Participatory Design Study about Privacy Enhancing Technologies for Wearable Activity Tracker Data-Sharing

Noé Zufferey[1], Kavous Salehzadeh Niksirat[1,2], Mathias Humbert[1], Kévin Huguenin[1]

[1]ISPlab - University of Lausanne
[2]EPFL

UNIL | Université de Lausanne

Background

- **Wearable activity trackers (WATs)** more and more numerous.
- Life and activity monitoring.
- Risk of malicious and curious usage.
- **Users can share their data** with **third-party apps (TPAs)**.
- **Users are not aware** of all the data they **actually** share and to who they share it.
- **Users do not well understand** how the WAT data-sharing ecosystem works.
- We need to design **new privacy enhancing technologies (PETS)** to protect their privacy.

Research Questions

What solutions will be suggested by WAT users to

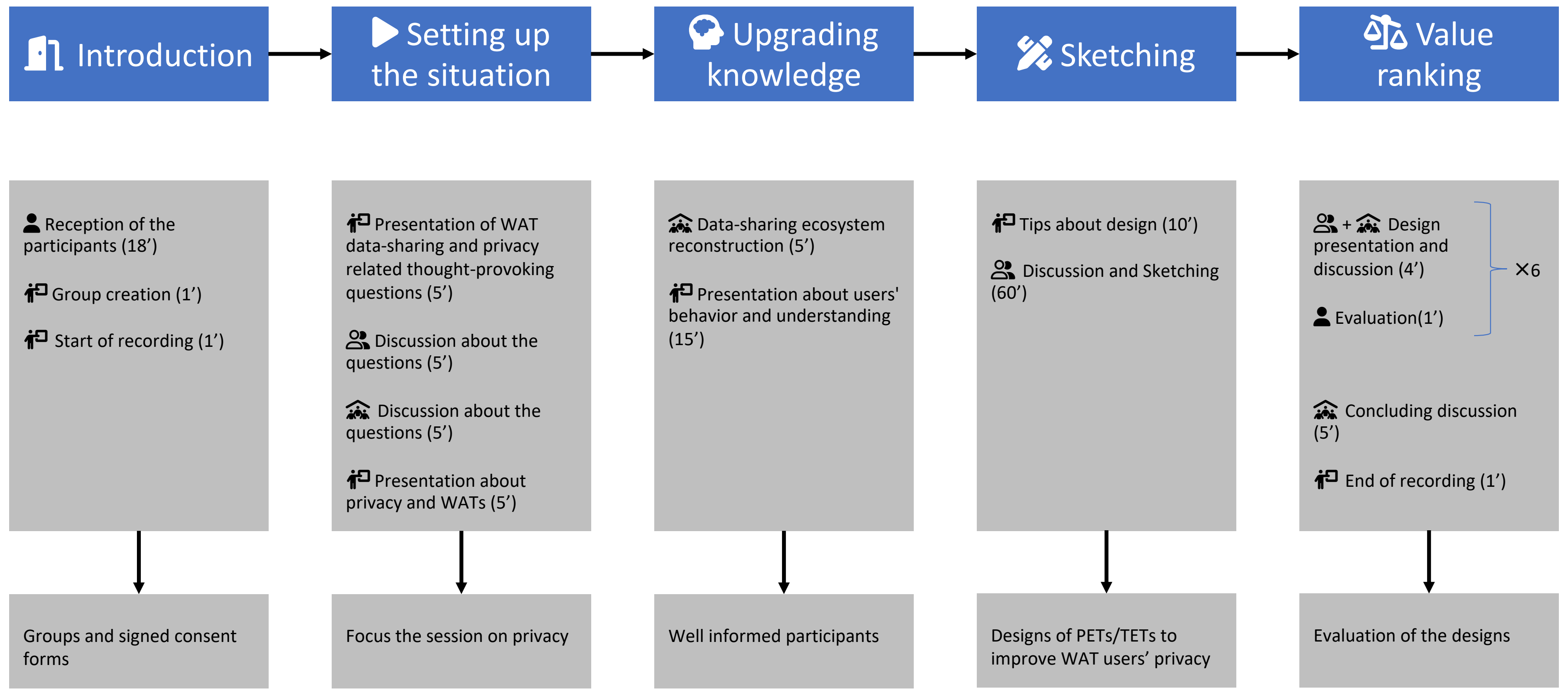
- help them **better manage data sharing** to avoid risky behaviors for privacy?
- help them **better understand the data-sharing** process?
- **obfuscate/aggregate their data** in order to improve their privacy?

