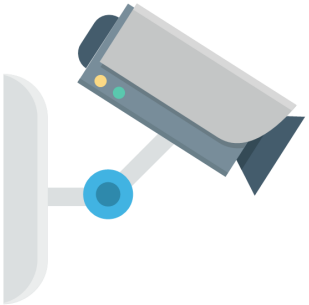
Privacy Expectations and Preferences in an IoT World

Pardis Emami-Naeini, Sruti Bhagavatula, Martin Degeling,
Hana Habib, Lujo Bauer, Lorrie Faith Cranor, Norman Sadeh

Carnegie Mellon University

DARPA

PERSONALIZED PRIVACY ASSISTANT PROJECT







Do you know:

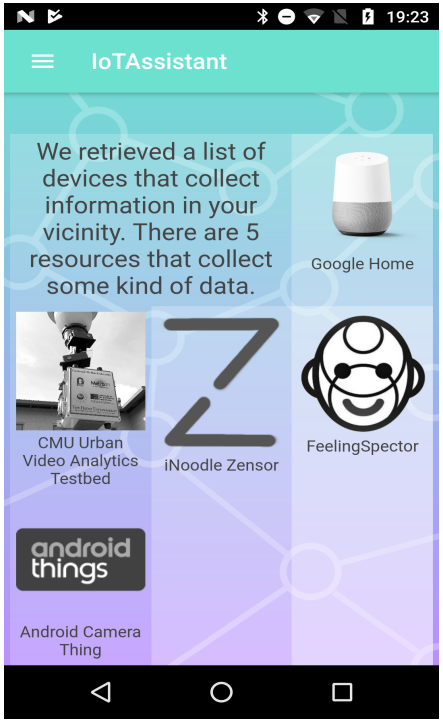
- **What** are they collecting?
- **Who** are they sharing your data with?
- **For how long** are they keeping your data?







Now imagine the future



- **What** are they collecting?
- **Who** are they sharing my data with?
- **For how long** are they keeping my data?

Design questions

- **Informing** people about data collections
  - What should we notify people about?
- Giving some **choices** to control privacy
  - What factors make people comfortable?
  - What factors make people allow/deny a data collection?

Design questions

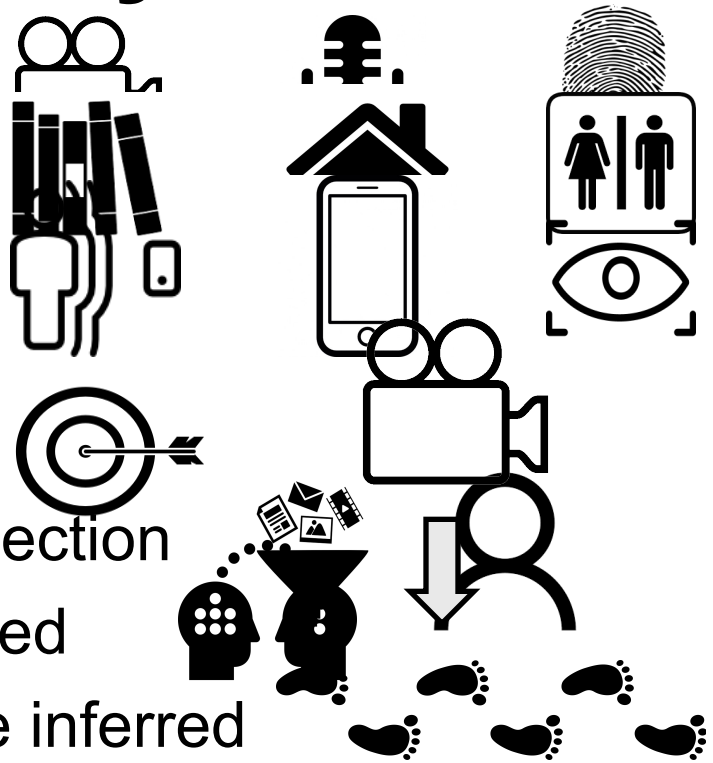
- Making the system **automated**
  - How well can we predict people preferences?

Vignette study

- Capture wide range of scenarios
- Stories about individuals, situations and structures which can make reference to important points in the study of perceptions, beliefs and attitudes (Hughes 1998)

Scenarios varied by 8 factors

- Type of data collected
- Location of data collection
- Device collecting data
- Retention time
- Purpose of data collection
- Who benefits from data collection
- Whether or not data is shared
- Whether more info could be inferred



