable consumers is the fear that sharing their data will leave them exposed to fraud and scams. Elderly consumers and those prone to impulsive behaviour in particular were identified as being vulnerable to and fearful of their data from schemes being used for this purpose.

> *"There's a real fear about scams which is making its way into the older population at an increasing rate, and anything where there are links, anything where there's handing over information, you're going to face a real barrier to a lot of older people engaging with that. And in many cases rightly so because they're being much more cautious".*

Stakeholder

As discussed in the previous section, data sharing comes with a number of risks which the development of Smart Data schemes should be sensitive to. On the other hand, efforts to increase the security of digital platforms may also inadvertently exclude vulnerable consumers. For example, while two-factor authentication enhances the security and resilience of a system, it can sometimes require users to have two devices instead of one, which may exclude low-income households or those experiencing digital poverty [44]. The mechanisms for ensuring privacy and security therefore need to be carefully considered.

Discussion in this area focussed on how to assure consumers that schemes are secure, rather than the actual privacy and security mechanisms that applications ought to use. The previously discussed points about terminology to be avoided, and clear and public redress where there are cases of things going wrong were the main suggestions here. Further discussion of appropriate redress mechanisms are to be found in the 'support and redress' discussion later in this section.

It is important again to think in terms of 'consumer centred design' when thinking about responding to vulnerable consumers' fears about privacy and security. One stakeholder made the point that consumers think about an application or service's level of privacy and security relative to other interfaces they interact with. So, for instance, positioning security measures in terms of how they compare to the measures a consumer's bank might use might be a better way to build trust and confidence than a detailed explanation of how those measures work.

> *"Most people are comfortable with having a bank account – there are communities who don't, and you've got to do something more specific with them – but if you can say, 'Your data with us has the same protection as your bank account,' then that'll be enough. It's definitely a huge leap forward".*

Stakeholder

[44] Autorité des Marches Financers Quebec, op. cit

Consent, consent management, and consent revocation

Summary of this subsection: design principles enabling a good consent journey in Smart Data schemes

Giving consent:

7. Include *minimum* standards for consent forms within scheme design, to ensure a concise explanation of which data is to be shared and how long it will be retained for, explained *in terms of* the functionality which it enables.

8. Ensure that vulnerable consumers can access schemes and consent to share their data via preferred offline, non-application-based channels, such as via telephone.

9. Allow for a 'basic' consent option where only the data which is absolutely necessary for a particular function or service is granted.

Managing consent:

10. Consider establishing a cross-scheme Smart Data dashboard which provides consumers with a consolidated view of the data they have consented to share and the purposes for which they have consented to share it. Consumers should then be able to make changes to consent via this central dashboard.

11. Send periodic reminders to consumers through their preferred communication channel to provide them a summary of the data they have consented to share and prompt them to review it and make changes as appropriate.

12. For the most sensitive types of data (e.g., health or finance-related data) that are not critical to the specific service being provided directly to consumers, consider introducing a standard set of 'expiry times' for consent, to be used across schemes. These could be accompanied by prior reminders about the expiry and any impacts, possibly integrated into a cross-scheme dashboard.

Revoking consent:

13. Require a clear explanation of consent revocation processes to be included whenever consent is asked for or reminders to review consent are shared, to make the process as straightforward and low effort as possible.

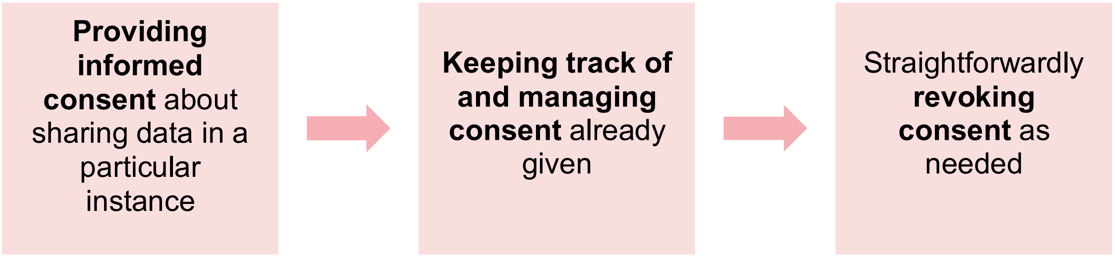
14. Introduce a 'cooling off' or grace period where consumers can withdraw consent without any adverse consequences or commitment to the services with which they shared their data.

Even after vulnerable consumers have been shown that they can trust a Smart Data scheme sufficiently to be open to participating, they will only feel comfortable actually sharing data in a particular situation if they feel that they are in a position to give informed consent regarding that decision. In this context, informed consent means permission granted by someone with clear awareness and understanding of the possible consequences, risks and benefits of the decision.

As with the previous pillar: if vulnerable consumers do not feel comfortable actually using the core functionality of the scheme, they will not benefit from the scheme. In the other direction, if consumers feel comfortable consenting but without sufficient information to fully understand the implications of that consent, they may be exposed to other possible harms (such as excessive personalisation and targeting, which will be covered in more detail in the next subsection).

As such, creating a consent journey that allows vulnerable consumers to readily make *informed* decisions about disclosing data, allows them to manage and keep track of the consent that they have given, and revoke it where necessary, are essential requirements for inclusivity. These three ‘stages’ of the consent journey are shown in Figure 3 below. This subsection discusses design principles that promote inclusivity at each of those three parts of the consent journey in turn.

Figure 3 – the consent journey in Smart Data schemes


Providing informed consent about sharing data in a particular instance
Keeping track of and managing consent already given
Straightforwardly **revoking consent** as needed

Stage 1: Ensuring consumers can give informed consent when they receive data sharing requests

Minimum standards for information included in consent requests

At the initial stage of giving consent, the main goal is to give clarity to consumers about what they are being asked to consent to and why, so that their decision can be an informed one. Similar to ‘trust’, the issues around consent also relate to the power and knowledge imbalance that exists between consumers and Smart Data schemes.

This is a difficult task, as the provision of consent can be a confusing process for vulnerable consumers, particularly those with low numeracy, literacy, and/or digital capabilities. Again, this need for clarity has to be balanced against the need to avoid overwhelming consumers with large amounts of technical information, as this may lead to consumers becoming overwhelmed and therefore cause decision-making paralysis[45], thereby making the consent process more difficult for vulnerable consumers rather than more straightforward as intended.

The most popular design principle among stakeholders in this context was again requiring consistent usage of terminology across applications and schemes, to ensure that vulnerable consumers are not confused by differently worded requests for the same pieces of information across different applications. Since **recommended design principle #5** already covers this, there is no need to provide a separate design principle to achieve this end in the context of consent.

Existing research concerning best practice in this space which may be drawn upon here[46], but participants in the primary research also gave specific recommendations concerning the minimum standards which might be needed. They supported requiring information on the

[45] Autorité des Marches Financers Quebec, op. cit

[46] Behavioural Insights Team, 2019. Terms and Conditions Apply [online] https://www.bi.team/blogs/terms-conditions-apply/ [accessed 29th March 2023]

specific piece of data that is being asked for and why, the immediate outcome of sharing that data, and the extent to which that data will be retained.

Whilst the specific pieces of data to be requested should of course be listed in any such request, it was suggested that they should be explained strictly in terms of why they are necessary for the specific service or function being offered, in order to maximise consumers' understanding (and further reinforce trust in the scheme). One stakeholder suggested that, if the function of the scheme is explained properly at the outset, the specific information requested should not be at all surprising – consumers should know exactly what it is going to be used for *prior* to actually being asked for it.