Methodology

3 participatory design sessions with a total of 26 WAT users

Each session with:

- **3 groups** of 2-3 WAT users
- Presentation about WAT data sharing and discussion about the privacy risks.
- Knowledge upgrade of how the data-sharing eco-system works.
- Presentation of the current literature status about the problems related to user data-sharing habits and understanding.
- PET Sketching (2-3 design for each group).
- Evaluation of the designs. (Feasibility, Effectiveness, Adoption, Usability)



Introduction → Setting up the situation → Upgrading knowledge → Sketching → Value ranking

Introduction: Reception of the participants (18’); Group creation (1’); Start of recording (1’) → Groups and signed consent forms

Setting up the situation: Presentation of WAT data-sharing and privacy related thought-provoking questions (5’); Discussion about the questions (5’); Discussion about the questions (5’); Presentation about privacy and WATs (5’) → Focus the session on privacy

Upgrading knowledge: Data-sharing ecosystem reconstruction (5’); Presentation about users' behavior and understanding (15’) → Well informed participants

Sketching: Tips about design (10’); Discussion and Sketching (60’) → Designs of PETs/TETs to improve WAT users’ privacy

Value ranking: + Design presentation and discussion (4’); Evaluation(1’) ×6; Concluding discussion (5’); End of recording (1’) → Evaluation of the designs

Individual activities, Group activities, Global Activities (all together conducted by the main investigator), Presentations (by the main investigator)

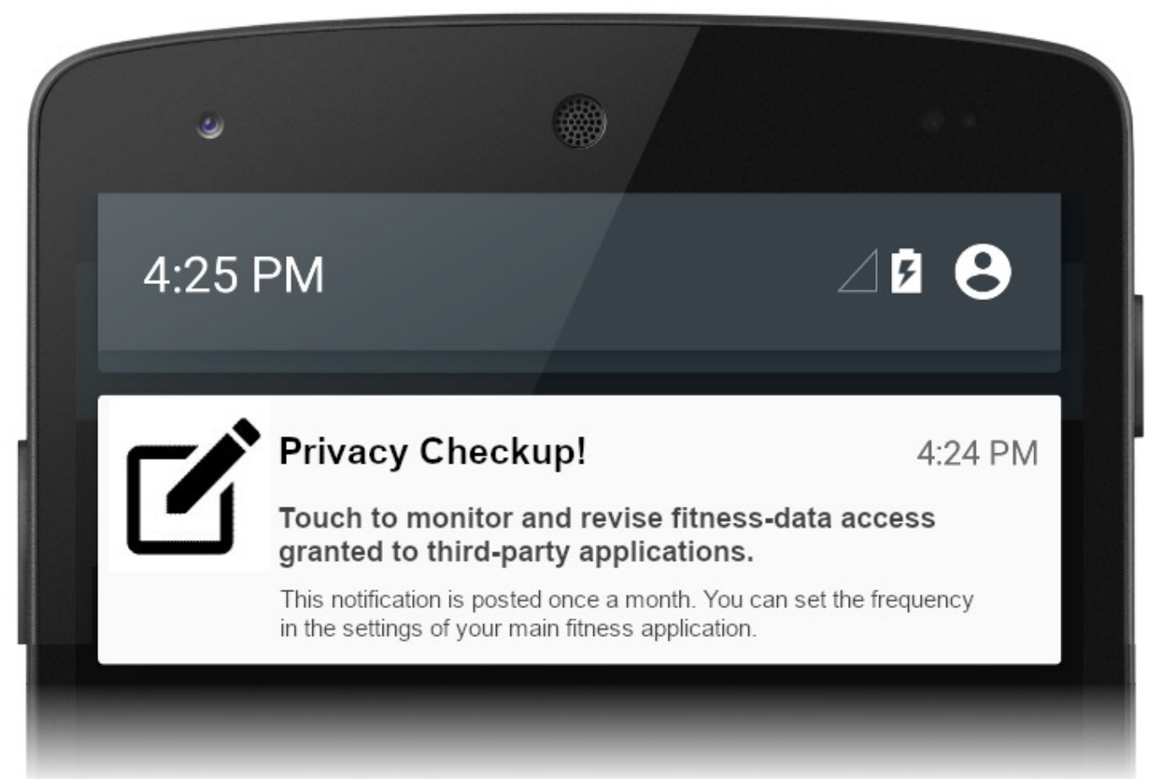
After the sessions:

- Coding of the different proposed designs to create PET categories.
- Evaluation of these categories by information security and cybersecurity experts using the same criteria than for the participants evaluations.

Results

7 different PET categories

- Sharing only part of the data
  - Specific timeframe ✓
  - Context ✓
- Transparency & Visualization
  - Explore the shared data and the different TPAs
  - Data sharing logs
  - TPA services usage statistics
- Reminders and Notifications
  - "Opt-in" data access renewal ✓
  - "Opt-out" data access renewal
  - Only information



