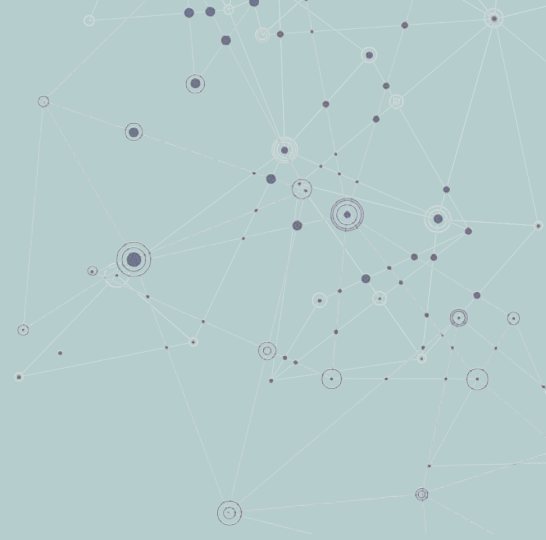
Britainthinks

Insight & Strategy

CDEI & DCMS | Public perceptions of digital identities and attributes: transparency, trust and data

Full report, March 2022

Contents



1 Introduction

CDEI and DCMS wanted to create a robust trust framework for digital identity solution providers

They commissioned primary research with citizens to:

1. Explore participants attitudes towards government-held data being shared for digital identity verification purposes.
2. Develop a nuanced understanding of how participants perceptions of, and expectations for, data sharing change depending on the level of data sharing – where the minimum level would be a 'yes'/'no' check.
3. Explore the level of transparency citizens want in relation to data sharing for digital identity.
4. Understand the attitudes of distinct groups who are likely to feel differently about data sharing, in particular, those who are disabled, digitally excluded, on lower incomes and/or from ethnic minority backgrounds.

Methodology

Participants were taken through three phases of research…

Phase One

Online focus groups
9 x 90 minute sessions, with 5-6 participants (UK citizens aged 18 and over)

Explored spontaneous associations and general attitudes to data sharing and spontaneous views of digital identities

Phase Two

Online task
Presented information on 4 use cases and gathered reactions

Presented information about data use through case studies, selected to represent a range of purposes, organisations, sources and technologies, as well as captured initial reactions and sorting

Phase Three

Online focus groups
9 x 90 minute sessions, with 5-6 participants (UK citizens aged 18 and over)*

Reconvened participants to explore informed views on digital identities, expectations for the future of digital identities – such as the level of transparency required and rules/principles governing the process

48 participants completed all three phases

This research was conducted between 1st February and 9th February 2022.

*In the second focus groups, 40-49s and 30-39s discussed use cases 1 & 2, 18-29s and 50-59s discussed cases 3 & 4, 60+ discussed cases 1 & 3, DE SEG and LTHC groups discussed cases 2 & 3, digitally excluded and ethnic minority groups discussed cases 1 & 4

Sample

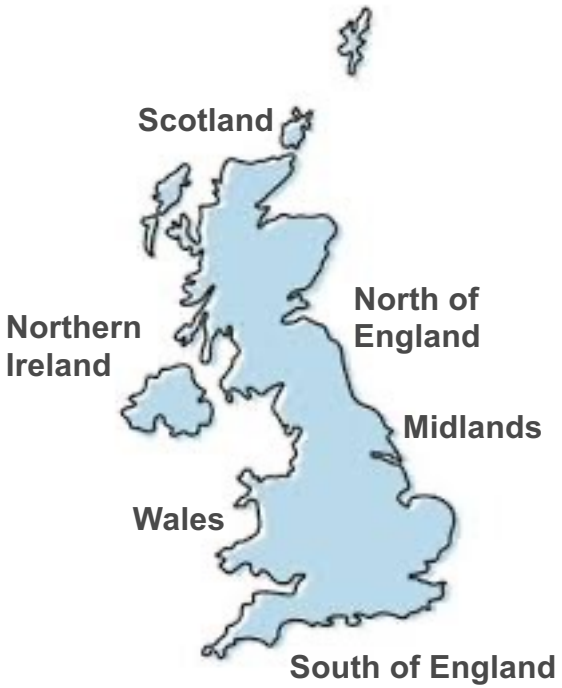
General participants: Each of the 5 groups were drawn from a different age cohort – this approach was taken as age is a key determinant of attitudes to, and cultural references for, technology and data use[1], meaning age-specific groups can give more focused and in-depth responses during a discussion.

