## **Focus group protocol**

## **Summary**

|  |  |
| --- | --- |
| **Detail** | **Timing** |
| 1. Welcome + Introduction | 5 |
| 1. Personal data + Attitudes | 15 |
| 1. Control | 10 |
| 1. Would you like more Control | 10 |
| 1. Protection | 10 |
| 1. Personal Data Store | 10 |
| 1. Personal data store (Out-of-home) | 15 |
| 1. Payment + marketisation | 10 |
| 1. Paying for Personal Data Store | 5 |
| 1. Debrief | 5 |
| **Total** | 95 Mins |

1. **Welcome + Introduction (5 mins)**

*Introduce moderator and research team (working on behalf of Bangor University), thank them for attendance, ask permission to record, reassure them of the anonymity of the data collection and results, no right or wrong answers; not expecting experts we’re just interested in your thoughts and experiences.*

*Netiquette – try and treat this as a discussion: respond to other participants; don’t interrupt. You can use the raise hand function. Connection problems.*

*Any questions? Start recording.*

1. **Personal data + Attitudes (15 mins)**

* Survey questions:
  + Which of the following devices do you use?   
    [desktop computer; laptop computer; smart phone; tablet; wearable technology (e.g., smart watch); smart speakers (google home; amazon echo)]
  + How much time do you spend online per day?
* Tell me about the types of apps and websites you like to visit
  + [What are your favourite sites/funniest video you’ve seen online?]
  + [What was the last site you visited?]
  + What was the last thing you did on online?

[Connecting question: did you have to sign up?]

* Do you understand what personal data are?
  + Can you give examples?
* Do you understand how organisations share and use your personal data?
  + Why are they collecting your data?
* How do you think this affects you?

(e.g., having content personalised, targeted with messages (ads, political etc)).

* + Is this use of your personal data good/bad? Why?

1. **Control (10 mins)**

* Do you ever feel at risk or out of control online? Can you tell me more about these situations?
* [Examples as prompts:
  + - Banking/finance (personal example: online deposit payment)
    - Social networks (unknown friend requests)
    - Signing up for new services (types of data requested)
    - Public Wifi hotspots (is access secure?)
    - Sharing and accessing devices (3rd parties)
    - Concerns about adtech/marketing tracking
    - Concerns about government tracking and surveillance
    - Using sites that are ethically dubious (file sharing, dark web, [pornography])]

1. **Would you like more control? (10 mins)**

* Would you like more control? If so, why?
  + What would you like to have more control over?
    - Financial matters (e.g., Lost money online via Paypal)
    - Security (e.g., passwords and accounts hacked or lost)
    - Online interactions (e.g., uncomfortable; aggressive; frustrating)
    - Privacy (e.g., not having to worry about tracking and monitoring)
* If not, why?
  + Nothing to fear/hide?
    - Challenge participants: Do marketers have a right? Shouldn’t they ask rather than take?
    - Example of inappropriate marketing (political mailings; pregnant girl example) – not necessarily that you have something to hide just unwelcome.
  + Current legislation is fine (GDPR)?
  + Nothing bad has ever happened to me
    - Why do you think that is?

1. **Protection (10 mins)**

* How do you go about protecting your personal data and privacy online?
  + Virtual Private Network (VPN)
  + Password managers (e.g., Lastpass)
  + Search engines that block advertising trackers and do not record my search histories (e.g., Duck Duck Go)
  + A personal email account that is end-to-end encrypted (e.g. ProtonMail)
  + Multiple accounts (email; social; single use).
  + Others (please specify)
* [Further prompt/connecting question]: Why did you choose these options?
* Do you pay for any of these? Why?
  + - Quality
    - Service
    - Extra protection
    - Suspicious of economy of “free”

1. **Personal Data Stores online (10 mins)**

* Opening question: Has anyone heard of Personal Data Stores?
* *Explanation:* A "Personal data store" is a smartphone app that lets people securely store and share their personal data. It gives you control over what is being shared with whom, for how long and for what purpose’. This might include data like your name and address which you need to fill out webforms or more specific data around health, for example.

Do you understand? [If, not use the safe/combination lock metaphor.]

* + (Online) scenarios to share:
    - Moving house
    - Change of phone number
    - Password storage
    - Reducing customer journey and data re-entry during signup.
    - Banking/payment details
    - *More needed?*
* Do you think a personal data store is a good way of storing and sharing data? Why?
* What types of data would you be happy/not happy to store and share using a personal data store? Why?
* [Can you explain your choices?]