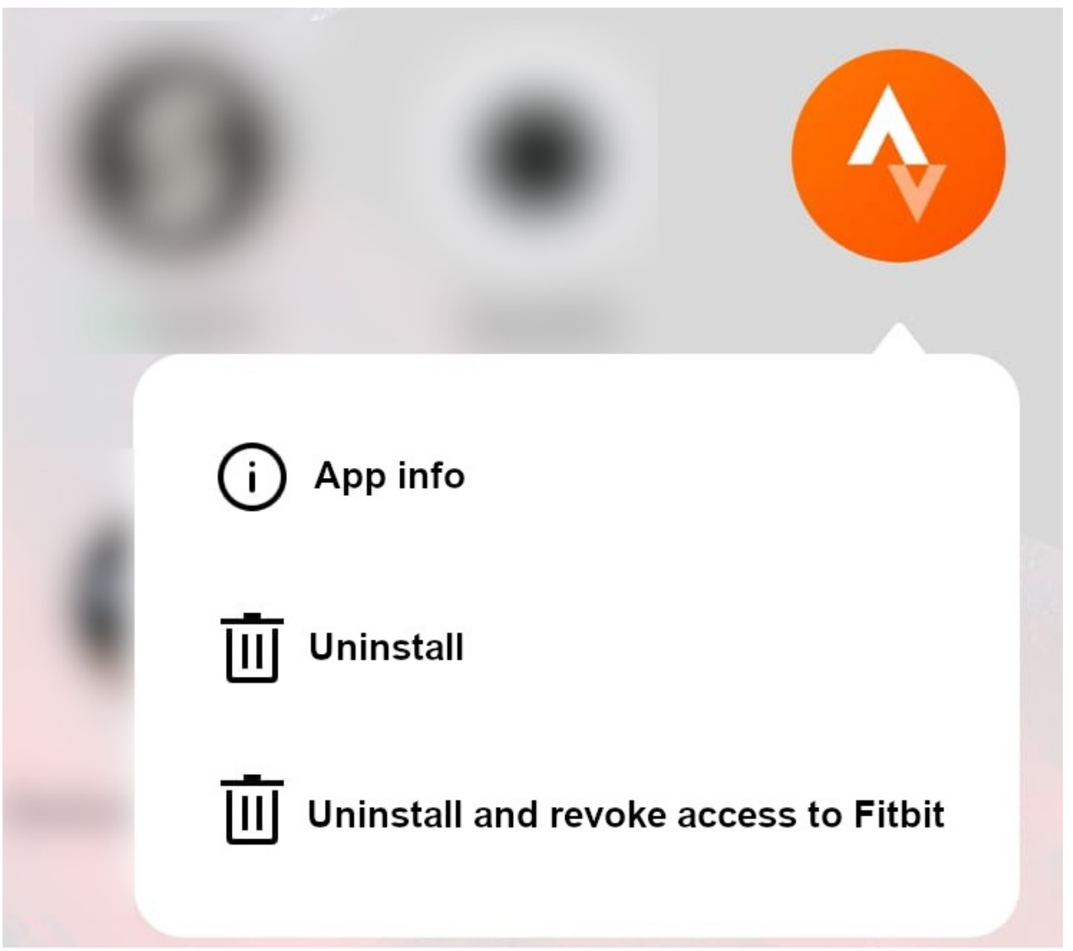
4:25 PM

Privacy Checkup! 4:24 PM

Touch to monitor and revise fitness-data access granted to third-party applications.

This notification is posted once a month. You can set the frequency in the settings of your main fitness application.

- TPAs limit
  - Cannot share with more than *x* TPAs
- Centralization & Verification
  - Specific app store
  - Plugins (no more TPAs, but plugins in the main app)
- Sensitization, Education
  - Video
  - Interactive consent form
- TPA's mobile app uninstallation/access revocation assistance
  - revoke access when uninstalling TPA’s service ✓
  - Automatic revocation (e.g., after a certain time of non-use)
  - send a request to remove data from TPA’s servers (GDPR) ✓