Age 18 - 29	Age 30 - 39	Age 40 - 49	Age 50 - 59	Age 60+

Criteria groups: These groups were comprised of participants with specific characteristics which were known/hypothesised to influence attitudes to data sharing and/or access to digital services, including people:

In vulnerable financial circumstances	Who are digitally excluded	From ethnic minority backgrounds	With long-term conditions or disabilities
Using the socio-economic grade (SEG) as a measure, as well as measures of financial vulnerability	Those that have minimal digital skills and who tend to avoid doing things online when possible	People from a range of ethnic minority backgrounds to reflect potentially different experiences	A mix of disability and long-term care, including both physical disability and communication needs

Regions represented



For all groups:

Demographics

An equal balance of:
- Gender (Male/Female)
- Socio-economic group (ABC1/C2DE)
- Mix of urban, sub-urban and rural locations
- Ethnic minority audience to broadly reflect local demographics

Attitudes

- Spread of:
  - Optimism towards data sharing
  - Levels of comfort with sharing data

All participants were recruited via free-find recruitment methods – whereby recruiters use a database of potential participants and recruit them based on desired criteria and/or recruit participants 'fresh' through on-street recruitment.
Limitations to this approach:
- Participants are not randomly selected but rather purposefully recruited to meet a criteria. This ensures representation of different groups but means that the sample itself is not representative.
- Findings are therefore qualitative rather than quantitative. As per the Association of Qualitive Research, qualitative research is ""Focused on understanding the nature of phenomena and their meaning, rather than their incidence."[2]
- Sample excludes future users of Digital Identities (under 18s).

[1] https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-participantsations/reports-and-briefings/active-communities/rb_sept13_age_uk_digital_inclusion_evidence_review.pdf
[2] https://www.aqr.org.uk/glossary/qualitative-market-research

Glossary of terms

SEG[1]: Socio-economic Group.
LTHC: Long-term health condition.
DI: Digital identity.
OC: Online community.

[1] These social grades are a system of demographic classification originally developed by the National Readership Survey and now used by many other organisations for wider applications and have become a standard for market research. The grades are often grouped into ABC1 and C2DE; these are taken to equate to middle class and working class, respectively.

Key insights

1. **Participants spontaneously felt the current process of identity verification works well and is not in need of urgent improvement.** When prompted with specific examples, however, participants saw drawbacks relating to convenience and security.

2. **The concept of a digital identity was well-received by most, with the exception of some digitally disengaged and SEG DE participants.** The benefits of convenience, and to a lesser extent security, stand out and strengthen after more time is given to consider the concept.

3. **Participants' main concerns with digital identities were related to third party providers and how they are funded**. Many were suspicious about how they will be profiting from providing the service and how their conduct will be managed. **Beyond that, participants had practical concerns about ensuring the service was reliable and easy to use.**

4. **Perceptions of the benefits and risks tended to be consistent across the use cases tested** (e.g. extent of data shared and type of check) and were more strongly tied to the overarching concept of a digital identity. As a result, they had **consistent expectations for transparency across use cases.**

Key insights continued

5. **Five key factors** influenced participants' stated likelihood to use a digital identity: **ease of use, reliability, personal control of data, clarity about funding of DI providers** and **safety and security.**

6. Participants wanted to be **told three things about a digital identity service** before it's in place to feel confident using it**:** what the service was and how it worked; that it was Government accredited; and a clear account of how it was funded.

7. **Participants disliked the idea of multiple digital identity services with different features or levels of service.** They saw a digital identity as a basic utility, and wanted to feel confident any provider will offer the same service and be accepted everywhere. They didn't see the benefit of having multiple providers competing, as this could mean inconsistent service.

2. Perceptions of current identification processes

Findings in this section were derived from phase 1 of the research

No participants felt that identity verification needs to be urgently improved from a consumer perspective

Factors behind satisfaction for current ID verification

Participants felt that **verifying IDs wasn't time consuming or difficult.**

They also felt the current system was **broadly inclusive:**

- Older generations/digitally excluded were familiar with passports, driver licenses etc.

"Showing drivers licence or your ID is easy, and seems secure because your data isn't kept or stored."

Person in financially vulnerable circumstances

Potential improvements for current ID verification

Participants felt the ID verification required **excessive information** to be given at times e.g. utility bills, and this process could be simplified/streamlined

There was too much value placed on a passport and some felt that there **needs to be a back-up for passports** in the event of theft/loss.

"I think things like losing your passport, carrying that around and the risk of that, nowadays seems a bit obsolete that it's not virtual."

Person with an LTHC or disability

The participants tended not to think about identity verification as a form of 'data sharing' that they participated in regularly

We asked participants to think about what information or data about their identity they had shared recently

Spontaneously, most participants thought about **signing up for services**, when asked about sharing information about their identity.

Participants tended to think about sharing personal information (about their identity) to access services including online shopping, Zoom accounts, delivery services, Netflix etc.

"Thinking of the last few weeks, I've shared my data for delivery services, and even to sign up for a Zoom account for this call."

Person with an LTHC or disability

Those with more recent experience of less common and more complex processes spoke about ***'proving'* their identity**.

These participants had recent experience of checks for international travel, opening a bank account, or buying a house.

Participants tended to focus on their role in proving their identity (i.e. showing their documentation) and gave little thought to the process beyond that (e.g. verification against Government held data).

"Applying for jobs you share pretty much all of your information, your address, your criminal history, your sex."

Participant aged 40-49

Participants found it challenging to identify strong positives or concerns about the process

Identity verification was accepted as a small and necessary component of important processes such as travel, opening a bank account, buying a house and starting a new job.

Within the context of these already complicated processes, ID verification was not perceived as an arduous or a significant barrier.

Most described the process as straightforward and saw it as secure.

