TOWARDS TRANSPARENCY IN THE INTERNET OF THINGS

Stephan Escher, Benjamin Weller, Stefan Köpsell, and Thorsten Strufe

stephan.escher@tu-dresden.de

Annual Privacy Forum
22. October 2020

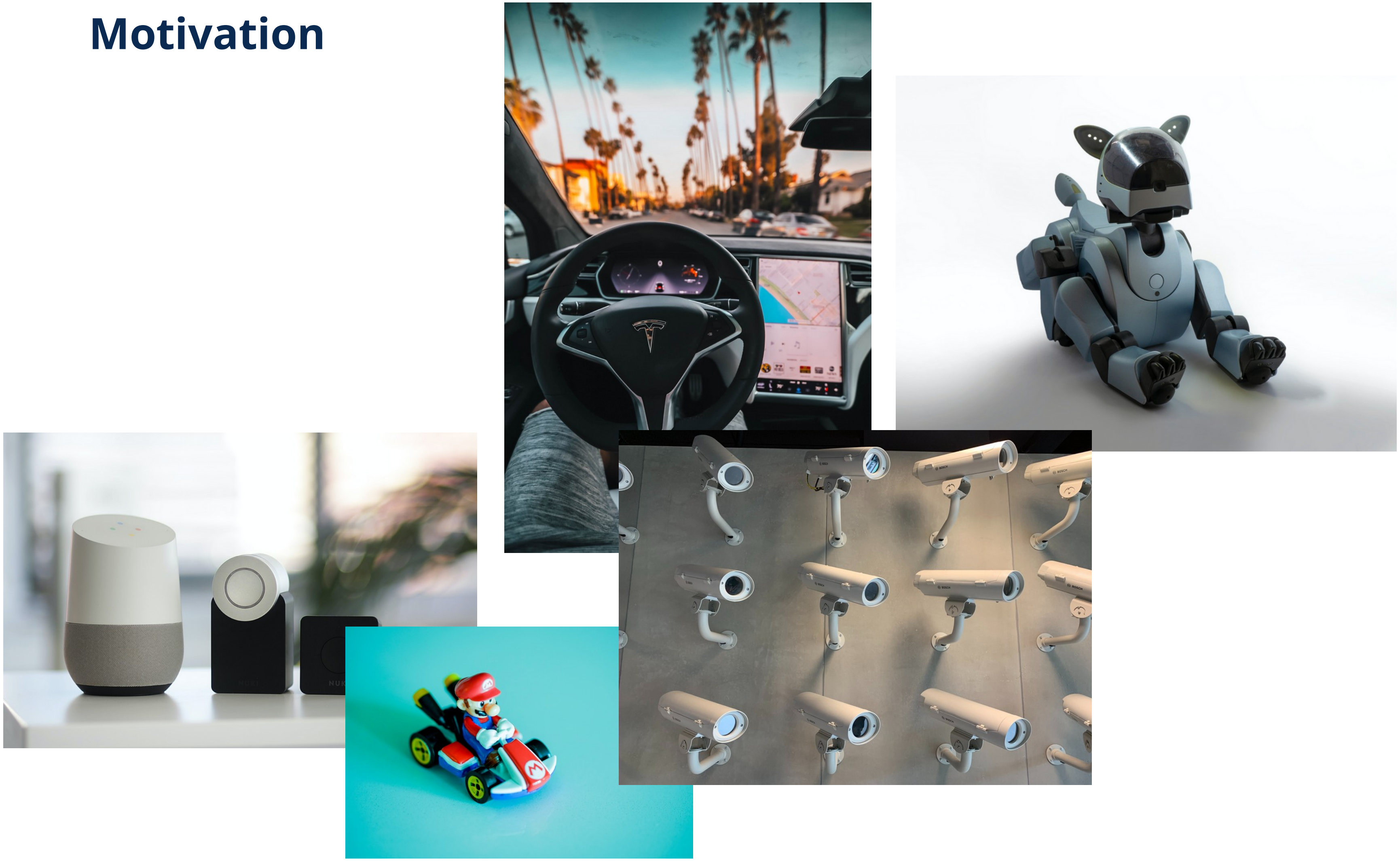
Motivation

Motivation

Motivation

Motivation

Motivation



Motivation

Motivation

Motivation – The Privacy Issue

- IoT devices become almost invisible

  → Recognition impossible

Motivation – The Privacy Issue

- IoT devices become almost invisible

  → Recognition impossible

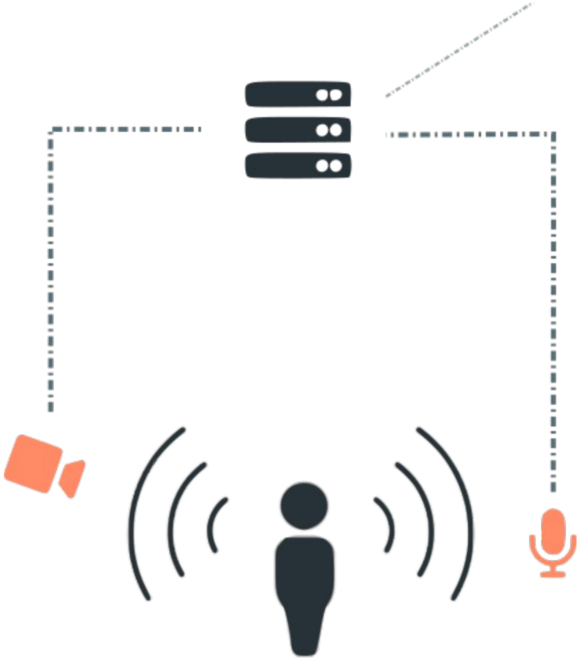
- No interface to convey privacy policies