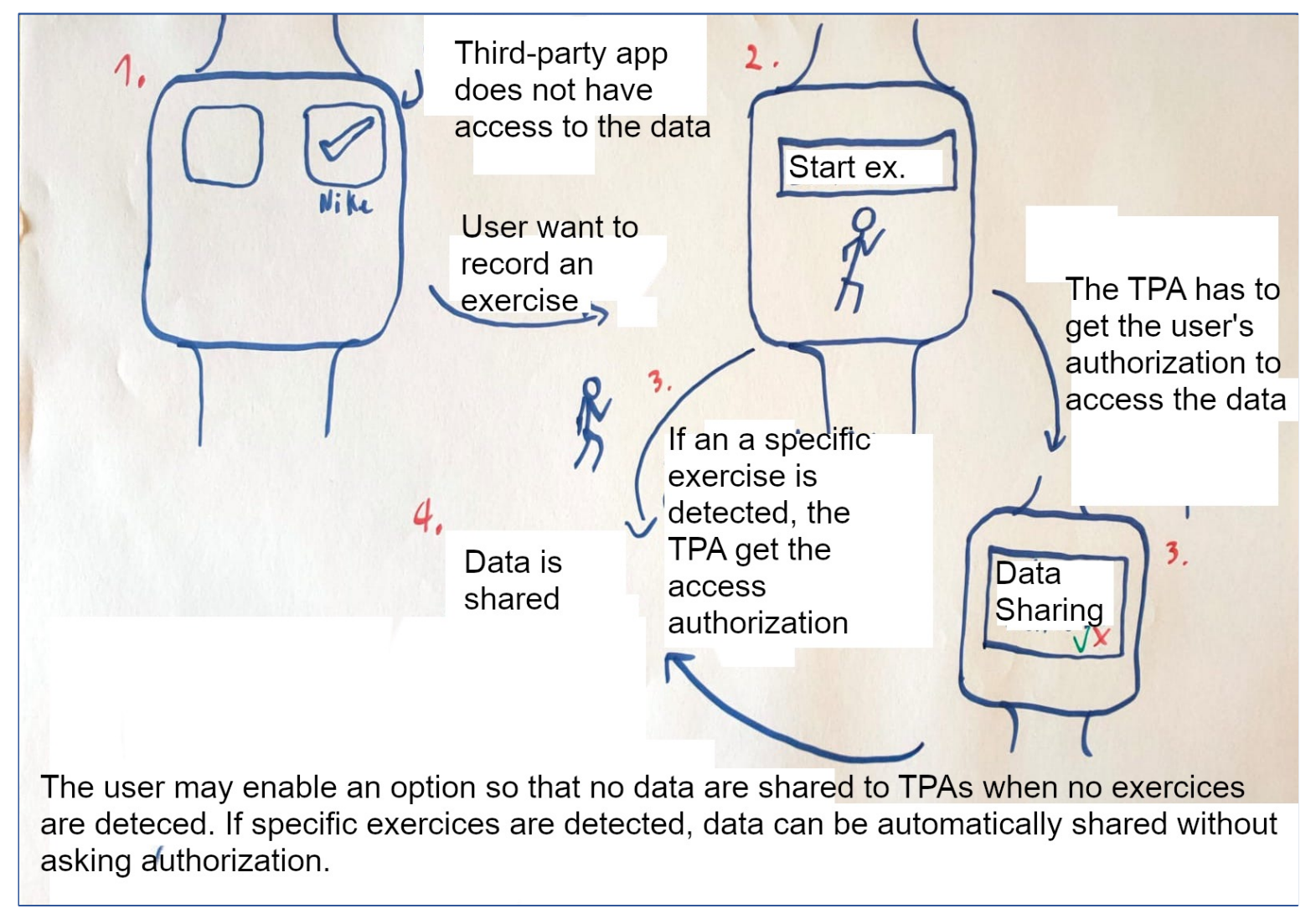
App info

Uninstall

Uninstall and revoke access to Fitbit

After analyzing all the categories and the results of both participants and expert evaluations, we so propose a global PET for data-sharing including multiple of these functionalities (✓) to which we propose to add **temporal aggregation** (option to share the data aggregated to the minute, hour, or day).

Design Examples



Third-party app does not have access to the data

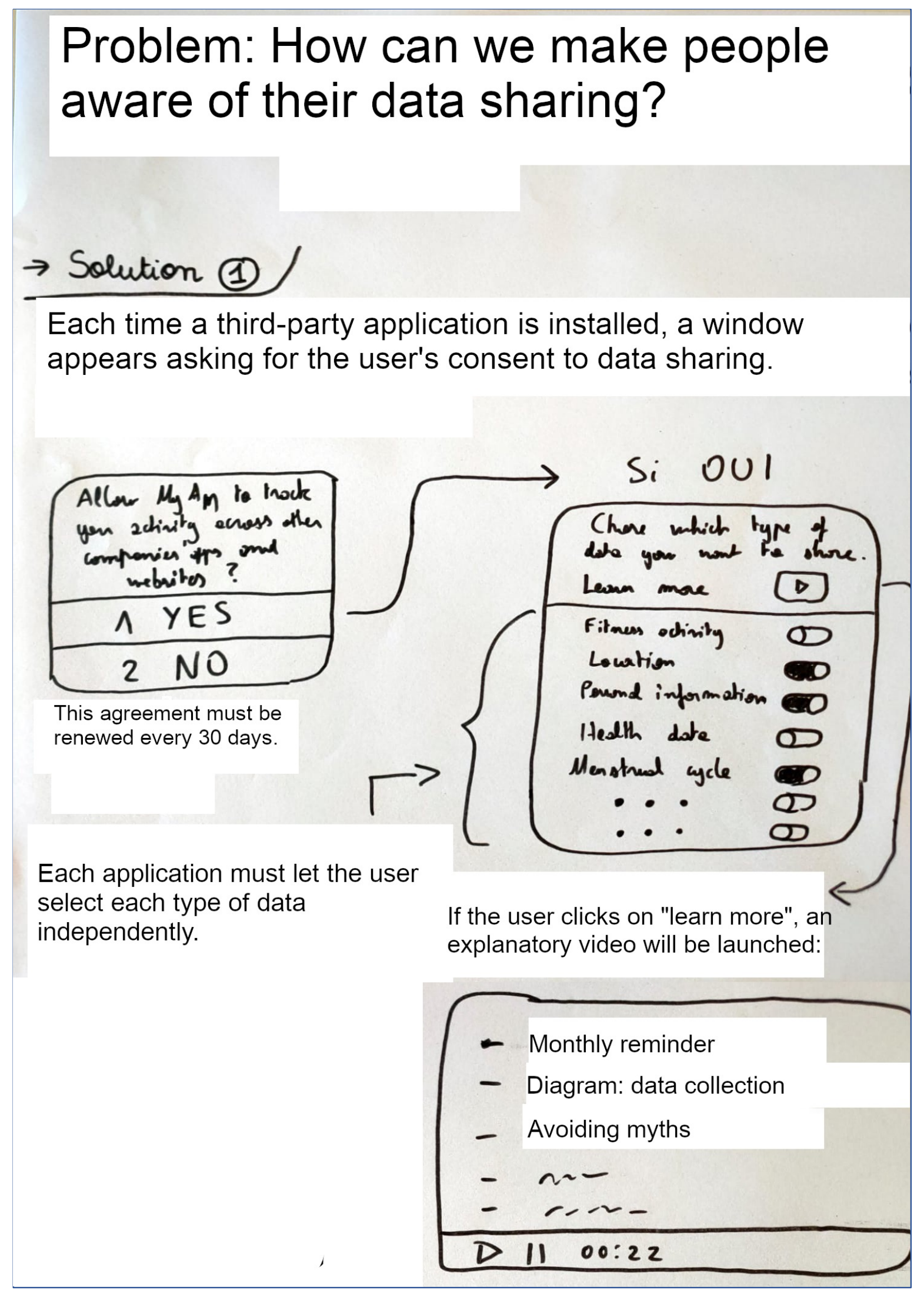
User want to record an exercise

The TPA has to get the user's authorization to access the data

If an a specific exercise is detected, the TPA get the access authorization

Data is shared

The user may enable an option so that no data are shared to TPAs when no exercices are deteced. If specific exercices are detected, data can be automatically shared without asking authorization.