> *"[The data that is needed and why it is needed should be included in] the articulation of the product anyway. So, how do you make sure that that's part of the description? If you're signing up to something, you need to know that it's going to cost you £250, and that the heat pump is bright pink. So, it's relatively straightforward to say [when articulating the product offering], 'it's bright pink, and it's going to take two weeks to install. The first payment is £250, and if you take a long time to get to the door, please let us know, so our engineer can take that into account'".*

Stakeholder

Being extremely clear about the specific function or service being offered was also identified as an important consideration, as some consumers with lower digital or financial literacy may not appreciate the difference between certain related use cases. One example given was the difference between a comparison tool and an auto-switching tool:

> *"[I remember a situation where] a lot of vulnerable customers thought [a service] was just a price comparison website. So, they put in their information, their details and then within 21 days they'd [had their energy supplier] switched because the agreement was that they would just switch them to the best deal. But it seemed like there was absolutely no understanding that that was what was going to happen. Obviously, it caused a lot of stress. […] I don't know […] if it was just a tiny little thing on the website that said, 'We're going to switch you automatically.' Or if it was just, like, 'Enter your usage and your postcode and we'll just let you know roughly what the deals are' [but this needs to be clear in this context]".*

Stakeholder

One way to think about this is in terms of the immediate outcome of providing consent. It is important to be clear when asking for consent what the immediate result of sharing that data will be, so that vulnerable consumers are in no doubt as to what exactly is being asked.

Some stakeholders also strongly felt that it should be made clear to consumers in all cases whether their information will be retained or not after the service for which it was originally requested has been provided – and if so, how long it will be retained for. For instance, if a consumer's data is collected to provide a comparison between energy tariffs, it should be made completely clear whether this data will be retained after this comparison has been presented to the consumer, or if only the resultant 'recommendations' will be retained, and the original data deleted.

> *“Being really clear whether a company stores your data [is essential]. It might be that they request your data, runs an analysis on it and generate an outcome and then delete the data that was used to generate that outcome. That's quite different to someone actually holding all the information that was used to generate the outcome and then being able to analyse that at a later date or aggregate it so that they're able to develop other products and services where it's not quite your data, but you are still contributing your data to it”.*

Stakeholder

Requiring the inclusion of this information as a minimum standard should be a relatively uncontentious measure for promoting informed consent, as this still leaves considerable scope for application providers to innovate and differentiate themselves from each other in terms of user experience.

However, as mentioned, this must be carefully balanced with the need to avoid overwhelming vulnerable consumers with large amounts of technical information. Therefore, this minimum standard should also include a requirement to ensure wording is kept concise, digestible and non-technical, without being too prescriptive about what providers should include. Stakeholders were keen to stress that anything too lengthy would simply not be read, which would undermine the consent process altogether.

> *“[Suppose] in the consent journey it said [the application provider is] only going to do these five things with it… and [there’s another list of] forty things that they're not going to do with it, [like] sell[ing] it to anyone else, pass[ing] it, us[ing] it for targeted marketing, or us[ing] it in any way that would be to [vulnerable consumers’] detriment. I just think the idea that people are going to read through that and make an informed choice… I just don't think that's realistic”.*

Stakeholder

This balance between clarity, conciseness, and avoiding being too prescriptive is a difficult one to strike. However, it is one that could plausibly be achieved via a ‘consumer centric’ approach similar to the one suggested in the previous subsection regarding information on how schemes work. Providing two levels of explanation would be effective: a short, concise summary which presents this essential information, with access to a more detailed or technical explanation of how the data is going to be used available only if consumers choose to view it. So long as this shorter explanation satisfied the minimum requirements and remained under a maximum length, individual application providers would still have the ability to experiment with different approaches over and above this.

> *“Offer the option for the technical information if they want it but don't give it to them for the start because you'll just overwhelm them. Not very many people will now read, let alone want to read, a six-page technical briefing on what's happening with the data. Most of the time they want a one-pager for everything, and it just needs to be this is what's happening, this is the data we're using, if you want a full list of everything we're using, you can go to this website”.*

Stakeholder

✓ **Recommended scheme design principle #7:**

Include *minimum* standards for consent forms within scheme design, to ensure a concise explanation of which data is to be shared and how long it will be retained for, explained *in terms of* the functionality which it enables.

Changing look, feel and format to promote clarity of consent requests

Providing information in a variety of formats to further enhance clarity for certain vulnerable consumers is a suggestion that is made throughout the literature. Practically, this might involve using pop-up screens, infographics, or videos to help explain what the user is consenting to share, and how it will be used, in a more digestible manner (Autorité des Marches Financers Quebec, 2022; Ofcom, 2020)[47].

Whilst varying the approach is highly likely to improve accessibility compared to a one-size-fits-all approach, the specific look, feel and format which best promote clarity will depend to a large extent on the specific needs and circumstances of the consumer in question. As the next section on 'control and choice architecture' outlines in more detail, the implication for scheme design here is more general: consumers should have the option of viewing information in a variety of formats to suit their needs, but extensive and iterative user testing and experimentation, even once schemes are live, ought to be conducted amongst vulnerable user groups in order to establish the ways in which approach should be tailored for different groups.

> *"[It's important] to actually see in the real world, how the customers respond to different [communications]. […] People don't normally think about this stuff. Like, if you ask someone, 'How would they phrase this to get your consent?', they'd be like, 'Wait, what are you talking about?' I think trialling is a really key thing in this to actually understand the different settings, or into the different typesets of data, what works. I think there just needs to be a level of experimentation".*

Stakeholder

Channels through which consent can be given

Stakeholders also stressed that making the process of giving consent in Smart Data schemes accessible to all requires service providers to offer a variety of channels through which to give consent, rather than only via smartphone applications. Those who have low digital literacy or limited access to digital devices are likely to be excluded from participating fully in schemes if this is the only channel through which data sharing can be consented to. Even for those vulnerable consumers who are able to access an application-based consent form then, difficulties in comprehension could well result if this is the only channel for consent available, thereby limiting the extent to which they are able to give informed consent.

[47] Autorité des Marches Financers Quebec, op. cit; Ofcom, 2020. *Consultation: Open Communications — Enabling people to share data with innovative services,* [Online]. Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0030/199146/consultation-open-communications.pdf

> *"[In Open Banking] we've got a competition remedy that's supposed to be helping everybody, that only works for 80% of the population [since not everyone is online]. I guess the solutions [to provide an offline alternative] are so unpalatable that no-one really wants to think about that you could go into your bank branch and sign up to open banking, but it should be an option for people. There should be a way of doing it that doesn't require you to be online".*

Stakeholder

Directly asking vulnerable consumers options for their communication channel preferences at the point of scheme signup is likely to be the most effective approach here. This would ensure that consumers felt as comfortable as possible, and would also ensure the requirement for people to be able to involve trusted family and friends mentioned in the 'trust' section could be accounted for.

There is no consensus on whether to require application providers to offer multi-channel consent such as via telephone, but stakeholders do flag concerns that if appropriate incentives are not put in place, some application providers may not offer this, and so further research may be needed on this point. As such, the suggested principle does not specify how a multi-channel approach ought to implemented:

✓ **Recommended scheme design principle #8:**

Ensure that vulnerable consumers can access schemes and consent to share their data via preferred offline, non-application-based channels, such as via telephone.

Amount of data included in one consent requested

Another balance to be struck is how much data ought to be asked for in one consent request. As discussed in the previous section, there is concern in the literature that users may be requested to share large amounts of data without a clear idea of what services within a scheme are using it may allow schemes to capture more data than consumers' use of services / the scheme may necessitate [48]. This would amount to uninformed consent, and so should be avoided. Stakeholders expressed support for there being an option to only grant a 'basic' level of consent in a given instance, where only the minimum amount of data shared to operate the service in question is granted – rather than a more sweeping consent to share large amounts of data for multiple use cases at once.

✓ **Recommended scheme design principle #9:**

Allow for a 'basic' consent option where only the data which is absolutely necessary for a particular function or service is granted.

Stage 2: Ensuring consumers can manage consent they have given

Having discussed several design principles for ensuring that the consent journey is inclusive at the point of giving consent, design principles are suggested to ensure that the consent management process allows vulnerable consumers to easily keep track of the data that they have consented to share.

[48] BEIS, 2018, op. cit; CISRO, op. cit

Centralised dashboard for consent management

A widely recommended measure to achieve this amongst stakeholders was a centralised consent dashboard for Smart Data schemes. This would allow consumers a single view of the data that they have shared, provided two key concerns are addressed. First, there is a fear of an excessive number of dashboards across schemes leading to consumers not actually using them. This could be resolved by having a single dashboard for all Smart Data schemes, rather than one per scheme or per industry:

> *"When you start stretching out across the whole Smart Data ecosystem, [there's a concern] that you've got dashboards with BT, with EDF, with Sky, with [your supplier across each of the industries in which schemes operate], you know, no-one's going to look at them. So there is this idea of a [single] dashboard, a central control place. Once you get to Smart Data, I think you need something like that".*

Stakeholder

The second concern expressed in relation to dashboards is that they are not something that many consumers will actually use regularly. However, stakeholders felt that they are limited use is not a major problem, as they remain reassuring for anyone who ever wants to take stock and/or revoke consent. Limited frequency of access is therefore not sufficient reason to advise against this measure, even if they are not sufficient as a sole measure for managing consent.