Motivation – The Privacy Issue

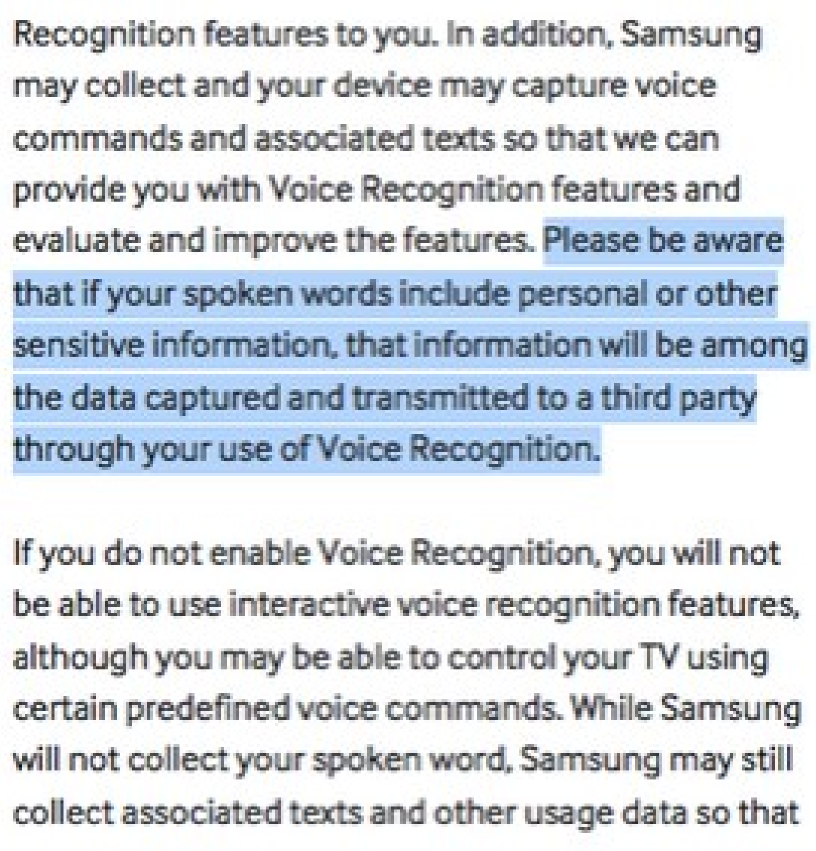
- IoT devices become almost invisible

  → Recognition impossible

- No interface to convey privacy policies
- Recording and processing of biometric data
- External processing