Problem: How can we make people aware of their data sharing?

→ Solution ①

Each time a third-party application is installed, a window appears asking for the user's consent to data sharing.

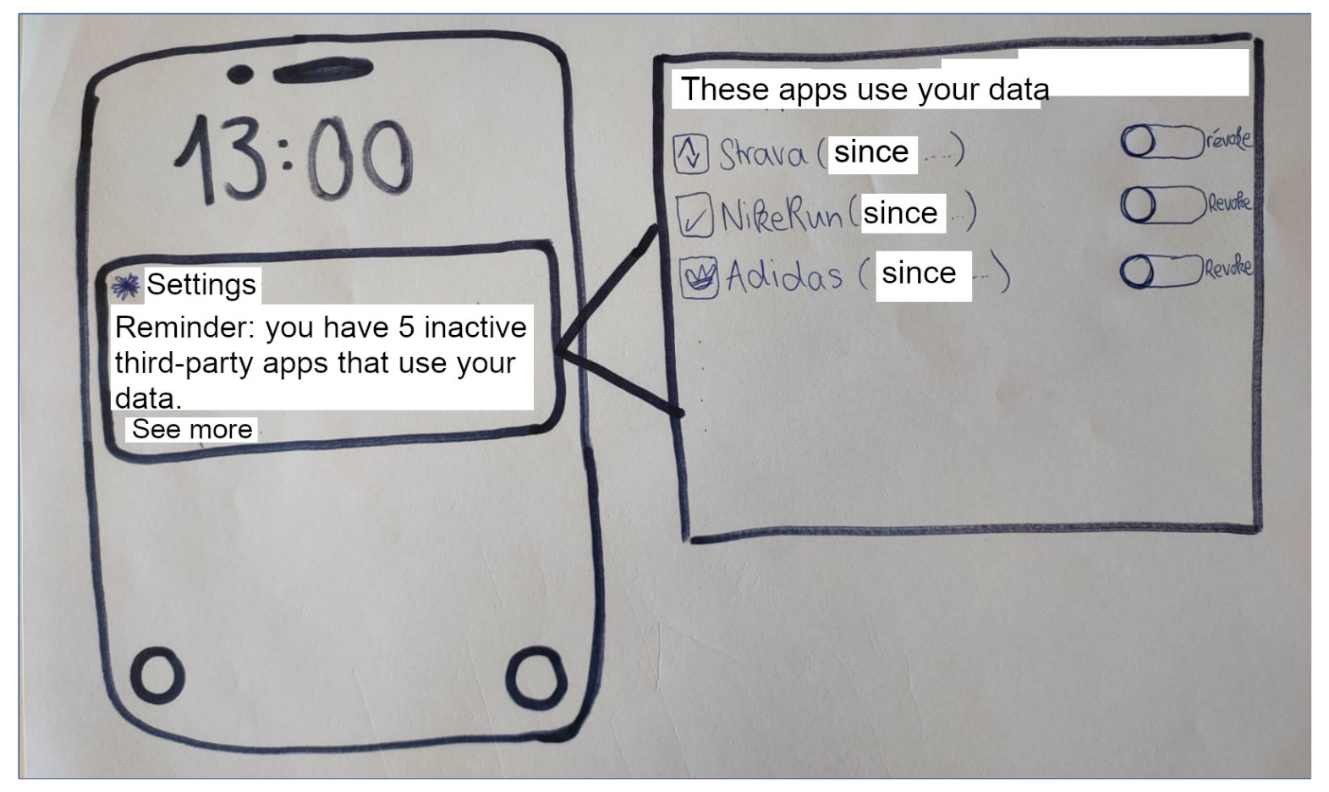
Allow My App to track your activity across other companies' apps and websites?
1 YES
2 NO
Si OUI
Chose which type of data you want to share.
Learn more
Fitness activity
Location
Personal information
Health data
Menstrual cycle
00:22

This agreement must be renewed every 30 days.

Each application must let the user select each type of data independently.