✓ **Recommended scheme design principle #10:**

Consider establishing a cross-scheme Smart Data dashboard which provides consumers with a consolidated view of the data they have consented to share and the purposes for which they have consented to share it. Consumers should then be able to make changes to consent via this central dashboard.

Reminders of consent that has been given

Stakeholders also suggested that consumers be sent periodic reminders of the consent that they have given. This measure would be a more active prompt for consumers to review and manage their consent. It was also felt that vulnerable consumers would notice and appreciate reminders and so it was slightly preferred to merely setting 'expiry dates' on consent, though of course these measures (and a dashboard) are not mutually exclusive.

This measure would allow those consumers with low digital literacy or limited access to digital devices to manage their consent, so long as these reminders are offered via multiple communication channels rather than solely through apps or online.

✓ **Recommended scheme design principle #11:**

Send periodic reminders to consumers through their preferred communication channel to provide them a summary of the data they have consented to share and prompt them to review it and make changes as appropriate.

Time-limiting consent

However, time-limited consent was still seen as a measure worth taking in addition to reminders, even if it was not seen as quite as important as the other measures proposed here. Moreover, some stakeholders felt it would assure consumers that they would be protected if they faced difficulties with application providers when trying to revoke consent.

> *“I've worked for so long with private companies that I'm just very sceptical that, if you put in a situation where you don't have any backstop at all, you could be in a situation where [you struggle to opt out]. I won't say names, but if someone's with a particular energy supplier or another one, they'd have very different outcomes in terms of whether the supplier made it really easy to opt-out of the data sharing and the other one made it really difficult. So, I think you'd have to have some sort of longer term, sunset clause where it says the data will be removed”.*

Stakeholder

However long this ‘sunset’ clause or backstop is to be, stakeholders supported this length of time being standardised across schemes, as it was felt that this varying by industry could be a barrier to consumers understanding the process. As such, the following design principle is suggested:

✓ **Recommended scheme design principle #12:**

For the most sensitive types of data (e.g., health or finance-related data) that are not critical to the specific service being provided directly to consumers, consider introducing a standard set of ‘expiry times’ for consent, to be used across schemes. These could be accompanied by prior reminders about the expiry and any impacts, possibly integrated into a cross-scheme dashboard.

Stage 3: Ensuring consent is easy to revoke

The final part of the consent journey to consider is revocation. In this context, revoking consent means a consumer withdrawing permission for specific data to be shared with trusted third parties as part of the Smart Data scheme. It does not necessarily mean withdrawing from the scheme altogether.

Stakeholders supported the notion that ‘good’ in this context means the revocation process being simple and low effort. In practice, this involves two elements: firstly, clear signposting of *how* the revocation process works, so that consumers are in no doubt about how to go about this; and secondly, the actual act of revoking being straightforward.

Frequent signposting of consent revocation processes

Requiring that revocation processes are made clear as often as possible would help on the first point. Whenever consent is asked for and whenever reminders to review consent are sent, including a clear explanation of the process to revoke consent would be helpful:

✓ **Recommended scheme design principle #13:**

Require a clear explanation of consent revocation processes to be included whenever consent is asked for or reminders to review consent are shared, to make the process as straightforward and low effort as possible.

Building confidence that data has actually been removed

Stakeholders did not provide conclusive recommendations on how the actual act of revoking can be made as straightforward as possible. That said, it was acknowledged that trust in the follow through of removing data is key in order to re-assure consumers and to further encourage vulnerable consumers to engage in smart data schemes.

> *“There's not enough regulatory oversight to [ensure private companies manage consent revocation properly], so really you need some sort of central body, whether it's the information commissioner or whatever, you can say, 'I signed up to this data [being shared], I want that data removed now and to reset.' Then that would take off a lot of the pressure. Again, you will still have people who will be a year, 2 years down the line, won't remember that was the case or won't be aware of it and then I would suggest you have to continue flagging it at some point in the press each year to say, 'last year we ran this campaign. We hope that you're enjoying it and that it works well for you, but if you're not, there is still an option to contact the ICO or whoever to have your consent withdrawn'”.*

Stakeholder

‘Cooling off’ periods for consent

One final consideration relating to revocation is a ‘cooling off’ or grace period, where consumers can revoke consent without consequence. This was a relatively popular measure among stakeholders.

> *“I like cooling off periods. You know, you sign up for this, we'll send you some details, have a think about it, if you change your mind in 24 hours we'll delete everything and it'll all go back to exactly how it was.”*

Stakeholder

This measure has a number of benefits, including protecting consumers more prone to impulsive actions from the harms of sharing data where it does not benefit them, and provide further reassurance to consumers more generally. However, the specifics of implementing this measure need to be further defined, as there was no clear consensus on the length of this cooling off period, and whether it should apply only to the act of data sharing, or any services signed up for. For example, revoking consent for a price comparison or account management tool might be fairly straightforward, but the matter is less straightforward if the context of the data sharing is an auto-switching application, and the consumer has already been switched as a result of consenting. For now, the more general principle that a cooling off period of some kind should be implemented is suggested:

Recommended scheme design principle #14:

Introduce a ‘cooling off’ or grace period where consumers can withdraw consent without any adverse consequences or commitment to the services with which they shared their data.

Choice architecture and consumer control

Summary of this subsection: design principles enabling good consumer control and choice architecture in Smart Data schemes

15. Make decisions as clear and unbiased as possible, enabling consumers to make educated and uninfluenced decisions in their own favour.

16. Better deals or preferential prices should not be based on the amount of data a consumer is willing to share, and consumers who are less engaged in schemes should not pay more for the same products and services as those who are using schemes more extensively and regularly.

17. If personal data is retained and aggregated (with consumers' permission) to inform the development and marketing of specific products, there should be clear guidelines on what is considered fair targeting and pricing to avoid vulnerable consumers being offered inappropriate products, that they still have the choice of a range of products to meet their needs and/or that they do not pay a premium for the same services compared to non-vulnerable consumers.

18. How easy or difficult transactions are within schemes (the level of 'friction' attached to them) should be risk-based. When high risk decisions are being made it is important that risks are clearly communicated and that cooling off periods or buffers are built into application design.

19. Ensure that design throughout applications allows trusted family, friends or other advisors to help vulnerable consumers, but also that this be implemented in a way that does not require consumers to give that advisor full control.

This subsection considers the design features and architecture necessary to support and protect vulnerable consumers once they are already using Smart Data applications. Control and choice architecture refers to how an application guides a user to navigate, use, and prioritise its services and functions. This section explores design principles that promote utility for vulnerable consumers and cautions against architectures that may lead them to act against their own interests.

Preventing choice architecture from biasing consumers towards decisions

One of the biggest and overarching concerns in this area is the ability of applications to target and benefit from vulnerable consumers' lack of understanding, their behaviors or their characteristics/circumstances. Targeting refers to the practice of tailoring the app's features and content to specific user demographics or characteristics and indeed, all consumers are susceptible to certain behavioral biases. The Competition and Markets Authority explains that 'We are also strongly influenced by context, including sometimes superfluous or misleading information like 'recommended' prices or inferior products added to a choice set'[49], which demonstrates the significance, and the potential impact targeting can have on all consumers.

However, the concern is that vulnerable consumers, as discussed in the previous section, may be at risk of higher levels of manipulation, with applications potentially able to manipulate

[49] Competition and Markets Authority, 2022. Online Choice Architecture How digital design can harm competition and consumers. [Online]. Retrieved from https://www.gov.uk/government/publications/online-choice-architecture-how-digital-design-can-harm-competition-and-consumers

them based upon their mood, personality, stress levels, and other factors relating to their circumstances[50]. Additionally, harm caused by targeting can 'disproportionately affect vulnerable consumers, for example, because they: i) are less able to bounce back from a financial loss or negative feelings; ii) may not be sufficiently confident to complain, return items or access compensation; and iii) may be less able to learn from, and avoid, the same experience in future'[51]. For example, a vulnerable consumer with low financial literacy might be drawn into an energy deal with a low first-month cost, without realising that monthly costs will increase significantly thereafter. Applications that push such deals towards consumers whilst aware of their financial situation, could be seen to actively encouraging them to act against their own interest.