When participants were asked spontaneously to think about perceived downsides of current ID verification processes, they tended to be tied to past examples where something had gone wrong e.g. losing their passport and having to re-organise travel plans, or that current identification verification processes can exclude vulnerable groups who struggle to access required documents.

"I think it's [verifying ID] fine. I just see it as standard practice when I'm getting a flight. It doesn't take too long and I can't really see another way of doing it."

Person who is digitally excluded

"Having experienced losing a passport abroad, it really hits you how serious it is, how valuable your passport is and that there's no real back-up plan if/when you do lose it."

Participant aged 60+

When prompted with specific examples, participants did see some drawbacks to the current process

Difficulty accessing documents

Some participants found it challenging to gather the necessary documents e.g. utility bills to prove their identity, and suggested that more marginalised people might find it even more difficult to access required documents.

More broadly, remembering ID at times was a drawback for some.

"If you don't have the required documents – it can be quite difficult, it can marginalise some people and I know some people don't have that access."

Participant aged 60+

Data security concerns

Whilst rarely a spontaneous concern, there was uncertainty around how personal information is being stored currently by businesses, raising questions around security. These included how long employers hold identification data, or how private companies store physical and digital copies.

Fear of losing important documents

Participants felt passports were a less convenient form of ID for less important processes e.g. verifying age. This was due to fear of losing their passport and the cost of replacing it. Moreover, losing a passport abroad can lead to considerable difficulties.

"If your pocket could be picked on holiday and you don't know, your passport could be copied and six or seven fake IDs made before you realise."

Participant aged 40-49

Others using fake documents

There was also some concern that current documents to prove an identity are easy to replicate and can be used for fraudulent activity.

Losing valuable ID when carrying out an everyday ID task was the biggest concern for participants with the current process

Showing physical ID to purchase alcohol/cigarettes

Concerns

Participants said they were:

- Worried about **losing valuable ID**, such as a passport when carrying out an everyday task.
- **Likely to forget this ID** in some instances.

A new employer asks for your passport to check.

Concerns

Participants said they were:

- Unsure **how long** the employer will store personal data.
- Concerned about **how** the new employer stores personal data and the risk of a potential breach.

Scanning a passport for travel

Concerns

Participants said they:

- **Had minimal concerns** with the current process. It is seen as part of the process of travelling and essential in keeping air travel safe. However, some did express concerns around **forgetting their passport.**

Most participants accepted these ID processes as a necessity, particularly if you want to travel or start a new job

"Bringing your passport out to buy alcohol seems too risky… it's something I associate more with travelling abroad and not something I would want to lose."

Participant aged 60+

"With private companies and employers, I'm just worried how my data will be held."

Person who is digitally excluded

3. Perceptions of digital identities

Findings from in this section are derived from all three stages of the research

During the first session we introduced participants to the concept of a digital identity

Participants were shown the slide on the right and guided through an explanation of how digital identities could work for identity verification.

This explanation covered key points including that digital identities would:

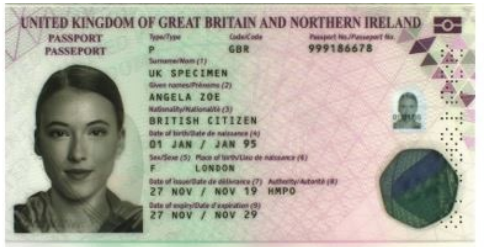
- Be delivered by the private sector;
- Involve these organisations accessing Government-held data;
- Have different forms of verification (e.g. Yes/No vs. More detailed access);
- Have standards set by Government and all providers who sign up will need to adhere to those standards.

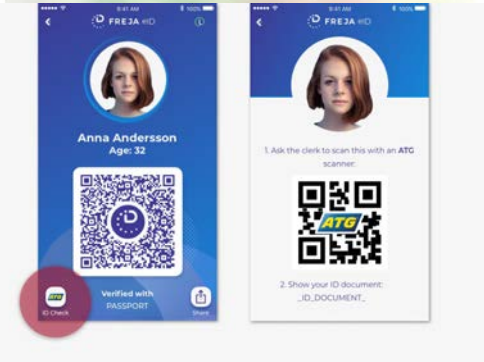
What is a digital identity?

At the moment, when we do things, like move jobs or home, buy insurance or travel abroad, we often have to prove that we are who we say we are. We usually do this by showing an identity document like a drivers licence or passport. The person at the other end has a look at the document, maybe takes a photocopy, and then contacts the government organisation that issued the document to check that it's real. For example, they might contact the passport office and ask if passport number 123 really exists.

In the future, instead of handing over a paper document, these checks could be done digitally. Instead of showing my drivers license every time I need to prove who I am, I show my drivers license number once and get a 'digital identity'. The digital identity company check my drivers licence against the central list, and give me back a code. I show this code to anyone who needs to check my identity so they know I am me. But they won't see any other information, like my address, that is written on my drivers licence. In other cases, the digital identity might include some simple info about me, say my date of birth too.

The Government will also set standards that providers will need to adhere to





9

Many participants were intuitively able to connect the concept of a digital identity to their experiences of verifying their ID currently.

This means that the benefits of DIs stood out and are easily grasped and concerns were often secondary.