If the user clicks on "learn more", an explanatory video will be launched:

- Monthly reminder
- Diagram: data collection
- Avoiding myths



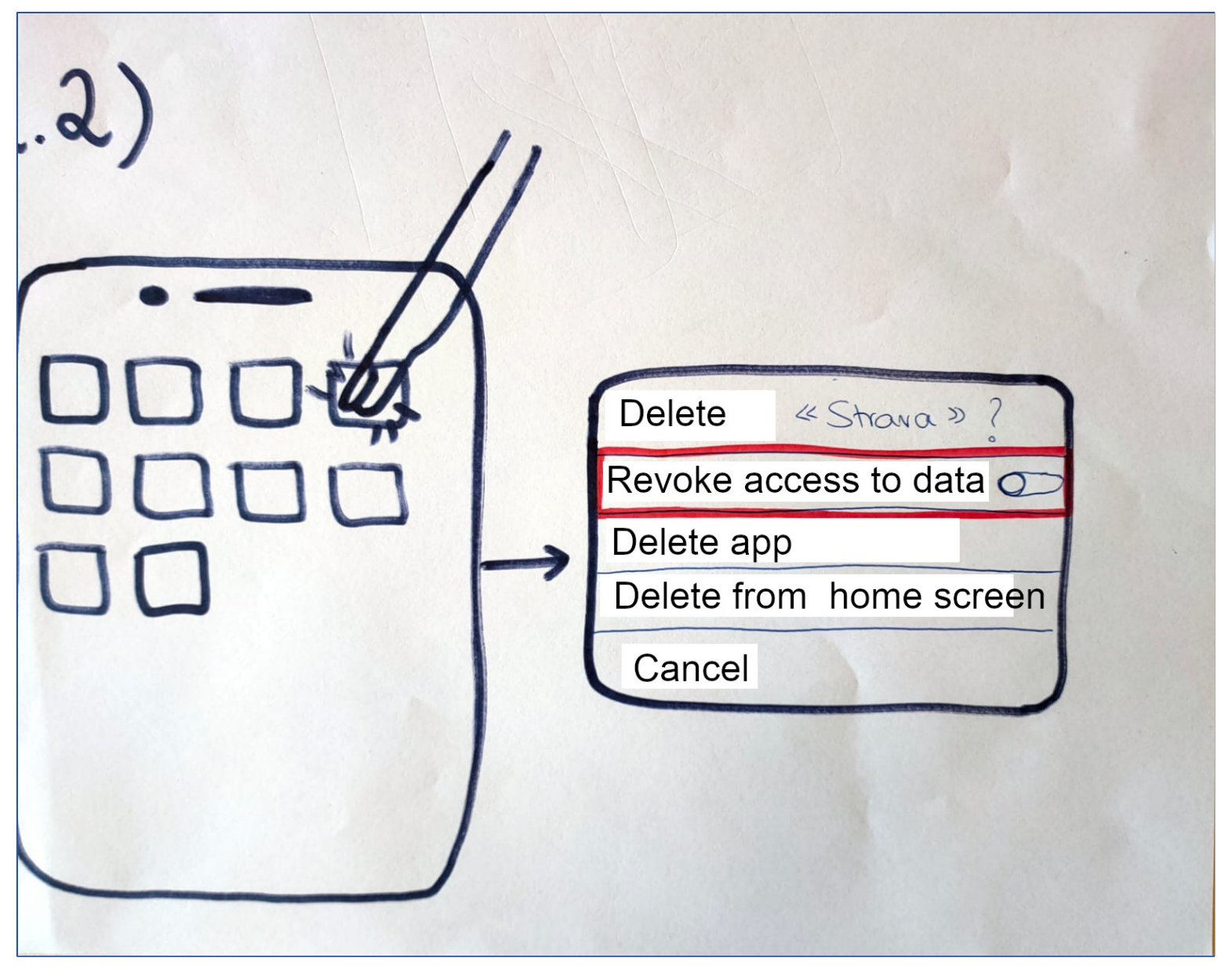
Settings

Reminder: you have 5 inactive third-party apps that use your data.