> *"You want a comparison website or a third-party provider to be able to provide a vulnerable customer with the packages designed for them, but at the same time, we wouldn't want to allow either that platform or those providers to then, well, you'd not want it to be a negative targeting, and excluding".*

Stakeholder

Stakeholders agreed that applications should not unduly target consumers and that such behaviour is bad practice and should be avoided. However, it was felt that there is limited scope to enforce such ethics onto businesses and app designers. Transparency was viewed as one way to help ensure applications are correctly and fairly using customer data. However, applications must also build in time and scope for consumers to think critically about the information or decisions presented to them – transparency alone does not amount to good choice architecture. Control and choice architecture design principles in turn, and as will become evident, should aim to empower consumers to advocate for their own interests.

One way to empower consumers is through enhancing clarity and presenting decisions in an unbiased manner, as when information is not clearly displayed, or presented in a biased way, consumers may be pressured into making decisions that do not benefit them[52].

Clear and factual communication about products or services can lead to more informed decision making by consumers. When consumers have a better understanding of the benefits and drawbacks of a product or service, they are more likely to make choices that align with their interests and needs. Additionally, prescriptive communication about the benefits of a product or service can help prevent disappointment and potentially encourage greater uptake.

> *"It's that terminology and language can't be stressed enough about, you know, using this in plain English, plain maths as well where that's relevant, but simple words that customers understand."*

Stakeholder

Additionally, an issue that arises when information is presented in a biased way or is presented in such a way as to cause "choice shaming" is that consumers may make uneducated or pressured decisions that do not benefit them. "Choice shaming" is a

[50] Consumer Policy Research Centre, 2020. *Unfair trading practices in digital markets - evidence and regulatory gaps,* [Online]. Retrieved from https://cprc.org.au/wp-content/uploads/2021/11/Unfair-Trading-Practices-in-Digital-Markets.pdf

[51] Competition and Markets Authority, op. cit

[52] The concept of 'choice shaming' also emerged within stakeholder discussions of this issue. This is when the choice an application wants or is encouraging a consumer to make, is presented in such a way as to make the other option seem inferior in comparison.

phenomenon where companies present the choice they want consumers to make as the only or best option and the alternative choice as inferior or undesirable.

> *"Choice shaming [is] the idea that the choice that the company wants you to make is proposed as this[…] excellent and almost inevitable choice, and the choice to the contrary is seen as this negative thing, 'Oh, I don't want great targeted adverts."*

Stakeholder

For example, a company might suggest that consumers should purchase a more expensive product because it's "better" than the cheaper alternative, even though it may not be suitable for their needs or budget. "Choice shaming" can be especially problematic for vulnerable consumers who may be more likely to trust the recommendations of the company or feel pressure to conform to social norms.

✓ **Recommended scheme design principle #15:**

Make decisions as clear and unbiased as possible, enabling consumers to make educated and uninfluenced decisions in their own favour.

Ensuring consumers are not penalised for withholding data

Another concern for choice architecture is that those consumers who opt not to share their data will be penalised, or that decisions are presented to consumers in terms that make this seem to be the case. If there is a large disparity in the quality of choices presented to consumers, and the best options are ones which are dependent on whether a user shares extensive data, this might be seen to bias consumers towards a particular decision. Stakeholders referred to this concept as a 'privacy premium':

> *"There could be a privacy premium. It's a really difficult one. There are already lenders who will offer you a lower rate if you share your data. They'll literally say, 'You know, we'll take 1% off the APR if you share your data.' I mean, it's really […] early but [there is a] privacy premium."*

Stakeholder

This is an issue, as a privacy premium has the potential to exclude vulnerable consumers who are reluctant to share data. Furthermore, a cautious attitude towards data sharing is arguably a positive. This premium could ultimately lead to many vulnerable consumers missing out, despite them acting in a way that digital safety guidance would possibly recommend.

In the other direction, a privacy premium could lead some vulnerable consumers to share large amounts of personal information even if it is not in their best interests, in order to access what is positioned as a better deal. Encouraging excessive data sharing complicates the decision process for those who struggle to know who and what to share with organisations. Vulnerable consumers who feel pressured into taking actions may be opened up to increased risks, so this premium is to be avoided. For example, for those who are financially vulnerable or have low financial resilience, such a premium could make their situation worse.

Recommended scheme design principle #16 and #17:

Better deals or preferential prices should not be based on the amount of data a consumer is willing to share, and consumers who are less engaged in schemes should not pay more for the same products and services as those who are using schemes more extensively and regularly.

If personal data is retained and aggregated (with consumers' permission) to inform the development and marketing of specific products, there should be clear guidelines on what is considered fair targeting and pricing to avoid vulnerable consumers being offered inappropriate products, that they still have the choice of a range of products to meet their needs and/or that they do not pay a premium for the same services compared to non-vulnerable consumers.

Ensuring appropriate levels of 'friction'

Friction is a key aspect of app design. In experience design, friction means the ease with which a consumer can accomplish a particular goal using an application. In this context, there should be an appropriate level of friction when a consumer is asked to share personal data and/or engage with a particular use case within a scheme.

Often designers focus on how to minimise friction, to allow consumers to smoothly pass through an app and to access their desired service with ease. However, friction also plays an important role in creating space for questioning and for emphasising the importance and significance of a decision. One area where friction is being positively used is within gaming:

> *"Gaming has introduced some [friction…. So] if you do a new transfer on your bank it pops up and says, 'Are you sure you want to do this transfer?' On gaming they've actually slowed it down so that [there is] buffering. They build in buffering and things like that to make it take longer, [….] and it's not just an egg timer or a thing that's on the screen, it's giving [you] thinking time, are you sure you want to do this?"*

Stakeholder

Given that Smart Data schemes look to take the effort out of data sharing, it may seem counterintuitive to build friction back in. However, ensuring that decisions are presented to consumers in a way that makes them seem easy and manageable, in instances where these decisions can be quite consequential is a situation that must be avoided. That being said, app providers should be considerate as to when and how they implement friction, as while friction can be beneficial in certain situations, it is not always necessary nor desirable for every decision-making process. Therefore and as suggested by stakeholder during the research, the amount of friction integrated into an application should be dependent on the risks involved with each action.

Applications may be naturally inclined to push users towards the next purchase, further data sharing, or service expansion. Therefore, building in "thinking time" can be highly beneficial for consumers. By allowing for adequate reflection time before a decision can be made, consumers can make informed decisions that align with their needs and values, rather than being influenced solely by the application's goals. These opportunities for users to pause and consider their options can also help to promote transparency and trust, which in turn creates a more positive user experience.

For instance, the action to take out a loan which is to be automatically repaid from a consumer's bank account (much like the example given in the previous section), might be regarded as a high-risk action, as it is one that has financial consequences that have the potential to lead to harm for certain vulnerable consumers, if it is not an appropriate action for them to take. For instance, those with a history of impulsive behaviour and low financial resilience could be harmed by this action being too easy to take, as they may then be committed to automatic repayments which they cannot afford. As such, this action is one where a risk-based approach would determine that a high level of friction should be required in app design – the risks of harms arising from low friction are relatively high, so it follows that the friction built into the app should be high for this action. Conversely, an action which has no potential to lead to harms for vulnerable consumers should be one where there is as little friction as possible.

It is important to strike a balance between minimising friction and ensuring that adequate safeguards are in place to protect consumers' interests. By adopting a risk-based approach to friction, designers can tailor their application's user experience to specific scenarios and users, reducing unnecessary barriers while maintaining a level of security and privacy that aligns with the associated risks.

> *"The amount of friction should be risk-based – I think friction is good where there's risk. So, it's about framing the user experience around the risk that's attached to it."*

Stakeholder

Recommended scheme design principle #18:

How easy or difficult transactions are within schemes (the level of 'friction' attached to them) should be risk-based. When high risk decisions are being made it is important that risks are clearly communicated and that cooling off periods or buffers are built into application design.