This will be explored further in this upcoming section.

Spontaneously most participants supported the concept of a digital identity

Participants across all groups were able to highlight several benefits with digital identities, including how they could be easy to use every day.

Convenience

Across the groups, participants saw digital identities as a more convenient way to verify ID. Specifically:

- The process would be simple and easy to use e.g. not having to gather documents together for them to be checked.
- The process would be faster than typical ID checks.
- Greater convenience for those who do not have access to physical ID.
- More likely to carry your phone vs. ID (so therefore less likely to forget your ID).

"We are at a stage where things needs to be digital. For convenience, it could also be a generational thing. I have a wallet but I don't carry it around with me."

Person with an LTHC or disability

Security

To a lesser extent, participants across the groups saw the additional security provided by digital identities as a benefit. Particularly:

- Not having their data stored e.g. by employers; plus benefits for organisations of reducing risk of liability should something go wrong.
- Not having to share irrelevant information about themselves.
- Reducing the risk of losing physical ID documents (and associated data), plus most see their phone as secure due to biometric features.

"There's no other information, like your address, so it makes it less likely that someone would use your information, like your name and address, for other purposes."

Participant aged 40-49

However digitally disengaged and financially vulnerable participants were more sceptical about digital identities

Spontaneously, participants in both of these groups were more likely to feel hesitant and expressed scepticism about digital identities.

These participants tended to have lower levels of trust in the intentions of institutions, including the Government and private companies.

As a result, they were more likely to feel sceptical about the concept of digital identities and express concerns about:

- How the data will be held and kept 'up to date'.
- Who will 'see' their information.
- How the Government will execute the verification.
- Whether people would be forced to use a digital identity.

"I don't trust the Government, you know they can't do technology because of track and trace. I wouldn't sign up for it."
Person who is digitally excluded

"I wouldn't be comfortable with the private sector. It feels a bit invasive."
Person who is digitally excluded

Participants tended to describe a sense of ‘inevitability’ about the introduction of digital identities

A wider trend of moving away from ‘paper copies’.

The wider adoption of QR codes e.g. for airport security or Covid passports.

Many acknowledged they readily share information with third party providers currently.

This meant people could see digital identities as an evolution of the current method, rather than a “new” process. It meant participants tended to feel comfortable with the process.

Younger participants in particular tended to be most accepting and less likely to feel strongly about either the benefits or concerns of digital identities.

“I think if you’d asked me two years ago I’d have given you a very different answer. But we’re so used to using QR codes now, it seems normal.”

Participant aged 50-59

“I don’t think I think twice about sharing data, we do it all the time […] I think [using digital identities] is just a natural progression, I can really see it happening.”

Person from an ethnic minority background

Participants spontaneously assumed DIs will be 'consumer-owned' and multi-use

- When describing the benefits of DIs, participants tended to talk about a single digital identity that can be used across use-cases.
  - E.g. buying a home, purchasing age-restricted products *and* for right to work checks.
- This was seen as **vital to deliver additional convenience** beyond the current system of identity verification.
  - Many felt that if they had to repeatedly create new digital identities for different scenarios there would be no benefit to them.

Consumer-owned digital identity

In addition to the specific examples you looked at on the online community, another way that digital identities could be used would be for people to have a digital identity that they could use for lots of different purposes.

For example, you could use the same digital identity (e.g. scan the same QR code from the same digital identity provider) to verify who you are when opening a bank account, booking an international flight and when starting a new job.

Britainthinks Insight & Strategy

11

Participants were only able to identify a few minor additional benefits after further consideration of digital identities

Participants continued to see the main benefits to be convenience and security. After further time to consider, they also highlighted:

Less stress

Complex and significant processes like buying a house or moving job will become **less stressful**, if ID verification is more convenient.

"My children are both nationals of EU countries, and have had a National Identity card since they were babies. The card is much more user-friendly than what we have in the UK when it comes to proving identity, age, applying for jobs, buying a house, traveling overseas etc."

Participant aged 50-59

Greater accuracy

Some feel that there is a **lower risk of human error** if data is being provided digitally, though other participants challenged this.

"With computers / being online there is less margin for human error and fake documents etc."

Participant aged 18-29

Less risk of fraud

Some also feel that this technology would make it easier to **prevent crime** e.g. reducing opportunity for forgery, and **track criminals** or criminal behaviour.

"[Using digital identities at the airport would require] less people involved, less airport process / training, the potential to reduce time, the potential to reduce costs [and would make it] easier to track potential criminals."

Participant aged 18-29

In the online community and second focus groups, participants developed new concerns & existing concerns were reinforced

Participants were given an online task that involved learning about different use cases for digital identities

Can I trust DI providers?

- Participants expressed concerns about the conduct and motivations of private providers. They Included:
  - **Data privacy -** if providers will sell their data (or associated insights) onto other organisations.
  - **Data security -** if / how data will be stored by providers; and how it will be transferred to Government.
  - **Conduct and regulation -** who will be overseeing these providers and how well rules will be enforced.