Motivation – The Privacy Issue



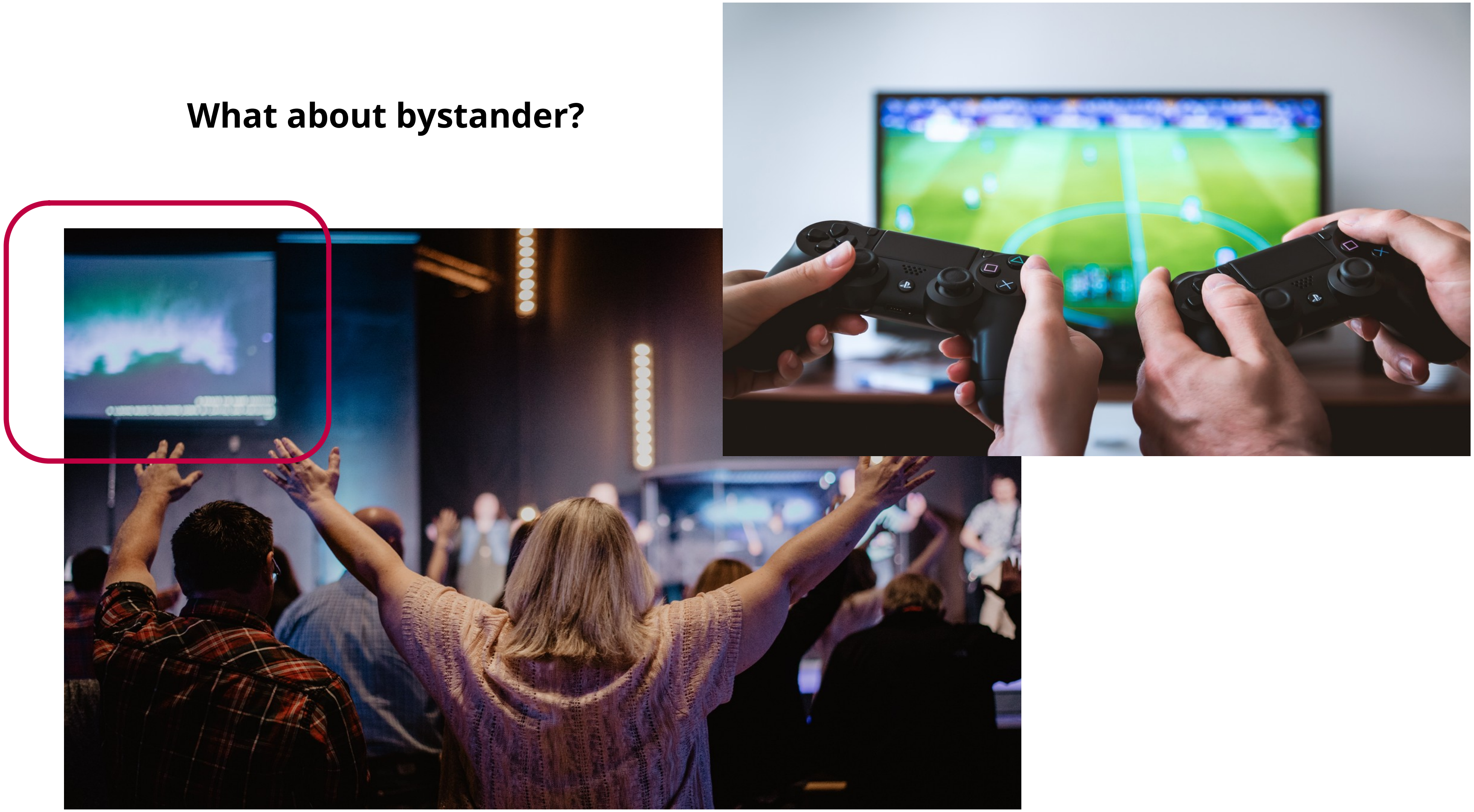
Recognition features to you. In addition, Samsung may collect and your device may capture voice commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features. Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.

If you do not enable Voice Recognition, you will not be able to use interactive voice recognition features, although you may be able to control your TV using certain predefined voice commands. While Samsung will not collect your spoken word, Samsung may still collect associated texts and other usage data so that

Samsung Smart TV - '15

Motivation – The Privacy Issue

What about bystander?



Motivation – The Privacy Issue

→ **Foreign Control over personal data of bystander**

Motivation – The Privacy Issue

→ **Foreign Control over personal data of bystander**

→ Needed: Solution for **Transparency** (and Intervention) in IoT

- Focus: IoT which capture biometrical data (audio, video)
- Focus: Smart Home

Motivation – Scenario

- Bystander which are confronted with IoT devices
- IoT devices could capture audio and / or video (biometrical data)
- User has no possibilities to detect or prevent capturing of his data
- Needed: Transparency solutions

HELLO, WELCOME TO OUR HOUSE!
THANKS FOR INVITING US!
ALEXA, ORDER TWO TONS OF CREAMED CORN.
ALEXA, CONFIRM PURCHASE.

WHEN VISITING A NEW HOUSE, IT'S GOOD TO CHECK WHETHER THEY HAVE AN ALWAYS-ON DEVICE TRANSMITTING YOUR CONVERSATIONS SOMEWHERE.

Towards Transparency – Device Recognition

1. How can smart devices be recognized?

Towards Transparency – Device Recognition

- Technical / external approaches may not detect all devices

- Assuming regulation

  → Devices have to identify themselve

  → Transmission of privacy policies etc. to the user

Towards Transparency – Device Recognition

- According to GDPR …
  - „It should be **transparent** to natural persons that **personal data concerning them are collected**, used, consulted or otherwise processed and to what extent the personal data are or will be processed.“

    (GDRP, recital 39, par. 2)
  - „The principle of **transparency** requires that **any information and communication** relating to the processing of those personal data **be easily accessible and easy to understand**, and that clear and plain language be used.“

    (GDPR, recital 39, par. 3)