Involving a trusted advisor throughout whilst still retaining ultimate control over the process

As has been discussed in the previous subsections, allowing vulnerable consumers to easily involve a trusted family member or friend is an important measure to take to ensure the inclusivity of schemes. There are some further measures over and above what has already been discussed in the context of trust and consent that are needed in order to promote consumer control here.

One measure is allowing trusted parties to have visibility of decisions made without the consumer having to give away control of the decision making process. Leong and Gardner (2021) cite Toucan as an application where trusted advisors were involved in such a way; the application allows users to safely nominate a trusted party to receive alerts and assist them to avoid compulsive overspending, without the need for giving away full control to a Power of Attorney[53], thus allowing the consumer to receive support and assistant without giving up control of the process or fully delegating it to another party. This concept of selecting a trusted third party is especially pertinent for individuals with mental health problems or low financial capability who may rely on family and friends for assistance with financial decision-making.

[53] Leong & Gardner, op. cit

Moreover, there are several other vulnerable groups who could benefit from such a mechanism, such as elderly individuals who may be struggling with dementia and require a trusted person to review and have access to their account. Similarly, those first language is not the native one may find it challenging to fully comprehend the information presented to them. In such cases, the ability to nominate a relative or another trusted individual who is proficient in the language could be useful.

> *"I'd say cognitive impairment and dementia – that's probably where you're talking about [needing] a third-party nominee".*

Stakeholder

While a large number of stakeholders saw utility in nominating a trusted party, some risks were also mentioned, as was discussed in previous subsections. Namely, this approach requires a vulnerable consumer to have an individual within their support network who they could nominate. It also relies on the third party being trustworthy.

> *"[It is questionable to what extent we can] trust a third party being able to monitor as well, to make sure that what you're sharing is in your [interest]".*

Stakeholder

This strengthens the need to ensure that trusted parties can be involved in a manner that still allows the vulnerable consumer to retain as much control as possible over the process:

✓ **Recommended scheme design principle #19:**

Ensure that design throughout applications allows trusted family, friends or other advisors to help vulnerable consumers, but also that this be implemented in a way that does not require consumers to give that advisor full control.

Support and redress

Summary of this subsection: design principles enabling good consumer control and choice architecture in Smart Data schemes

20. Wider, wrap-around support and troubleshooting should be delivered by a consistent and clear point of contact (e.g., the data holder), and be accessible through multiple formats - including offline communication channels.

21. Create a system for redress, ideally by widening an existing regulators scope to include Smart Data schemes, as these institutions are often already familiar to consumers.

As mentioned in the section overview, support refers to assistance and guidance that can be provided to consumers in a Smart Data scheme, to help them understand and manage their data, whereas redress refers to the process of addressing and resolving complaints or issues that consumers may have with how their data is being handled or used.

Existing literature does not discuss the importance of support and redress in great detail, though stakeholders were quick to argue that support and redress should play a key role in Smart Data scheme design. Providing visible opportunities for support and redress has many benefits, including supporting the pillars or desired outcomes already identified: trust, consent and control. However, stakeholders regarded support and redress as important enough to be considered a pillar or desirable outcome in its own right:

> *"Support and redress, I think, [ought to be] a fourth pillar. Again, it's for everybody, but I think the idea that this is part of a broader thing that you can complain to [which has] always got your back. You're not just out in the wilderness sharing your data with God knows who".*
>
> **Stakeholder**

Ensuring that consumers can easily access support mechanisms

When it comes to support, it is crucial that this is easily accessible within applications. This not only means that opportunities for support needs to be available and clearly advertised, but also that the forms this support takes are accessible and has many forms. As discussed within previous subsections, allowing for offline forms of contact is beneficial to vulnerable consumers and so should be prioritised when designing support mechanisms.

> *"It does need to be easy. I mean I find it incredibly frustrating with everything that I do online. If I want to speak to a human, you can't find a number, you can't find a link because they don't want you to ring them. So that does need to be made-, and also, once I've got to the point of exacerbation, when I can't do it anymore online, you can tell how old I am by saying this, I'm going to have to speak to a bot and that makes me even more mad. Or, speak to some voice recognition thing that doesn't understand what I'm saying."*
>
> **Stakeholder**

✓ **Recommended scheme design principle #20:**

Wider, wrap-around support and troubleshooting should be delivered by a consistent and clear point of contact (e.g., the data holder), and be accessible through multiple formats - including offline communication channels.

Ensuring that consumers feel confident they will receive redress where appropriate

Redress is a slightly more complicated matter than support, in that it requires an institution to oversee and enforce the process. This may be a newly established overarching Smart Data regulator, or existing industries regulators, or ombudsman.

Whatever mechanism is used, stakeholders emphasised the strong importance of visible and clear systems for redress when consumers face issues or experience harm due to something going wrong.

Creating clear procedures and opportunities for redress is essential because it ensures that consumers see those managing their data as having a responsibility to act in their favour, since they will be held accountable if they fail to do so. This in turn helps to improve trust and confidence in schemes, as by providing consumers with a support network and a clear path to redress, they are more likely to trust the data holder or app provider and feel confident that their concerns will be addressed.

Similarly, when it comes to consent, a key worry of vulnerable consumers is how they will or if they can remove consent for their data to be used. Making the routes for redress clear, should they experience any issues which are not their fault, ensures that consumers feel like they are being safeguarded from harms and increases their confidence and likelihood to use a scheme. Therefore, it is very important that clear and visible redress is built into Smart Data schemes for reassuring vulnerable consumers that they are adequately protected when participating in these schemes.

Stakeholders felt that an important part of this was having clarity regarding liability and the party which is responsible for enforcing the redress system. The literature notes that, at present, "determining ultimate liability in fraudulent or erroneous transactions may be challenging, [as…] national liability frameworks are not adjusted to account for Open Banking and data sharing between multiple parties"[54] . In that context, developing a clear Smart-Data-specific framework for liability and making it clear which body or bodies are responsible for ensuring that liable parties promptly compensate consumers where appropriate would provide welcome reassurance that there will be resolution when things go wrong.

As was the case in the previous discussion about trustmarks, the body or bodies responsible for overseeing this system should ideally be one(s) with which consumers are already familiar and trust. Therefore, it would be more effective to use existing bodies, such as individual industry regulators, who have established reputations and a track record of working to protect and promote the needs of the consumer. By giving responsibility for ensuring redress frameworks are followed to recognised bodies, scheme design will ensure consumers have greater confidence in the redress process and feel more protected when using Smart Data schemes.

[54] Basel Committee on Banking Supervision, 2019. *Report on Open Banking and application programming interfaces*. [Online]. Retrieved from https://www.bis.org/bcbs/publ/d486.pdf. Review of international Open Banking Schemes, including the UK.

Recommended scheme design principle #21:

Create a system for redress, ideally by widening existing regulators’ scope to include Smart Data schemes, as these institutions are often already familiar to consumers.

Conclusions and future considerations

There is significant opportunity for Smart Data schemes to make day-to-day transactions simpler and more efficient, ultimately benefiting consumers through time and money saved. Moreover, Smart Data schemes could enable better targeting of support to those eligible, something which is particularly important in the context of the current rise in the cost of living. However, as shown by this research, without careful design Smart Data schemes risk excluding those with vulnerable characteristics, or even cause further harm. Each of the principles suggested aims to mitigate a specific risk or harm posed by Smart Data, but it should be noted that none have been directly tested with vulnerable consumers. Principles relating to user experience design – particularly the consent journey, consent dashboards, trustmarks and support services – would benefit from further research to validate that they deliver on the needs of vulnerable consumers and do not have unintended consequences.

Alongside the principles developed through this research, there are four overarching considerations for inclusive Smart Data scheme in the future:

1. **Inclusive design is best achieved through principles which address specific needs or outcomes, rather than ones targeted at specific types of vulnerability. Making outcomes such as trust and control the focus could streamline the design process and deliver better outcomes than creating principles which are specific to each type of vulnerability.** Vulnerability is complex. Within each of the four main categories of vulnerability identified by the FCA, the interplay between the numerous sub-characteristics is unique for each consumer. Vulnerability is also changeable, and a consumer can move in and out of being classified as having vulnerable characteristics over their lifetime. Finally, there is often shame around self-identifying as having vulnerable characteristics and collecting this information can feel intrusive. This research has shown that, whilst it is important to have an appreciation for how specific vulnerable characteristics interact with Smart Data, focusing on a set of specific needs can streamline the design process whilst also ensuring schemes are accessible to a wide range of different vulnerabilities. However, not all needs can be satisfied through inclusive digital design, and the rollout of Smart Data schemes is likely to require investment in offline channels (telephone and face-to-face) to provide alternative avenues for consumers to engage with schemes.

