Focus Group Protocol

Opening

(Thank you all for participating in this focus group discussion.)
As generative AI capabilities are gradually integrated into mobile operating systems and various applications, multimodal data such as voice, images, text, geolocation, and app content are continuously collected and processed. Mobile phones are transforming from "tools" into highly intelligent, proactive decision-making "assistants." While this transformation enhances user experience, it also significantly amplifies uncertainties regarding privacy and security, such as: where exactly is the data being used, how are permissions clearly defined when accessing data across applications, and are there sufficient protection mechanisms for vulnerable groups? This discussion takes typical use cases of "GenAI smartphones" as its starting point, with the core objective being **to address privacy protection issues, we will jointly produce a number of feasible technology and product design solutions.**
In terms of process, we will first have an icebreaker session, and then introduce example scenarios to help everyone gain a relatively consistent understanding of the "GenAI smartphone". Following this, through an open discussion, we will guide everyone to discuss the feasibility and practical implementation of the solution from different perspectives. Finally, we will provide a brief summary of the discussion.
The discussion will identify the most valuable privacy-preserving designs and focus on their technical feasibility and potential challenges. This discussion will last approximately 60 minutes.
During the discussions, we will record audio and video and collect paper materials. The collected data will be used solely for this research. You have the right to access, correct, and delete your data. Your participation in this project is voluntary, and you can withdraw at any time without giving a reason. You can skip any task you do not wish to participate in at any time for any reason, without explanation. There are no right or wrong answers to the questions we prepare. All your answers will be kept strictly confidential, anonymized, encrypted, and reviewed only by the researchers of this project.
Do you still have any questions?

Icebreaking (5 minutes)

Quick, sequential, simple self-acceptance.

Scene alignment (3 minutes)

(The host first introduces the use cases of the GenAI smartphone.)

In-depth discussion (40-50 minutes)

Okay, now let's move on to the second part: an in-depth discussion.

The forms you've received contain all the technical suggestions compiled from previous interviews, which will later be presented in the slides.
Our goal is to quickly assess their effectiveness and technical feasibility, and to discuss each suggestion in depth from three aspects: technical feasibility, technical challenges and limitations, and impacts and trade-offs.

For each suggestion listed in the slides, please do two things later:
Step 1: Rate all suggestions (1-5 points)
(1) Effectiveness in addressing privacy issues (1–5 points)
Definition: To what extent can this suggestion reduce privacy breaches and improve data security?

- Example of a 1-point score: It offers almost no privacy protection; for example, it only changes the text on the interface without any actual improvement in privacy.
- Example of a 5-point score: Significantly improves privacy and security, such as completely blocking unnecessary data access or providing very granular access control.

(2) Feasibility of the plan (1–5 points)
Definition: Is this solution "feasible" within the current technical framework, regulatory requirements, and business logic of the product?
The key here is "whether it can be done" and "whether there are obstacles", rather than "how difficult it is to do".
Rating example:

- 1 point (almost impossible):
    - It requires a major system-level overhaul, which is not supported by the current technology stack.
    - This involves the cross-border flow of sensitive data and violates regulations.
    - This could severely impact core business logic or cause unacceptable user experience conflicts.
- 5 points (highly feasible):
    - The current framework already has basic support; you just need to add an interface or switch.
    - It does not violate any policies and does not change the core architecture.
    - It will not conflict with existing processes.

(Example: Specifying permissions more clearly → No change to technical structure, no regulatory risks → High feasibility)
(3) Technical difficulty (1–5 points)
Definition: Within the existing technological framework, how much engineering work and development cost is required to implement this function?
The focus here is on "how difficult it is to do" and "how high the cost is," which is different from feasibility.
Rating example:

- 1 point (very easy):
    - Minor UI adjustments.
    - Adjust existing API parameters.
    - Add front-end prompts or text.
- 5 points (extremely difficult):
    - It is necessary to add new underlying data structures or refactor the existing architecture.

    - New privacy control modules or encryption mechanisms need to be developed.
    - It requires end-to-end cloud collaboration, multi-team coordination, and long-cycle iteration.

(Example: Establishing an independent "local privacy sandbox" → The concept is feasible, but implementation is extremely difficult)

(4) Impact on user experience (1-5 points, suggestions for the UI layer)

Definition: To what extent would implementing this suggestion improve the user experience?

Rating example:

- 1 point (little improvement or likely to cause problems)
    - The user's steps have neither been reduced nor made clearer.
    - A more complex UI and more fragmented information actually increase cognitive load.
- 5 stars (Significantly improves user experience)
    - The interaction process is more intuitive, making it easier for users to understand and operate.
    - Clearer permission prompts and more readable information reduce misunderstandings and anxiety.
    - It helps users complete operations quickly without creating extra steps or burdens.

Step 2: Conduct in-depth discussions on the proposed solutions.

We will discuss each option in turn, with each option taking about 5 minutes.

The discussion will be structured as follows. Please try to focus your remarks on these three aspects:

- Effectiveness: What impact will it have on performance, user experience, and security?
- Technical feasibility: Can this solution be implemented within the existing technological framework? What technical components, algorithms, or systems are required?
- Technical challenges and limitations: What problems might be encountered? Are there limitations related to computing resources, model size, or access restrictions?

I will also guide and remind everyone to focus on the key points during the process of each solution. Meanwhile, we have designated personnel to record the technical details and key points of each solution. Now let's start with the first solution. Please share your thoughts on the technical feasibility of this solution.

Summary (5 minutes)

Okay, our discussion is coming to an end.

Let me quickly summarize the results of today's discussion on the six suggestions:

(Brief summary: feasibility, challenges, consensus)

Our current general assessment of these proposals is as follows:

(Which solutions can be further developed? Which solutions currently require more data, further technical verification, or additional exploration?)

If anyone has anything to add to today's conclusions, we can set aside a little more time to discuss it.

If not, then this discussion ends here. Thank you all very much for your participation and in-depth contributions!