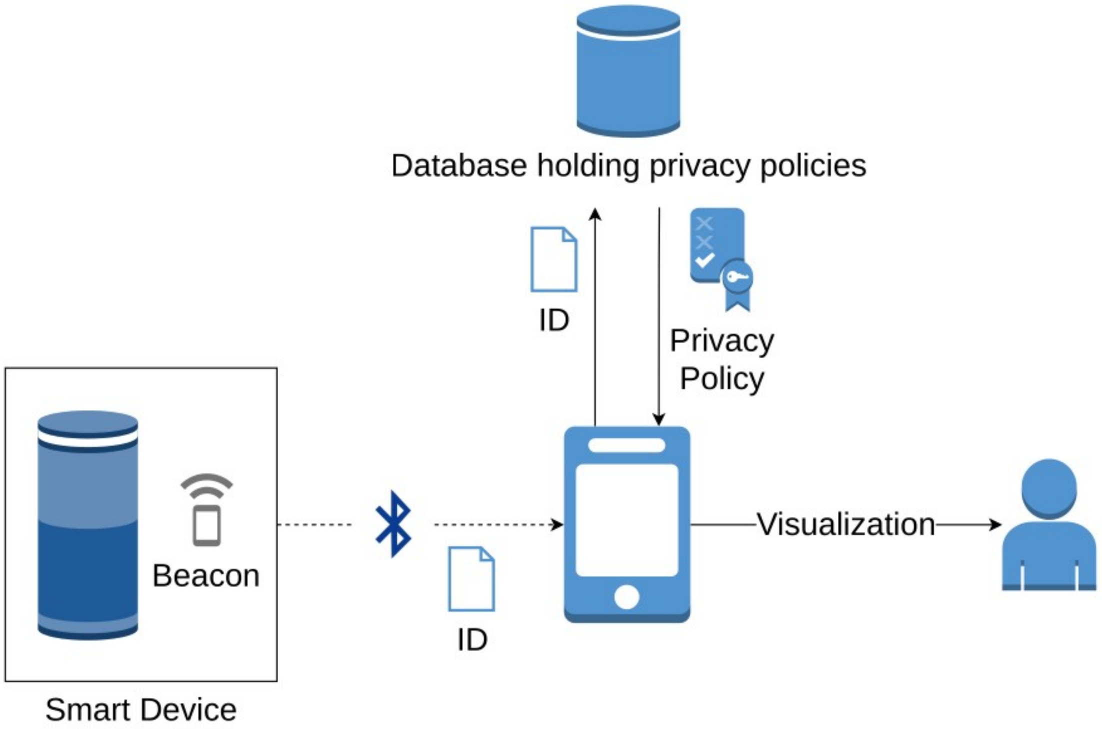
Towards Transparency – Information Transmission

2. How can privacy information be transmitted to the user?

Towards Transparency – Information Transmission

- Digital communication – usage of smart devices / wearables
  → daily usage
- Direct vs. Indirect communication with smart devices
  → direct communication, broadcast
- Communication channel
  → Bluetooth LE
- Information encoding
  → by reference

Towards Transparency – Information Transmission



Towards Transparency – Information Content

3. Which information should be transmitted?

Towards Transparency – Information Content

- Device information: data capturing (audio, video), type, manufacturer, …
- Data processor / manufacturer information – privacy policies

- Excluded:
  - Data controller / owner
  - Third party apps and their privacy policies
  - Device location
  - …

Towards Transparency – Information Presentation

4. How could this information be presented?

Towards Transparency – Visualization

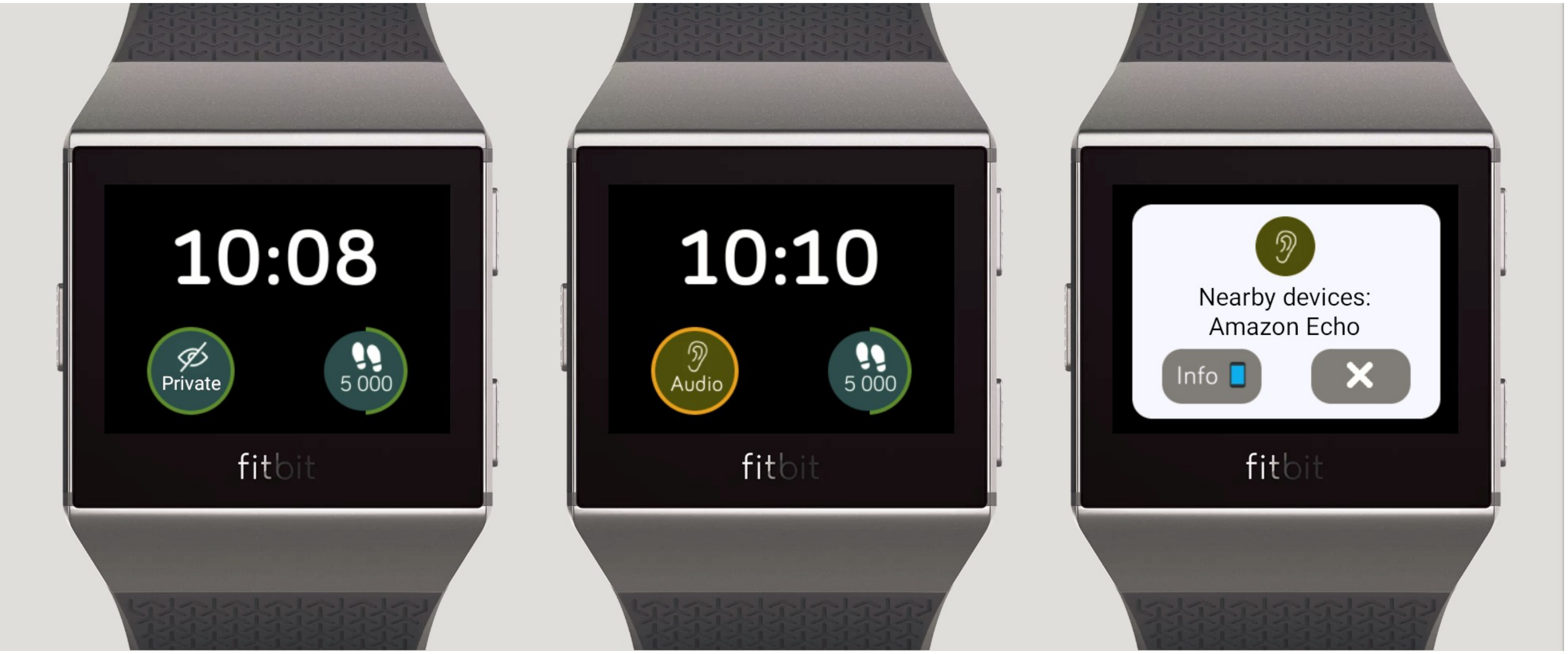
- Daily usage: Balance between information richness and usable interface