2. **Schemes should be based on a fair and transparent exchange of personal data for services, and each use case should clearly demonstrate the tangible benefit it provides to consumers.** Consumers' personal data holds significant value to them and the firm holding that data, yet a common theme throughout this research has been that the benefits of sharing this data is often poorly articulated and understood. Going forwards, schemes should move beyond headline engagement and place more emphasis on understanding, monitoring and improving the specific outcomes said to be delivered by Smart Data schemes. Given the value a consumer's personal data holds, ensuring consumers should retain overall control over their data at all times. This should be reflected in consent and revocation processes, as well in limiting scope for consumers to be unknowingly influenced or restricted in decision-making because of the data they have shared. To support this, the regulatory framework should require a regular audit of how data is collected, used, and destroyed.

3. **The regulatory framework for Smart Data schemes needs to strike a balance between standardisation and innovation.** Behind many of the principles discussed in the report lies a need to make the language and interfaces of Smart Data schemes simple and consistent as familiarity is particularly important for giving vulnerable consumers the confidence to engage. However, stakeholders acknowledged that

over-standardisation of aspects such as the consent journey or choice architecture could impact innovation, and lead to a mismatch between the level of risk of a use case and the controls in place. Instead, the regulatory framework should clearly articulate certain *minimum standards* for data holders and app providers in terms of the language they use, the information they provide to consumers about risks and benefits, and how long data is held for.

4. **Who is accountable when things go wrong needs to remain clear and consistent even as the landscape becomes more complex.** Amid the exchange of information between data holders and app providers to deliver Smart Data use cases, it is vital for inclusion that it remains clear which party has overall accountability for remedying issues. This is especially important given that Smart Data schemes will facilitate the entry of many new and lesser-known firms into the market, making the landscape more complex to navigate. This accountability needs to be underwritten with a strong regulatory presence for each scheme through new powers of existing industry regulators. This is preferable to establishing a new regulator because of their institutional knowledge and the trust they already have amongst consumers.

However, despite all of the above considerations being meaningful findings they should be considered in light of the limitations mentioned in earlier sections. To reiterate those limitations are:

- The qualitative nature of the research mean that the study involved a limited number of participants, which could mean that not all opinions have been adequately represented.

- No vulnerable consumers were included in the study, and we did not conduct any user testing. As a result, the conclusions are based solely on the experiences and viewpoints of experts, rather than on the actual usage of a particular processes.

- It is also important to note that certain scheme-specific considerations may not be evident in these generalised discussions and they must be accounted for.

- There was a notably smaller proportion of experts from advocacy groups and so the views and knowledge of those who work closely with vulnerable consumers are limited in comparison to other experts.

- Due to the tight timing of the research project, the extent and thoroughness of the literature review and qualitative research were restricted.

It is worth noting that these limitations should not undermine the value of this research, but rather should be taken into account when considering their relevance within sectors or specific application design. As with any research, the findings presented should not be considered exhaustive or universally applicable.

Appendices

Appendix A – Literature review

The research began with a review of existing literature to identify existing evidence for designing inclusive Smart Data schemes and digital policies, and therefore inform the design of the workshop and in-depth interviews with scheme stakeholders.

The literature was searched broadly using Google Scholar. The following search terms were agreed with the Department of Business and Trade based on previous research in the area, and were used in appropriate and varied combinations: “API”, “digital design”, “Consumer Data Right”, “CBDC”, “harm”, “low digital skills”, “low digital literacy”, “low income”, “Midata”, “Open Banking”, “Open Communications”, “Open Energy”, “Open Finance”, “poor health”, “Smart Data”, “vulnerability”, “vulnerable consumers”, “WeChat Pay”. In addition to these search terms, some sources were added based on their inclusion in the bibliographies of other free-found sources.

We identified and listed all relevant literature in an excel framework with key information such as:

- Author
- Title
- Publication date
- Methodology
- Source quality (recency, robustness, representativeness, bias and relevance)
- A brief summary of the abstract and potential relevance to the study

The initial search for literature identified 43 sources. Given the time available for this phase of the project, it was deemed possible to select 20 of the sources deemed most relevant to the study to be reviewed in detail and thematically analysed.

Below is a table providing more detail on the design features identified by the sources. For details of the 20 sources that were reviewed in depth, please see the bibliography where these sources are marked with an *).

The table is organised in descending order of the frequency of mentions, although it is worth noting that none of the design features received a particularly high number of mentions. This is because many sources in the review focused on highlighting 'issues' rather than proposing solutions. Therefore, the design features identified served as prompts for discussion during the workshop/interviews, rather than an exhaustive list.

Design feature	Number of sources which mention
Designing against predatory algorithms and targeting	4
Trusted third party	2
Building in friction	2
Promotion of an application through a recognised organisation, group or charity	2
Clear and simple presentation of information	2
Intuitive self-guided design	1
Trust mark	1
Implementing a regulator	1

Appendix B – Stakeholder workshop / interview discussion guide

The following discussion guide was developed in collaboration between researchers from Savanta, and the Smart Data team in the Department for Business and Trade and was used to guide discussions in focus groups.

The focus groups were comprised of senior stakeholders from a wide variety of sectors: telecoms, utilities (water and electricity), banking, finance and charitable organisations. There was also a mixture of firms who hold customer information, app providers, and advocacy groups in attendance. The groups were designed to spread industry knowledge and stakeholder types (data holder, app providers etc) evenly across the groups, to prevent a concentration of one type of stakeholder in any single group and to encourage diversity and rich discussion within individual focus groups.

Timings	Questions
10 mins	Hi everyone, welcome and thank you again on behalf of the Department for Business and Trade for attending today. We are excited to have you here and hope we can work together to create some design principles to ensure that future Smart Data schemes are inclusive of vulnerable consumers. As mentioned in the introductory presentation, our group will be focusing on **developing inclusive Smart Data schemes.** My name is _________, this is my colleague _________. We'll also be joined today by some of our colleagues from DBT who have come to listen to what you have to say first-hand. Few bits of housekeeping before we begin: • We will be working in our small groups for about an **hour and a half**, so will aim to wrap up for a break / refreshments around 11:45am. • You're welcome to leave the room at any point to go to the bathroom, get refreshments etc. but please try to avoid doing so at the same time as someone else. • Bathrooms can be found on this floor near the _________ We'll be **recording** the conversation, just for note taking purposes, if you are happy for us to do so. Everything you say will remain **anonymous**, and your name won't be linked to this research at all. The other thing to note is that you all come from a variety of backgrounds, including holders of consumer data, app providers, and advocacy groups. We are really interested in hearing what each of you think – there are **no "right" or "wrong" answers** to anything we're talking about today. We may also discuss things that you have never given much thought to before today and that's absolutely fine.
15 mins	**I want to begin by discussing how you have come across the concepts of 'Smart Data' and 'vulnerable consumers' before today.**

	What, if anything, did you know/had you heard about 'Smart Data' schemes before today? • *If familiar/heard,* how / where have you come across this in your work? • *If any participants are unfamiliar or discussion is limited, read out the following description of Smart Data:* **Smart Data is the secure sharing of customer data combined with product and performance data with authorised third parties, facilitated by an interoperable framework. Through this innovation, consumers are able to harness the value of their own data and save time, money and effort by allowing third parties to offer them services across a wide variety of industries such as banking, finance, telecommunications and utilities. Open Banking is an example of a Smart Data scheme.** • How positively or negatively do you feel towards the development of Smart Data schemes for [Finance/Banking/Utilities/Telecoms]? • Why do you say this? What are the benefits and limitations of these schemes? **And before today, how, if at all, have you come across 'consumer vulnerability' in your own work?** • If clarification needed, read the following definition of vulnerability from the FCA: **A vulnerable customer is someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care.** • What types of vulnerable consumer are a particular priority for your sector and / or are most likely to face challenges in your sector? • Overall, what measures are you taking / advocating for to support vulnerable consumers access digital services in your sector? **As you heard in the presentation, our literature review uncovered trust, consent, and control as important pillars for inclusive Smart Data schemes. What were your initial reactions to the findings presented?** • How does this compare to what you already knew about Smart Data, digital design, and consumer vulnerability? • Did anything surprise you? **Was there anything missing? Which pillars, if any, would you add / change?** Why do you think this is an important addition to the scheme? *Moderator to make a note of any additional pillars and revisit during the deep-dive discussion.*
10 minutes	**I now want to focus in on the needs of consumers who have different types of vulnerability. Vulnerability is a spectrum, and all**

consumers are at risk of becoming vulnerable at some point in their lives.