See more

These apps use your data

since
since
since



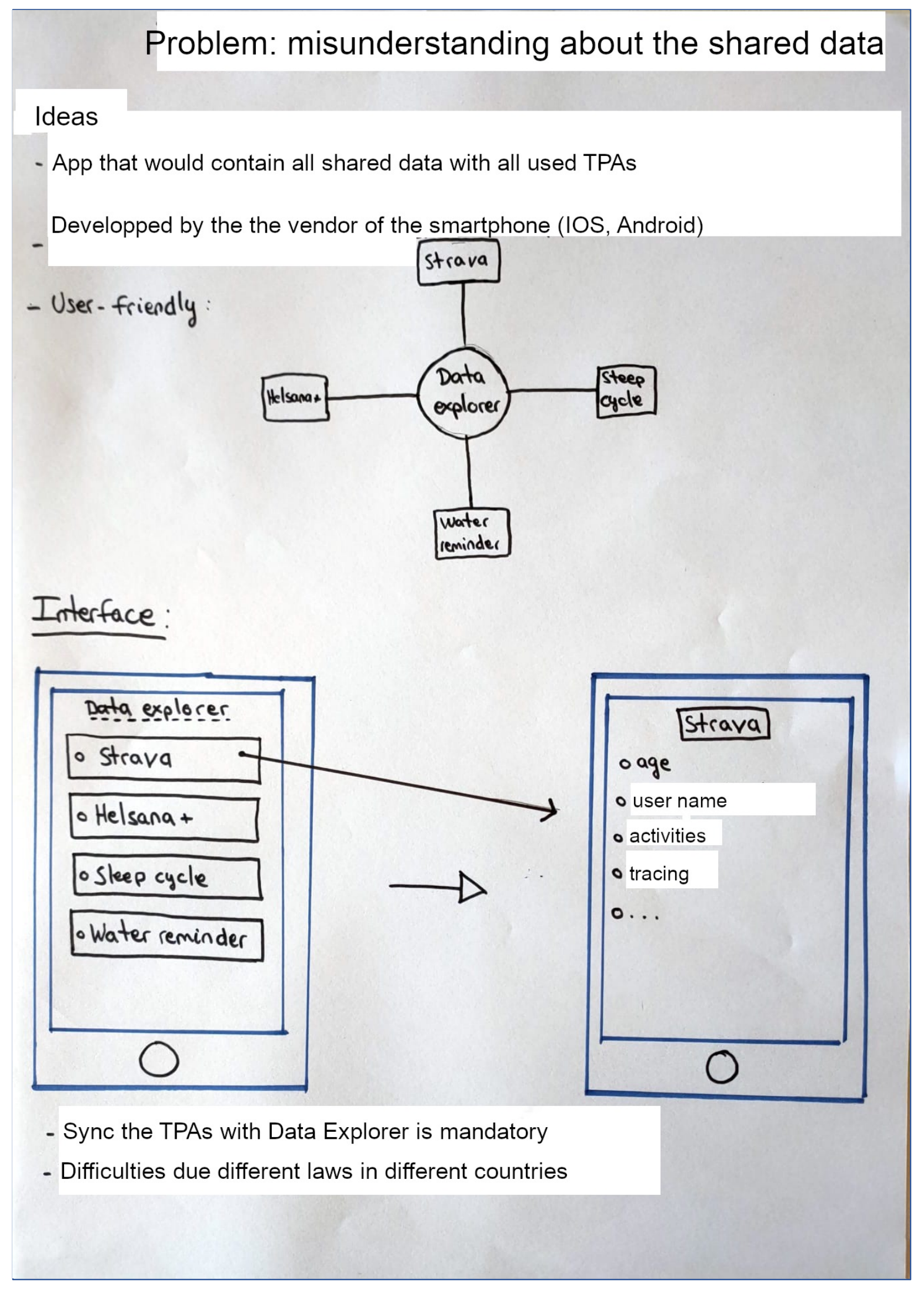
Delete

Revoke access to data

Delete app

Delete from home screen

Cancel



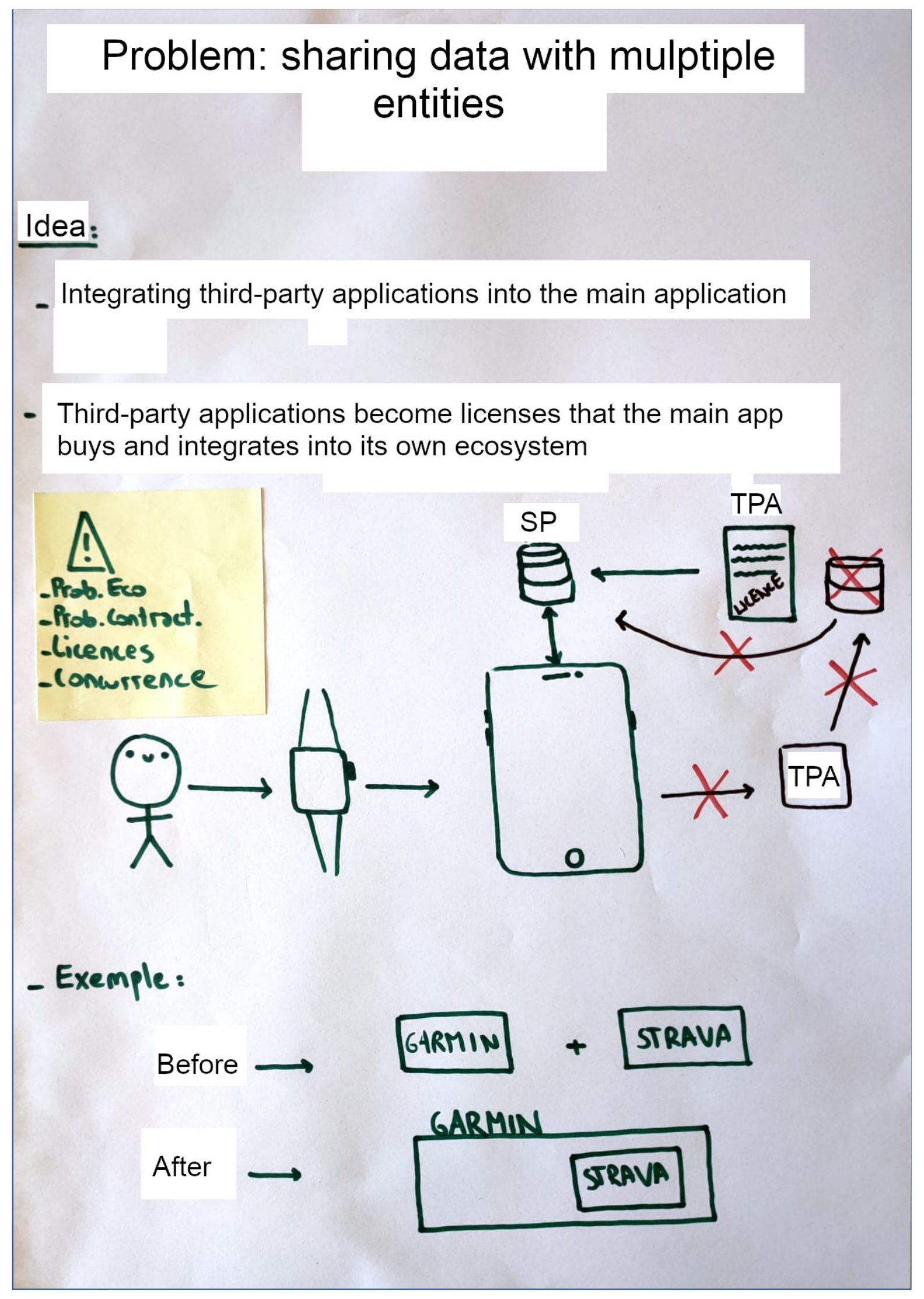
Problem: misunderstanding about the shared data