- Idea: Split information into hiearchy
  - High level: Aggregated information
  - Low level: Detailed information

Hierarchy

1. Device count, recording channels (audio, video), privacy grade
2. Device type (e.g. smart speaker, smart tv, …)
3. Exact device type with corresponding privacy policies

First Prototype

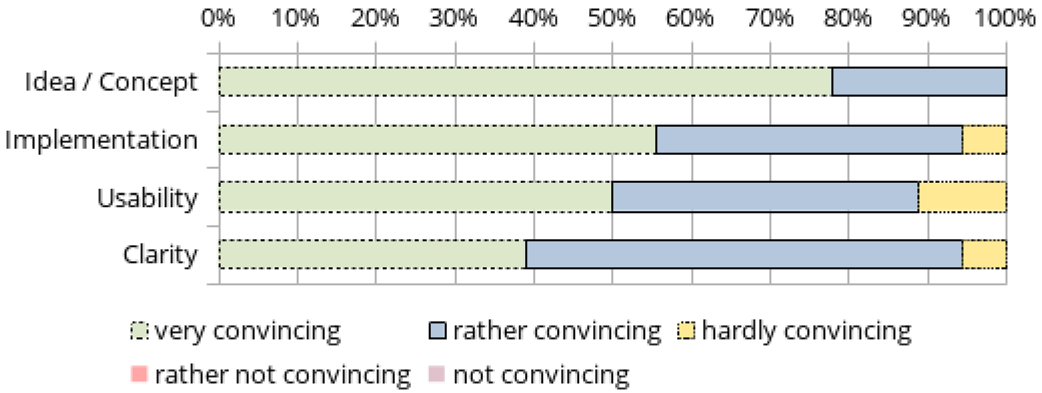


Preliminary Evaluation

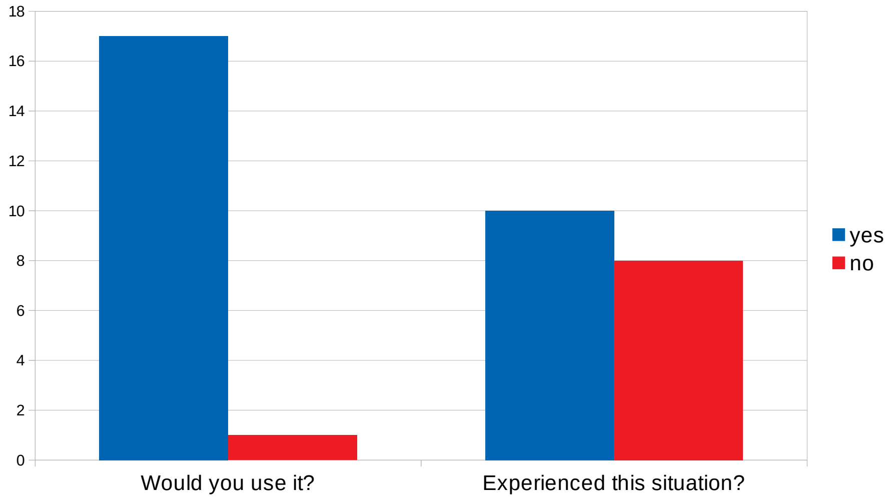
- 18 participants
- Setup: Smart watch solution and Amazon Echo
- Implementation:
  - Introduction to smart devices and our work
  - Hands-on with smartwatch
  - Completion of questionaire