Participants reported wanting to hear more about *who* the providers of the service would be, before they would feel comfortable using a digital identity. This was in line with how participants reported approaching data sharing in other scenarios relating to intimate or financial data.

Can I trust how DI verification will work?

- Participants also express practical concerns, although these tended to be less strong than concerns about the providers themselves. They included:
  - **Being unable to access your device** e.g. if you forget your phone or it runs out of battery.
  - **Concerns if the system went down** and you wouldn't be able to verify your ID.
  - **Excluding certain groups** who may feel less confident using digital technology.
  - **Organisations not accepting DI** and therefore being unable to verify your ID.

These concerns lead some participants to think it would be necessary to hold a physical copy of their ID as well, which would undermine the benefits of convenience.

Perceptions of the potential risks of digital identities grew with further consideration (verbatim)

Can I trust DI providers?

"Does the government have the correct protocols and regulations in place to ensure the individual's data is protected in this electronic environment? Who will oversee the process and are they independent of the government?"

Participant aged 60+

"Would we have to pay for it or would it be free?"

Person who is digitally excluded

Can I trust how DI verification will work?

"I feel that business would be reluctant to take it up, as there are already some simplified versions of digital IDs and many businesses don't accept these."

Person with a long-term health condition or disability

"What troubleshoot options and/ or back ups [will be] in place in the event the system experiences issues?"

Person with an LTHC or disability

Perceptions of specific use cases of a digital identity

Views of the benefits and risks of specific use cases matched the broader views of DIs.

Participants were more likely to be concerned about the consequences of mistakes and the process going wrong, rather than data security.

Use Case 1*: Starting a new job

45 / 52 said they would use this service. Security stood out as the key benefit, however, concerns around the service 'not working' were heightened in this use case relative to others.**

- Participants felt that it was **more secure for an employer not to be responsible for holding copies of passport details** where they could be leaked or exploited. (Mentioned by 4 of the 5 groups)

"[This case] limits the amount of sensitive data that your employer needs to hold about you. [It] eliminates the risk of human error occurring and your scanned documents being leaked etc."

Participant aged 18-29

- Participants expressed concern about **not having a specific digital identity requested** by an employer e.g. if their provider is not accepted by the employer. (Mentioned by 4 of the 5 groups)
- Or **having incorrect data shared through a digital identity**, and not being able to explain themselves. (Mentioned by 3 of the 5 groups)
- They felt both these concerns could **exclude** people from certain jobs. (Mentioned by 4 of the 5 groups)

"Some employers may not accept it as being adequate proof unless it was made law to do so."

Person with an LTHC or disability

**Use case 1 was shown to all participants in the online community and discussed in detail in 5 groups (Participants aged 30 – 39, 40 – 49, 60+, those who are digitally excluded and those from an ethnic minority background) in phase 3 of the research. Please treat all discussions of the proportions of participants / focus groups expressing a certain viewpoint as indicative rather than representative data due to the small base sizes involved and the non-representative, qualitative nature of the sample.*

**52 participants completed the online community

Use Case 2*: Getting car insurance

41 / 52 said they would use this service. Participants saw the additional convenience from a quicker process as the key benefit, however, were also concerned about if things 'go wrong'.

- Participants saw a benefit in the ability of a digital identity to **prevent the need to repeatedly fill out forms** with the same information. They saw this as expediting a time-consuming process. (Mentioned by 3 of the 4 groups)

- Participants expressed concern about **incorrect information** being shared without their knowledge, resulting in: (Mentioned by 3 of the 4 groups)
- An **incorrect quote**, without the opportunity to explain yourself. (Mentioned by 2 of the 4 groups)
- A **time-consuming and potentially stressful process** to try to resolve the situation. (Mentioned by 2 of the 4 groups)

"[It is] fast, and easy access to my information, no hassle of filling in a long survey online."

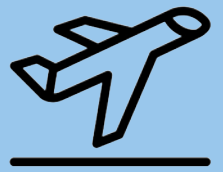
Person from an ethnic minority background

"It could be time consuming and potentially costly if incorrect information is stored."

Participant aged 30-39

**Use case 2 was shown to all participants in the online community and discussed in detail in 4 groups (Participants aged 30 – 39, 40 – 49, those who are in financially vulnerable circumstances and those with long term health conditions) in phase 3 of the research. Please treat all discussions of the proportions of participants / focus groups expressing a certain viewpoint as indicative rather than representative data due to the small base sizes involved and the non-representative, qualitative nature of the sample.*

Use Case 3*: Taking a flight



44 / 52 said they would use this service. Participants saw increased national security as the key benefit, however concerns about the accuracy of the system could undermine that.

- Participants saw airports as one of the most important places verify ID. They felt that using a digital ID in this context may **prevent people entering or leaving the country without the correct permissions documentation** if made compulsory. (Mentioned by 3 of the 5 groups)
- It may also **speed up the process of going through the airport** (therefore making it less stressful). (Mentioned by 3 of the 5 groups)

"It's quicker and simpler, less stressful and more automated."