1. **Personal Data Store out-of-home (15 mins)**

A personal data store can also be used when you are away from home and even offline. Here are some examples of how a personal data store might work.

* Retail
* Sharing data about body shape, clothing styles, age, gender and budget with selected shops to enable tailored service and/or discounts via a one-off choice option on your smartphone.
* Would you use a personal data store in this way? *(why?/why not?)*
* What about if your reactions were tracked to help them tailor the service?
* Sports stadiums
* Opt-in sharing data about your heart rate via a wearable technology (e.g. Apple Watch) to monitor crowd emotion and feed this back at key moments (eg footballer scores a goal) into displays in the stadium (eg changing lighting, images, sound etc) , to heighten the crowd’s experience and make it a more immersive environment based on biofeedback.
* Would you use a personal data in this way? *(why?/why not?)*
* Data passports
  + Selecting specific and only relevant info (I have/haven’t been vaccinated).
  + Use to get into a workplace, school &c.
  + Would you use a personal data in this way? *(why?/why not?)*
* [Further scenarios – avoid unless necessary: Reduced insurance premiums; access to health information]

1. **Payment + marketisation of data (10 mins)**

* How do you feel about being paid for your personal data?
  + Does this seem like a good idea?
  + Can you think of any reasons why this might seem unethical or wrong? (Privacy haves/have nots)
  + [Survey] What data would you share for payment?
    - Age
    - Gender
    - Location
    - Relationship status
    - Ethnicity
    - Sexual orientation
    - Health
    - Political views
    - Religious beliefs
    - Hobbies
    - Shopping history
    - Social media content (e.g. archive of Facebook posts and likes)
    - Mental outlook, mood and emotion

* Do you think you currently share mental outlook, mood and emotion data?
  + How do you think it used?
* What payment would you accept for this data? And for what uses?

1. **Payment for Personal Data Stores (5 mins)**

* In order to use a personal data store, would you:
  + be happy to pay?
  + let the app take a % you made by sharing your own data yourself?
  + allow them to use and sell selected aspects of your personal data, with your permission?

1. **Debrief (5 mins)**

* I just have a couple of follow-up of questions, as I’d like to make sure I’ve understood you properly…
* Thank you so much for your conversation today, it’s been *very* helpful.
* On behalf of Bangor University and Cufflink, I’d like to thank you all for taking precious time out of your day / evening, away from work and families to spend time with us sharing your valuable insights and opinions.
* This is really important work and it’s great that you’ve had an opportunity to help shape the future direction of apps that help you store and share your personal data.
* I’ll let Panelbase know that you took part and they should process the payment.
* Did anyone have any questions before I let you go?

[Highlighted elements indicate questions used to stimulate discussion.]

**Data recording and Transcription protocol**

The focus groups were recorded using Zoom’s in-built recording facility, with an audio back-up created using a local recording device. Audio files were sent to Rev.com for initial transcription. Some issues were found in these initial transcriptions (e.g., lexical errors; negatives; wrong attributions; clause position as final or initial). Transcripts were corrected and refined by moderator and anonymised and prepared as word docs for upload to Nvivo. Participants were given a pseudonym that reflected the demographic elements of their name (age, gender, and any national/cultural markers).

As the transcript was being prepared for thematic analysis, the focus was on content rather than interaction, so a relatively simplified transcription style was adopted. Choices included:

* Transcript divided based on completed speaker turns (as there was minimal overtalk/cross talk).
* Crosstalk has been removed if inaudible or backchanneling, i.e. if it provides information about the interaction but not the topic.
* No notation for minimal pauses, overlaps, interruptions, prosody &c.
* Adoption of some written discourse grammatical elements (full stop and commas) to aid comprehension.
* Turns start with capitals and end with full stop. However, if there is a short interjection by another participant that does not disrupt the flow of talk then the previous turn ends in a comma and the next turn starts lower case.
* Fillers/repetitions have not been added if missed by original transcription service.
* Where the moderator is talking a lot (i.e., description of personal data stores), turn has been converted into paragraphs for ease of reading.

Basic key:

… Pause and restart/correction

* Truncated word/turn

[XXX] Inaudible, each X represents a syllable.

[Word] Best approximation of inaudible content.

“Word” Quoting/Voicing (Participant takes on the voice of another, or themselves at a different point in time)

\*Action\* Denotes an action/vocalisation.

{Word} Identifying information replaced