Age	10-20	20-30	30-40	40-50	50-60
Count	5	5	2	4	2

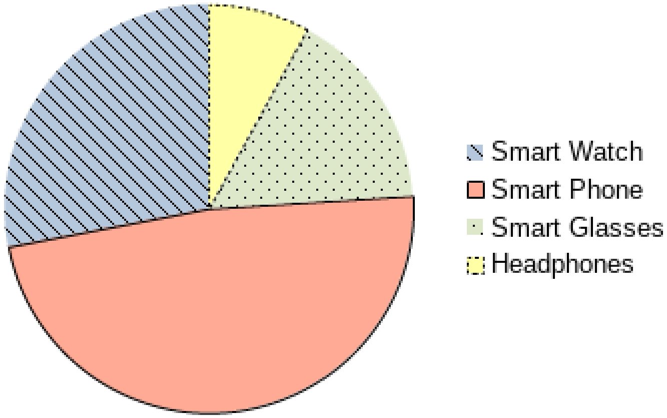
Preliminary Evaluation



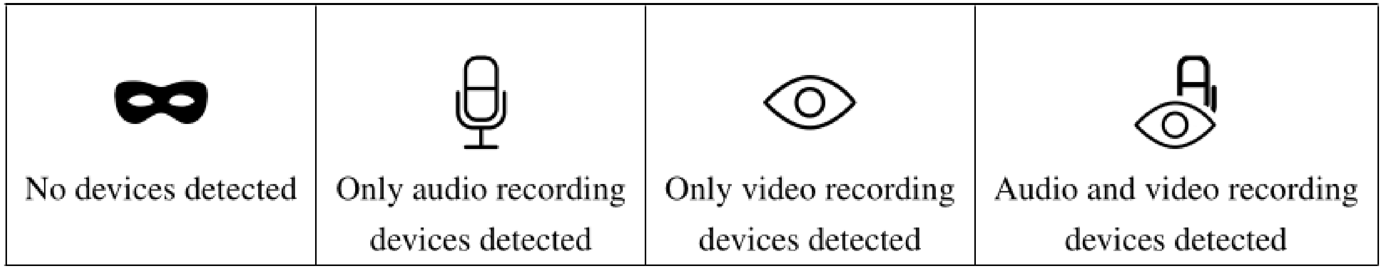
Preliminary Evaluation



Preliminary Evaluation

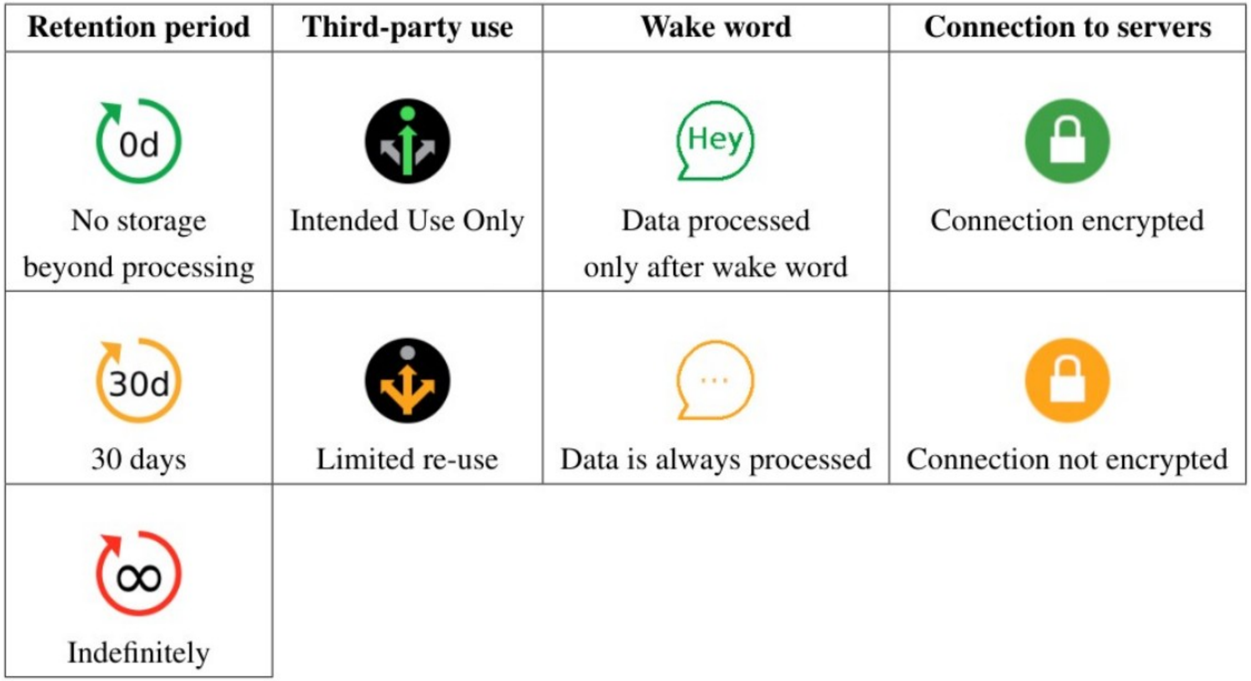


Improved Prototype – Information Visualization



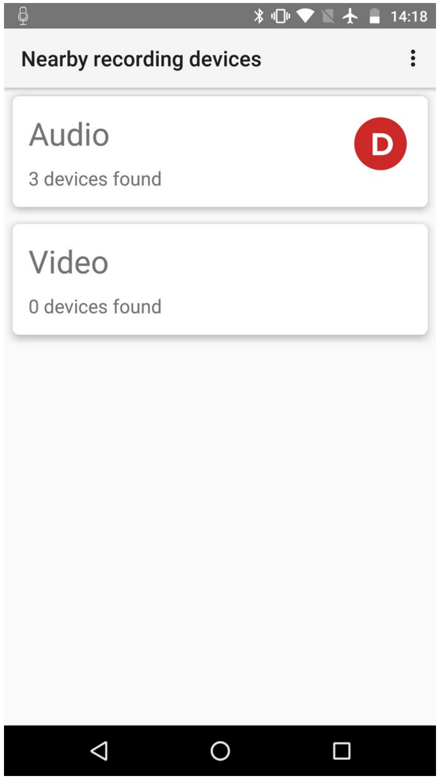
No devices detected	Only audio recording devices detected	Only video recording devices detected	Audio and video recording devices detected

Improved Prototype – Information Visualization



Retention period	Third-party use	Wake word	Connection to servers
0d No storage beyond processing	Intended Use Only	Hey Data processed only after wake word	🔒 Connection encrypted
30d 30 days	Limited re-use	··· Data is always processed	🔒 Connection not encrypted
∞ Indefinitely			