Participant aged 30-39

- A small group of participants (typically digitally disengaged, but also from across the groups) **felt uncomfortable about face scans and found them intrusive.** Whilst accepting of it in an airport context, they worried about it being used elsewhere e.g. CCTV. (Mentioned by 3 of the 5 groups)
- Others worried about the accuracy of the technology and the **large knock-on impact in the event the technology fails** or makes a mistake. (Mentioned by 4 of the 5 groups)

"I feel like this is very intrusive to my personal identity."

Person who is digitally excluded

**Use case 3 was shown to all participants in the online community and discussed in detail in 5 groups (Participants aged 18 – 29, 50 – 59, 60+, those who are in financially vulnerable circumstances and those with long term health conditions) in phase 3 of the research. Please treat all discussions of the proportions of participants / focus groups expressing a certain viewpoint as indicative rather than representative data due to the small base sizes involved and the non-representative, qualitative nature of the sample.*

Use Case 4*: Opening a bank account

43 / 52 said they would use this service. Participants saw security as the key benefit, however concerns about the accuracy of the system can undermine that.

- Participants appreciated the **chance to verify their address without having to present a letter** containing personal and irrelevant details e.g. utility usage. (Mentioned by 4 of the 4 groups).
- It is also felt to make the process more convenient, due to **having to source fewer documents.** (Mentioned by 4 of the 4 groups)
- Others felt this could make **bank accounts more accessible** to those without physical forms of ID. (Mentioned by 2 of the 4 groups)

"[It is better for] personal security as I wouldn't have to hand any documents with my address on to bank."

Person from an ethnic minority background

- Participants were more likely to express **general concerns about digital identities** e.g. data security, excluding certain groups, the service going down, when thinking about this use case. (Mentioned by 2 of the 4 groups)
- Some participants expressed **heightened concerns due**
- **to the 'financial context'** meaning potential consequences if something goes wrong are more significant. (Mentioned by 2 of the 4 groups)

"Could fraud be easier? It is already extremely hard for unhoused people to open a bank account and this would make it impossible."

Participant aged 30-39

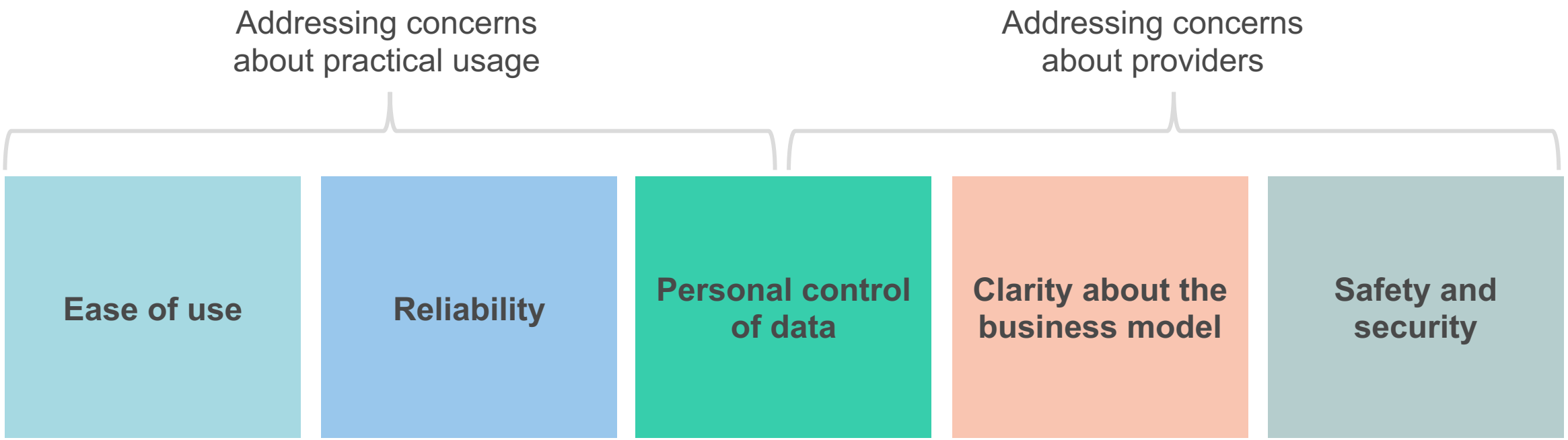
**Use case 4 was shown to all participants in the online community and discussed in detail in 4 groups (Participants aged 18 – 29, 50 – 59, those who are digitally excluded and those from an ethnic minority background) in phase 3 of the research. Please treat all discussions of the proportions of participants / focus groups expressing a certain viewpoint as indicative rather than representative data due to the small base sizes involved and the non-representative, qualitative nature of the sample.*

4. Conditions for use and expectations of transparency

Findings from in this section were derived from phases 2 and 3 of the research

Five conditions influenced the likelihood of participants saying they would be willing to use a digital identity service

Analysis of all focus groups showed that five factors are influential in the likelihood of participants willingness to use a DI service:



These factors addressed their concerns about practical usage of DIs and DI providers.