Here are some personas for you to read through that brings this to life…

- **Poor health:** Lucy is a middle-aged woman who has a long-term mental health condition which impacts her mood. She is prone to impulsive behaviour, with a history of addiction. These factors make it difficult for her to budget, and so she often relies on her friends' support in order to manage her finances.
- **Life events:** Mollie has caring responsibilities for her younger brother, who has a long-term and severe physical health condition. Mollie's time is extremely limited as she juggles having to help her brother with day-to-day tasks with also working full-time.
- **Low financial/emotional resilience:** Zaynab works on a zero-hour contract, and her hours vary considerably week on week meaning her income is unpredictable. This also means that she does not have the savings needed to pay any unexpected expenses, should they arise, and she is already well into her overdraft.
- **Low capability:** Alan finds technology in general difficult to use; he never really had to develop digital skills when he was working, and now he's retired he uses the internet very infrequently. When he does, he often feels overwhelmed by how to navigate around and use online interfaces; he's therefore very fearful of doing something 'wrong' and putting his personal information at risk.

Do you recognise these personas in your work? To what extent do you think these consumers would want to, or be able to, participate in Smart Data schemes?

- What challenges could they experience in trying to participate in Smart Data schemes?
- What could encourage/enable vulnerable consumers to participate in Smart Data schemes in the first place?

How would you expect each of these consumers to engage with Smart Data schemes, and how would this differ from non-vulnerable consumers using the schemes?

- What would be the benefits to them?
- What risks might they be particularly susceptible to if they were to participate in Smart Data schemes? And what barriers to participation might they face?
- To what extent would non-vulnerable consumers experience these same challenges and risks?
- Within schemes, who should be responsible for identifying and supporting vulnerable consumers?

	• Are there specific data sets for vulnerable consumers that might be missed in generic smart data schemes? And would the inclusion of any specific data sets lead to potential harms for vulnerable consumers? **What practical steps should your sector take to design schemes which are inclusive of vulnerable consumers?** • What learnings, if any, can the sector draw from the design of other digital services / apps? (e.g., the NHS app, the COVID-19 tracking app) o How can the following smart data enabled use cases be made inclusive…? ▪ Account switching for banking/energy/telecoms, transfer of investments between finance institutions, price comparison websites ▪ Payments (automatic bank overdraft borrowing, managing utility bills in a shared household, rounding up transactions and 'sweeping' them into one pot) ▪ Financial management (finance dashboards, account aggregation/management across providers) ▪ Smart onboarding (account/identity verification, affordability checks, auto filling forms)
50 minutes	**For the remainder of the discussion, I want us to work together to create some best-practice design principles for inclusive Smart Data schemes. We'll start with the key pillars highlighted by the literature review, but we are free to change them or add additional ones as necessary so don't hold back!** **Let's start with CONSENT.** • What does a 'good' user journey look like when it comes to obtaining consent and authorisation for data-sharing? o What extra measures may be required for vulnerable consumers? • How should schemes clearly explain what an organisation will do with data a consumer consents to share? o How much data should be 'bundled' and a consumer asked to share in one go? How, if at all, does this vary according to specific vulnerabilities? o How long should consent last? How should short- and long-term consent (e.g., to receiving ongoing communication about offers/better deals) be communicated? Should this vary according by vulnerability types? o How can app providers balance transparency of decision options whilst avoiding information overload? o How should complex information be presented in an accessible way? (e.g., for consumers who may have practical

difficulties reading documents online, on smartphones, for those who have low literacy/numeracy etc.)

- How should vulnerable consumers be able keep track of organisations they have consented to share their data with/manage their consents?

- What should the consent revocation process look like?

- How should consumers who do not choose to engage with Smart Data schemes be treated? What sort of deals / offers should they be show by default?

- Is there anything else relevant to 'consent' that needs to be taken into account when designing for vulnerable consumers/inclusivity?

Our next pillar is TRUST.

- This emerged as a key barrier to the adoption of Smart Data schemes. What do you think are the main drivers of lower trust in schemes and similar digital platforms among vulnerable consumers?

- Overall, what does 'good' look like when to comes to building trust with vulnerable consumers in digital platforms?

- One driver of low trust could be *low digital and financial literacy* and the fear of something going 'wrong'. How should Smart Data schemes be designed in practice to reassure this type of consumer?

- What *privacy and security* controls are / should be in place to minimise the risk of vulnerable consumers being targeted with scams / fraudulent activities? (e.g., avoid data leakage)
    - *If any current controls are referenced*: are existing controls appropriate for vulnerable customers specifically? Do any extra measures need to be taken over and above these to protect *vulnerable* consumers?
    - How can user experience design make vulnerable consumers feel 'safe'?

- What does 'good' look like when it comes to customer authentication for vulnerable users? To what extent is this similar or different to consumers overall?

- What language and designs should be used to convey accreditation and trusted providers? (e.g., a Trustmark)

- Who should be responsible for communicating with vulnerable consumers about the trustworthiness of Smart Data schemes? What tone of voice should be used?

	- What support should be available if something goes wrong? Who is responsible for resolving the issue, App providers and data holders? How should support be provided? - Do schemes need to build in alternatives for the digitally excluded? How should they do this? - Is there anything else relevant to 'trust' that needs to be taken into account when designing for vulnerable consumers/inclusivity? **The final pillar highlighted by our literature review is CONTROL.** - Smart Data schemes will allow apps to be developed for different use cases using Smart Data, for example switching accounts, making payments, finance management, and deal comparison. What do you think a 'good' App user experience design would look like for vulnerable consumers? - How should key decisions and information ideally be presented and structured to be accessible to different audiences? - How much 'friction' should there be in the user journey to ensure vulnerable consumers are making decisions in their best interests? What decisions should not become 'easy' under Smart Data schemes? - How should Smart Data schemes mitigate or prevent personalised pricing and excessive targeting using consumer data? - What other design features could impact negatively on vulnerable consumers? (e.g., play on behavioural biases, or encourage consumers to act against their own interests) How should these be avoided? - To what extent should vulnerable consumers be able to nominate a trusted third party (e.g., family/friend) to help them manage their account? **Are there any other features/pillars of inclusive Smart Data schemes which we have not already discussed?** - Why do you think this is an important addition to the scheme? - How would this help protect / lead to better outcomes for vulnerable consumers? - What practical steps/guidelines would schemes need to follow to achieve this?
10 minutes	**For the last part of this discussion I want us to focus on refining the principles we have come up with to present them back to the group.** **Looking at what we have written down on the flip chart…**

	• Can you see any common themes and challenges? How are these areas connected? • Which of these principles are essential? • And which of these principles are 'nice to have'? • Do you think these principles will be similar/different to other industries? • How can we begin to articulate these as a clear set of principles for designing Smart Data schemes? What should our 'elevator pitch' to the group be? *Thank and close.*

Reference list

*Texts that were a part of the 20 that were reviewed in depth

Alzheimer’s Research UK (n.d.), *Mild cognitive impairment* [Online]. Retrieved from https://www.alzheimersresearchuk.org/dementia-information/types-of-dementia/mild-cognitive-impairment.

*Autorité des Marchés Financiers Québec, 2022. *Insights into the risks and benefits of digital financial services for consumers.* [Online] Retrieved from https://lautorite.qc.ca/fileadmin/lautorite/grand_public/publications/professionnels/doc-reflexion-consos-tech_an.pdf.