Improved Prototype – Android Implementation

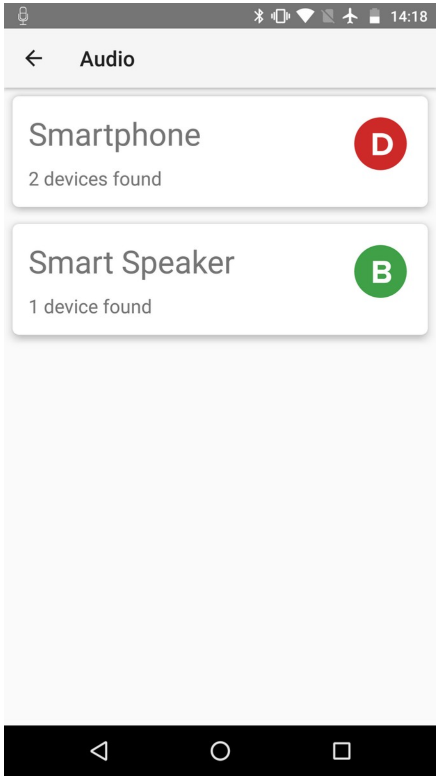


14:18

Nearby recording devices

Audio
3 devices found
D

Video
0 devices found

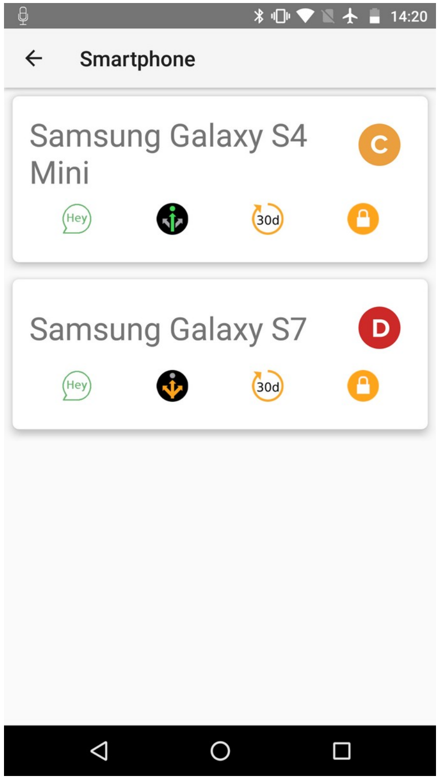


14:18

Audio

Smartphone
2 devices found
D

Smart Speaker
1 device found
B



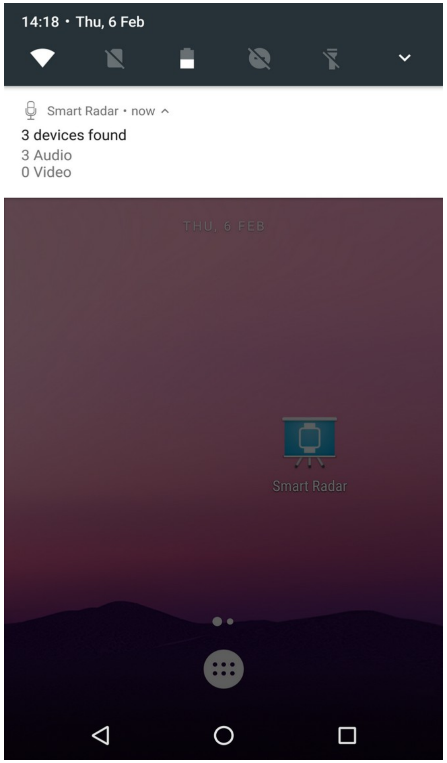
14:20

Smartphone

Samsung Galaxy S4 Mini
C
Hey 30d

Samsung Galaxy S7
D
Hey 30d

Improved Prototype – Android Implementation



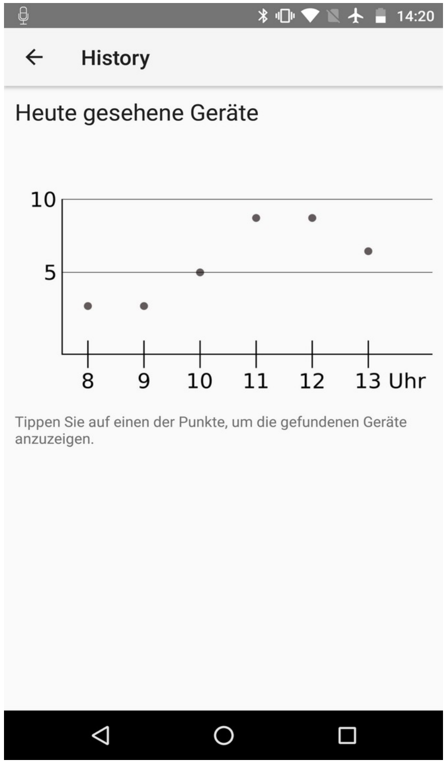
14:18 • Thu, 6 Feb

Smart Radar • now

3 devices found

3 Audio

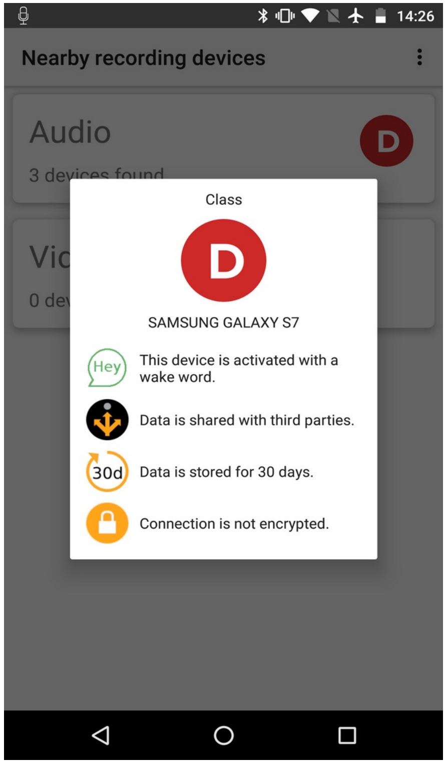
0 Video



History

Heute gesehene Geräte

Tippen Sie auf einen der Punkte, um die gefundenen Geräte anzuzeigen.



Nearby recording devices

Audio

3 devices found

Vi

0 dev

Class

SAMSUNG GALAXY S7

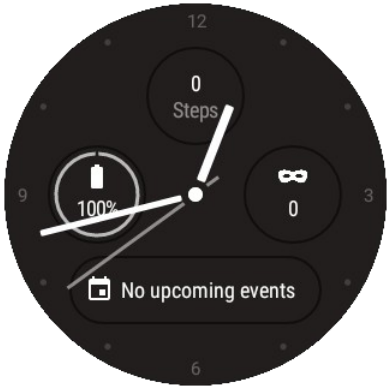
This device is activated with a wake word.

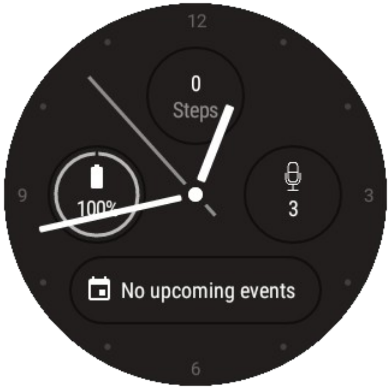
Data is shared with third parties.