To realise the full benefit of convenience, digital identities should feel easy to use

Participants were starting from a place where ID verification was not seen as a difficult or arduous process. The additional convenience participants felt digital identities offered would only be realised if the process is felt to be straightforward. They waned:

To have a simple understanding of what the service is and how it works...	**…however, they didn't want to make regular choices about the best provider …**	**...and they wanted any user journey to be straightforward.**
Participants wanted to know what they're using and what was required from them. The process should feel straightforward and easy to understand.	Participants did not want to have to continually make choices on providers (e.g. based on their security / reputation). To reduce choice, they wanted providers to offer the same service.	The primary benefit was convenience. If the process felt difficult to use, it was likely participants will revert back to physical copies of their ID.
"It should almost work like an Oyster card." *Person who is digitally excluded*	*"Would have to be a list of approved providers that we could all see."* *Participant aged 60+*	*"It needs to make my life easier."* *Person with an LTHC or disability*

Participants wanted the DIs to be reliable and providers to offer 24/7 helplines should the system 'go down'

Participants were concerned by digital systems 'not working' and presenting a barrier to the things they want to do e.g. travel, start a new job smoothly.

- Reliability in terms of **system maintenance i.e. they wanted the service to work at all times.** They will receive this assurance from:
  - Their own experiences;
  - Reported experiences from friends / family.

- Many said they would like to see providers **offer a 24/7 helpline**, as this would make them more confident in a matter being rectified, should it go wrong.

"[I would want to know about] system functionality and maintenance [and know] the system will always be up and running."

Person from an ethnic minority background

To bolster convenience benefits they also wanted DIs to be widely accepted by organisations

Participants wanted **DI providers they used to be accepted by organisations.** For example, if they were using a consumer-owned DI they did not want it to be rejected by a particular organisation and made to use another provider.

- This was important to ensure the benefit of convenience i.e. consumers could reliably use their DI as and when it would be needed.
- It would also make it more akin to ID verification at the moment i.e. passports are accepted everywhere, which is seen as straightforward and reliable.

"I'm concerned around the effectiveness of this. Will it be accepted everywhere, or only certain places?"

Person who is digitally excluded

"It's so much more convenient to have digital access to check identities rather than carry a passport/driving licence around."

Person with an LTHC or disability

However, most participants did not want DIs to be the only method of accepted ID verification

Some pushed back against being ‘forced’ to use a digital identity. Lower socioeconomic grade and digitally disengaged participants were most reluctant, but there was a degree of resistance to compulsory introduction of digital ID in all groups.

These participants wanted to see rules to make sure companies offer alternative ‘traditional’ systems.

“I just hope there's a choice, that's all really.”

Person in financially vulnerable circumstances

Other participants acknowledged the challenges with excluding certain groups from a digital identity, however, they viewed these challenges as minor issues and tended to be more accepting of the consequences.

They saw digital identities as another example of the trend of ‘digitalisation’ and that people should adapt if they want to use certain services.

“There will always be some people who are against change, but you have to accept it in the end because it is going to happen.”

Person from an ethnic minority background

Related to understanding the service, participants wanted it to be clear what information they chose to share and with whom

Participants wanted to feel in control of the verification process. This included:

- Clearly choosing what information they were asked to be verified each time they used the service.
- Some described seeing a record of past instances they have verified their information would be helpful.
  - This gives control and a sense of security e.g. similar to reviewing bank statements.
  - However they did not want this history to be visible to others.

I'd want to choose what information is going to be shared, so I know what's happening… I also don't want people seeing what checks I've done… I don't want my new job seeing I've had my ID checked to get a loan.

Participant aged 18 – 29

"I like to have my documents because I can see what has happened. I want to be able to print off if I have shared something using a digital identity."

Person in financially vulnerable circumstances

Participants wanted clarity about how DI providers make money and would prefer them not to be funded by data sharing

Participants consistently raised the question of 'how the service is paid for'? The lack of clarity led them to make the following assumptions:

Most preferable ⟷ Least preferable

The organisations (e.g. airlines, employers) pay for the service	The individual users pay for the service	DI providers make money via selling their data or insights to other companies
This option was preferred for two reasons. First, the transaction felt transparent (i.e. it is clear transaction, rather than the unclear profiting from selling data and/or insights). Second, the cost was borne by someone other than the consumer.	Although this was preferable to their data being sold on (as the transaction feels clearer), participants were unwilling to pay for the service. This is likely due to seeing current ID verification as 'free' (despite there being an upfront cost).	Participants were most concerned by this option as it tied back to one of their chief concerns about data sharing generally (that the recipient was profiting from them). The concern was heightened in the DI scenario, as they saw providers having access to a lot of valuable information.

Participants would prefer digital identity providers to be independent to avoid data being used for other purposes

- There was inherent scepticism about technology providers and what they do with data. This was particularly pronounced amongst lower socioeconomic grade and digitally disengaged participants.
- For that reason, participants would want providers to be single service i.e. only offer digital identities, even if they are being paid for by organisations or individuals.
    - This would help to allay concerns that providers are using intangible insights about them to fund other parts of their organisation e.g. via targeted ads.

"I wouldn't want an Amazon digital identity. And I wouldn't want an Aviva digital identity. They would do loads of stuff with my information."

Participant aged 50-59

"They should only be allowed to do this. They'll have access to so much powerful information."