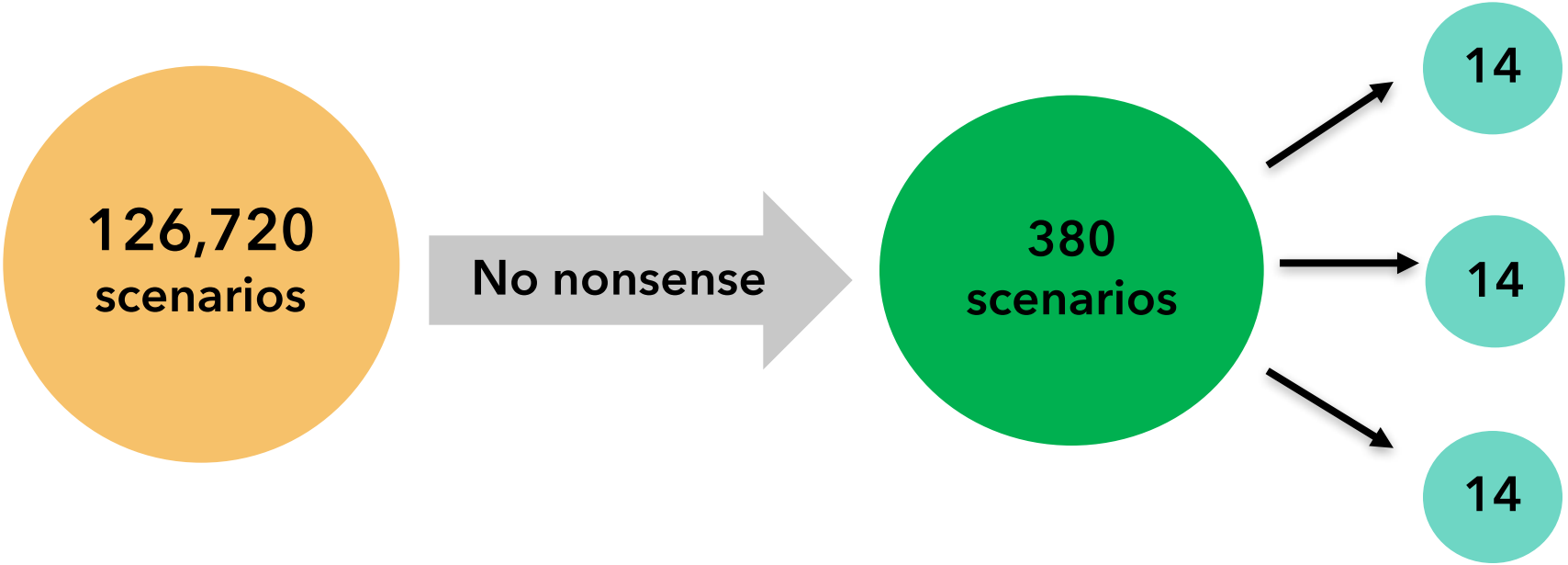
Example scenario

- You are at **[work]**. This building has **[cameras]** that are recording **[video of the entire building]**. The video is **[shared with law enforcement]** to **[improve public safety]** and they **[will not delete it]**.

Example scenario

- You are at a **[department store]**. This store has an **[iris scanner]** that scans customers' irises automatically as they enter the store in order to **[remotely identify returning customers]**. Your iris scan will be kept for **[one week]**.

Studied 380 IoT scenarios



Our participants

- 1007 Mechanical Turk participants
- From the United States
- Avg. age: 35.3
- ~15 minutes to complete

Questions per scenario

- *I would want my mobile phone to notify me [every time / only the first time / every once in a while] this data collection occurs.*
  - five point scale from “strongly agree” to “strongly disagree”

Questions per scenario

- *How would you feel about the data collection in the situation described above if you were given no additional information about the scenario?*
  - five point scale from “very comfortable to “very uncomfortable”
- *If you had the choice, would you allow or deny this data collection?*
  - Choices: allow, deny

Model selection

- GLMM + random intercept
- Backward elimination

Model: Every time notification

- Most impactful explanatory factor:
  - Biometrics for an unspecified purpose (coef: 0.88, 61%)
  - Presence for a not beneficial purpose (coef: -0.49, 27%)
- Least impactful explanatory factor:
  - data collected at a department store (coef: -0.69, 42%)

Model: Comfort level

- Most impactful explanatory factor:
  - Video collection happening today (coef: 1.39, 69%)
  - Biometrics (coef: -1.45, 28%)
- Least impactful explanatory factor:
  - Data being kept forever (coef: 0.10, 48%)

Model: Desire to Allow/Deny

- Most impactful explanatory factor:
  - Video collected at department store (coef: -0.9, 66%)
  - Presence collected at work (coef: 2.11, 36%)
- Least impactful explanatory factor:
  - Data being shared (coef: 0.52, 45%)

Prediction accuracy

- Comfort level:
  - ~81%
- Desire to allow or deny:
  - ~79%

Preferences in a nutshell

- Anonymous data types




"I'd be fine with data that doesn't identify me."

- Public vs. private




"[I would be] comfortable with public spaces, absolutely not comfortable in my home."

Preferences in a nutshell

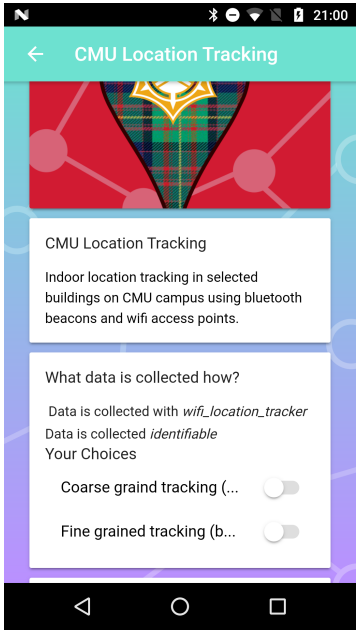
- Ranked 1st = Type of data + X
  - Notification → X = user perceived benefit
  - comfort → X = happening today
  - allow/deny → X = location

Our results → design

- Design personalized privacy systems
- In progress: experience sampling

More info: www.privacyassistant.org

Pardis Emami-Naeini, Sruti Bhagavatula, Martin Degeling, Hana Habib, Lujo Bauer, Lorrie Faith Cranor, Norman Sadeh



Carnegie Mellon University

DARPA