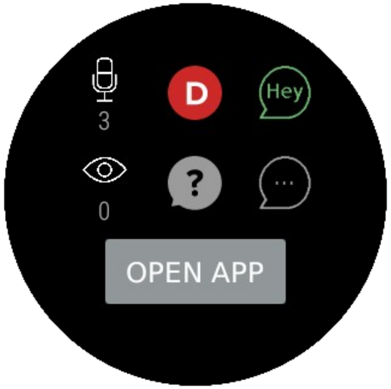
Data is stored for 30 days.

Connection is not encrypted.

Improved Prototype – Wear OS Implementation







Open Challenges

- BLE as communication channel
  - Range: video devices vs. BLE range
  - Daily usage: energy consumption of user devices
  - Technical Limitations (Cost, Robustness)
  - Moving IoT devices (smart cars, …)
- Privacy issues through BLE Ids for IoT device owner?
  - Tracking of wearables (AR glasses)
  - Detection of IoT devices – e.g. promotes theft?
  - …

Open Challenges

- Information content
  - Data controller / device owner
  - Third party apps
- Information visualization
  - Iconification of privacy policy information
  - Privacy abstraction to privacy grades (nutri score like)

Outlook

- Full evaluation of the concept
- Evaluation of impacts of transparency in IoT
- Usage analyses of the concept in everyday life
- Concepts for user-interaction

Thank you for your Attention

Images: Unsplash

Icons: Fontawesome, Freepik