Participant aged 18-29

Participants saw accreditation of DI providers as integral to creating a trusted, secure environment for consumers

- Participants were reassured by information that providers will be accredited in order to provider the service.
  - It implies there will be oversight and regulation from an independent entity.
  - Participants said that ‘kitemarks’ or ‘trust marks’ will be helpful symbols to look out for when deciding which provider to go with.
- That said, the current political context (of lack of trust in the Government and recent scandals about contracts) meant that participants feltuncertain about the accreditation process.
  - Some expressed a desire to know the process is impartial and fair.
- Despite reporting a desire for accreditation, participants did not report consistently checking for specific similar accreditations when sharing data and using digital services in other contexts.

“This is the sort of thing that needs a regulator.”

Participant aged 60+

“Companies should be accredited and not be granted the right to operate as digital identity providers just based on connections to government, such as with ministers for example.”

Person from an ethnic minority background

Participants had high expectations for the standards accredited DI providers should meet

Participants saw strict, effective, and 'independent' regulation as directly addressing their concerns about the conduct of third party providers. They expected to see:

Data security standards	Proactive commitment to transparent operations	Sanctions and a course of redress
There were high expectations that their data will be stored securely, due to the perceived high risk of identity theft.	For example, providers should agree to be regularly audited to ensure they're meeting the high standards.	Participants wanted to see providers punished (e.g. financially) should they fail to meet standards and a way for them to meaningfully complain if they were not satisfied.
"If someone could take that kind of information and some kind of identity theft. That's what would worry me." *Participant aged 40-49*	*"It can't just be that the provider is approved, the government needs to keep checking on them."* *Person in financially vulnerable circumstances*	*"There needs to be provider accreditation and sanctions for failures like data breaches, like for financial institutions."* *Person in financially vulnerable circumstances*

However, in general, participants were not clear on the specifics of the regulation they would like to see, nor did they desire to know more about it.

Instead, most tended to feel confident that the Government will employ experts to oversee providers appropriately.

"I don't know what regulation will make sure it's all secure. I don't think that's a question I should be answering – I trust the people with the right technical knowledge to make that call."

Participant aged 18-29

"I don't need to know what it is. Just that someone is overseeing it."

Participant aged 50-59

Participants had fairly simple transparency expectations for a digital identity service

Ultimately, participants wanted to be told three things about a digital identity service:

What it is and how it works

- Participants wanted to have a basic understanding of the process.
- They wanted to feel confident that it will be easy to use, reliable and in control of their data.

That it's Government accredited

- Participants saw this as providing assurance that the service will be safe, secure and regulated.
- However, they did not report consistently checking for similar accreditations when sharing data in other contexts.

A clear account of how DI providers are funded

- A key question for participants was how the service is paid for.
- Participants wanted to know this before engaging with DIs i.e. how will the companies use their data (if at all).

Participants wanted all DI providers to meet the same, high and consistent standards

Participants across all groups felt **identity verification is an important process that should be accessible to everyone**.

In line with this, **they wanted the decision about which DI provider to use to be simple, with no risk to consumers** that they may inadvertently select a provider that is any of the following:

- Difficult to use
- Unreliable
- Does not give them control over their data
- Has an unethical business model (i.e. is selling their data)
- Stores their information in an insecure way

In order to have trust in the marketplace they believed the Government will need to:

- Set standards in these areas
- Enforce those standards

Participants wanted all DI providers to meet the same, high and consistent standards (verbatim)

"I would rather there just be one provider so I didn't have to think about who to use."

Participant aged 20 - 29

"I don't want to have to make any choices or think about if it's good or not. They should all do the same thing."

Participant aged 50 - 59

"I hope it's an even playing field, where each provider has the same standards."

Participant aged 60+

"There needs to be a benchmark in place, like an accreditation for providers similar to Ofsted, and they all have to meet this standard."

Participant who is digitally excluded

For more information, please contact:

Lucy Farrow | Associate Partner
lfarrow@britainthinks.com
Max Templer | Research Director
mtempler@britainthinks.com
Allie Jennings | Research Lead
ajennings@britainthinks.com
Darragh McHenry | Senior Research Executive
dmchenry@britainthinks.com
Tom Lusuardi | Research Executive
tlusuardi@britainthinks.com

Thank you

info@britainthinks.com

T: +44 (0)20 7845 5880

www.britainthinks.com

BritainThinks
West Wing
Somerset House
London
WC2R 1LA
United Kingdom

Appendix

Socio-economic Group. Classifications are based on the following:

Grade	Social Class	Chief Income Earner's occupation
A	Upper middle class	Higher managerial roles, administrative or professional
B	Middle middle class	Intermediate managerial roles, administrative or professional
C1	Lower middle class	Supervisory or clerical and junior managerial roles, administrative or professional
C2	Skilled working class	Skilled manual workers
D	Working class	Semi-skilled and unskilled manual workers
E	Non-working	State pensioners, casual and lowest grade workers, unemployed with state benefits only.

[1] These social grades are a system of demographic classification originally developed by the National Readership Survey and now used by many other organisations for wider applications and have become a standard for market research. The grades are often grouped into ABC1 and C2DE; these are taken to equate to middle class and working class, respectively.