*Babina, T. et al., 2022. *Customer Data Access and Fintech Entry: Early Evidence from Open Banking,* [Stanford University Graduate School of Business Research Paper, No. 19-35]. [Online]. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333269

Basel Committee on Banking Supervision, 2019. *Report on Open Banking and application programming interfaces*. [Online]. Retrieved from https://www.bis.org/bcbs/publ/d486.pdf

*Beckert, W. & Siciliani, P., 2018. *Protecting vulnerable consumers in "Switching Markets".* Working Paper. [Online] Retrieved from https://ifs.org.uk/sites/default/files/output_url_files/WP201823.pdf

The Behavioural Insights Team, 2019. Terms and Conditions Apply [online] https://www.bi.team/blogs/terms-conditions-apply/ [accessed 29th March 2023]

BEIS, 2021b. *Regulatory Powers for Smart Data Impact Assessment (IA),* [Online]. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/915974/smart-data-impact-assessment.pdf

*BEIS, 2021c. *Smart Data Research: Customer experience guidelines for Smart Data schemes in regulated industries,* [Online]. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/993345/smart-data-research-customer-experience.pdf

BEIS, 2021a. *Smart Data Working Group: Spring 2021 report,* [Online]. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/993365/smart-data-working-group-report-2021.pdf

BEIS, 2018. *Implementing Midata in the Energy Sector: Government response to the Call for Evidence*. [Online]. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/729908/midata-energy-sector-government-response.pdf

*Chan, R., et al., 2022, *Towards an understanding of consumers’ FinTech adoption: the case of Open Banking*. International Journal of Bank Marketing, 886-917, 40(4).

Citizens Advice, 2019. *Smart data: putting consumers in control of their data and enabling innovation.* [Online]. Retrieved from https://www.citizensadvice.org.uk/Global/Public/Policy%20research/Documents/Consultation%20responses/Citizens%20Advice%20consultation%20response_%20smart%20data%20review.pdf

**Competition and Markets Authority, 2022. *Online Choice Architecture How digital design can harm competition and consumers*. [Online]. Retrieved from *https://www.gov.uk/government/publications/online-choice-architecture-how-digital-design-can-harm-competition-and-consumers*

*Consumer Policy Research Centre, 2020. *Unfair trading practices in digital markets - evidence and regulatory gaps,* [Online]. Retrieved from https://cprc.org.au/wp-content/uploads/2021/11/Unfair-Trading-Practices-in-Digital-Markets.pdf

*Croxson, K., Frost, J., Gambacorta, L. & Valletti, T., 2022. [Online]. *Platform-based business models and financial inclusion,* Retrived from https://www.bis.org/publ/work986.pdf

*CSIRO Data, 2018. *CDR Open Banking Workshop: Defining the UX of Consent,* [Online]. Retreived from https://consumerdatastandards.gov.au/sites/consumerdatastandards.gov.au/files/uploads/2018/12/Defining-the-UX-of-Consent-5.1-No-Appendices.pdf

*Dela Torre, J. T., 2022. *How can Open Banking be Implemented in the Philippines that will be Beneficial for both the Banks and the Unbanked/Underserved?,* Working Paper. [Online]. Retrieved from https://www.bsp.gov.ph/Pages/ABOUT%20THE%20BANK/Events/By%20Year/2022/Research-Fair-2022/Research_3_Day_2_Open_Banking.pdf

*Elliot, K., 2022. *Know Your Customer: Balancing innovation and regulation for financial inclusion,* Data & Policy, 4, e34. Retrieved from https://www.cambridge.org/core/services/aop-cambridge-core/content/view/81ECE6589B2932FDCAD400E41EA36661/S2632324922000232a.pdf/div-class-title-know-your-customer-balancing-innovation-and-regulation-for-financial-inclusion-div.pdf

FCA, 2021. *Guidance for firms on the fair treatment of vulnerable customers,* [Online]. Retrieved from https://www.fca.org.uk/publication/finalised-guidance/fg21-1.pdf.

FCA, 2022. *Financial Lives 2022 survey: insights on vulnerability and financial resilience relevant to the rising cost of living.* [Online]
Retreived from: https://www.fca.org.uk/data/financial-lives-2022-early-survey-insights-vulnerability-financial-resilience
[Accessed 15 March 2023].

*FinTechNZ, 2022. *Aotearoa Open Finance and Digital Equity*. [Online]. Retrieved from https://fintechnz.org.nz/wp-content/uploads/sites/5/2022/03/FinTechNZ-Report-2022_digital_03.22.pdf.

*Gaur, A. et al., n.d. *The Social and Distributional Outcomes of Digitalisation in the UK Retail Energy Market in 2025.* [Online]. Retrieved from https://www.cepa.co.uk/images/uploads/documents/Capstone_Final_Report.pdf

Gikay, A. A., 2020. *Discrimination, Vulnerable Consumers and Financial Inclusion.* Milton Park, Abingdon, Oxon; New York, NY: Routledge, 2021.: Routledge.

Gloag, A., Mackenzie, P. & Atay, A., 2019. *New fraud protections for people at risk,* [Online]. Retrieved from https://demos.co.uk/wp-content/uploads/2019/06/Cifas-digital-final.pdf.

Hilhorst, S., 2018. *New tech, old problems: A report on the Barclays financial inclusion roundtable,* [Online]. Retrieved from https://www.demos.co.uk/wp-content/uploads/2018/08/Demos-New-tech-old-problems.pdf

Honecker, F. & Anderson, N., 2022. *How can new financial technologies help to tackle social exclusion?,* Economics Observatory [Online]. Retrieved from https://eprints.gla.ac.uk/279337/

*Kelly, E., 2022. *Statutory review of the consumer data right: report.* The Australian Government (the Treasury). [Online]. Retrieved from https://treasury.gov.au/publication/p2022-314513

*Leong, E. & Gardner, J., 2021. *Open Banking in the UK and Singapore: Open Possibilities for Enhancing Financial Inclusion,* Journal of Business Law, Issue 5 [Online], Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4194256

Liu, J. Z., Sockin, M. & Xiong, W., 2021. *Data Privacy and Consumer Vulnerability,* [Online]. Retrieved from http://wxiong.mycpanel.princeton.edu/papers/Privacy.pdf

Munro, D. & Fellow, S., 2022. *Innovation, Regulation, and Trust in Open Banking and Digital Currencies,* [Online]. https://www.thefutureofmoney.ca/Munk.School.The.Future.of.Money.Discussion.Paper.pdf

Ofcom, 2020. *Consultation: Open Communications — Enabling people to share data with innovative services,* [Online]. Retrieved from https://www.ofcom.org.uk/__data/assets/pdf_file/0030/199146/consultation-open-communications.pdf

Office for National Statistics. (2020). *Internet access – households and individuals, Great Britain, 2020*. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2020.

Open Banking, 2023. *UK reaches 7 million Open Banking users milestone.* [Online] Retrieved from https://www.openbanking.org.uk/news/uk-reaches-7-million-open-banking-users-milestone/
[Accessed 15 March 2023].

*Open Banking, 2021. *Open Banking-TPP Customer Survey 2021 Report on survey results collected by post, telephone and online V1.0 November 2021*. www.marketingmeans.co.uk

*Plaitakis, A., & Staschen, S. ,2020. *Open Banking: How to Design for Financial Inclusion*.

*Reynolds, F. & Chidley, M., 2018. *Consumer Priorities for Open Banking*, [Online]. Retrieved from https://www.openbanking.org.uk/wp-content/uploads/2021/04/Consumer-Priorities-for-Open-Banking-report-June-2019.pdf

Thaler, R. H. & Sunstein, C. R., 2008. *Nudge: Improving decisions about health, wealth and happiness*. Yale University Press.

*Tooth, R. & Cox, K., 2021. *Implementation of an economy-wide Consumer Data Right - Strategic Assessment,* The Australia Government (The Treasury). [Online]. Retrieved from https://treasury.gov.au/sites/default/files/2021-08/c2021-182135-strat.docx

*UNESCO. (n.d.). *UNESCO Guidelines for Digital Inclusion for Low-skilled and Low-literate People DRAFT v1.2*. www.designkit.org,

Zachariadis, M. & Ozcan, P., 2017. *The API Economy and Digital Transformation in Financial Services: the Case of Open Banking,* SWIFT Institute (Working Paper No. 2016-001). [Online]. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2975199