Ideas

- App that would contain all shared data with all used TPAs
- Developped by the the vendor of the smartphone (IOS, Android)

user name
activities
tracing

- Sync the TPAs with Data Explorer is mandatory
- Difficulties due different laws in different countries



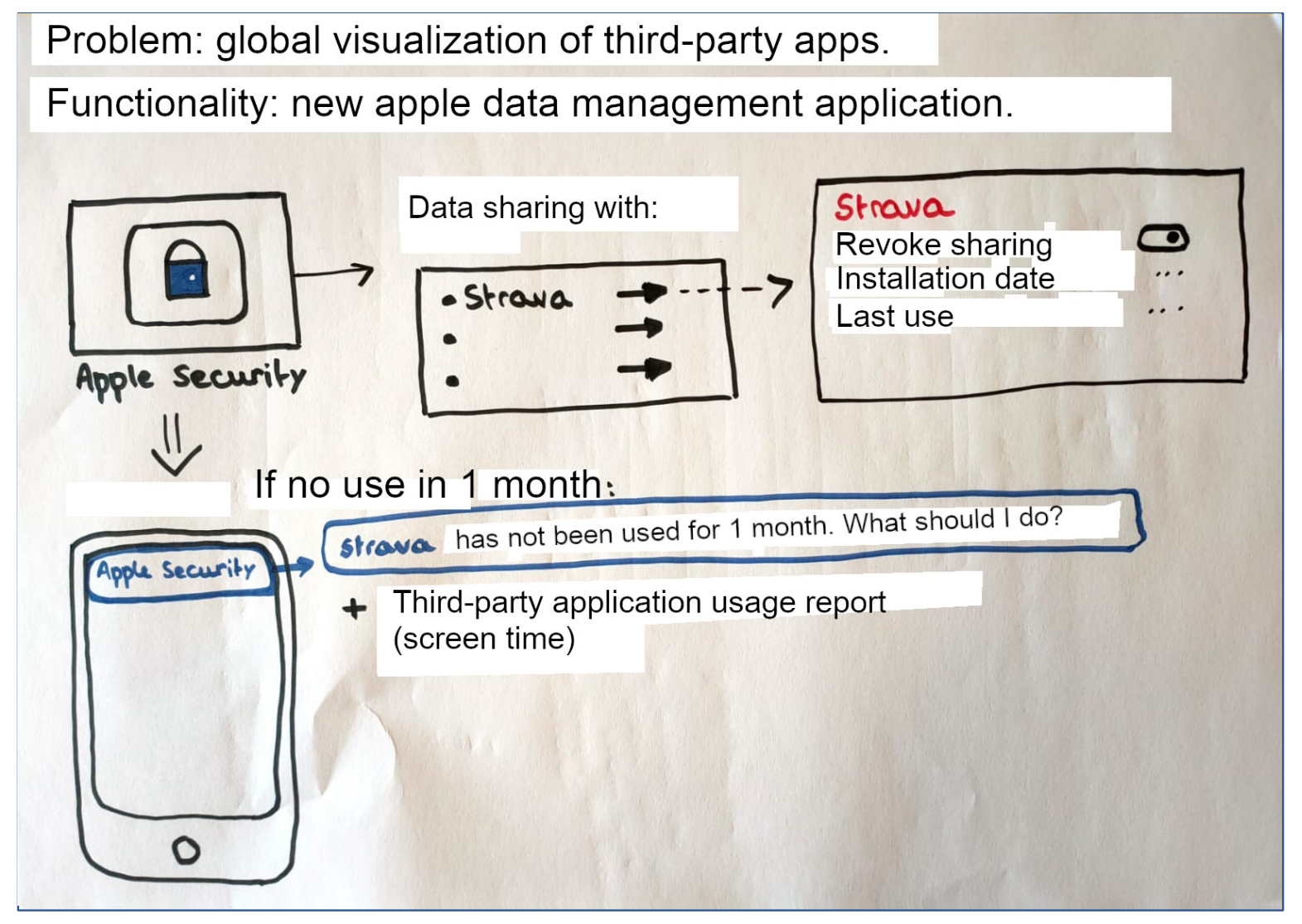
Problem: sharing data with mulptiple entities

Idea:

- Integrating third-party applications into the main application
- Third-party applications become licenses that the main app buys and integrates into its own ecosystem

Before

After



Problem: global visualization of third-party apps.

Functionality: new apple data management application.

Data sharing with:

Revoke sharing

Installation date

Last use

If no use in 1 month:

has not been used for 1 month. What should I do?

+ Third-party application usage report (screen time)