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

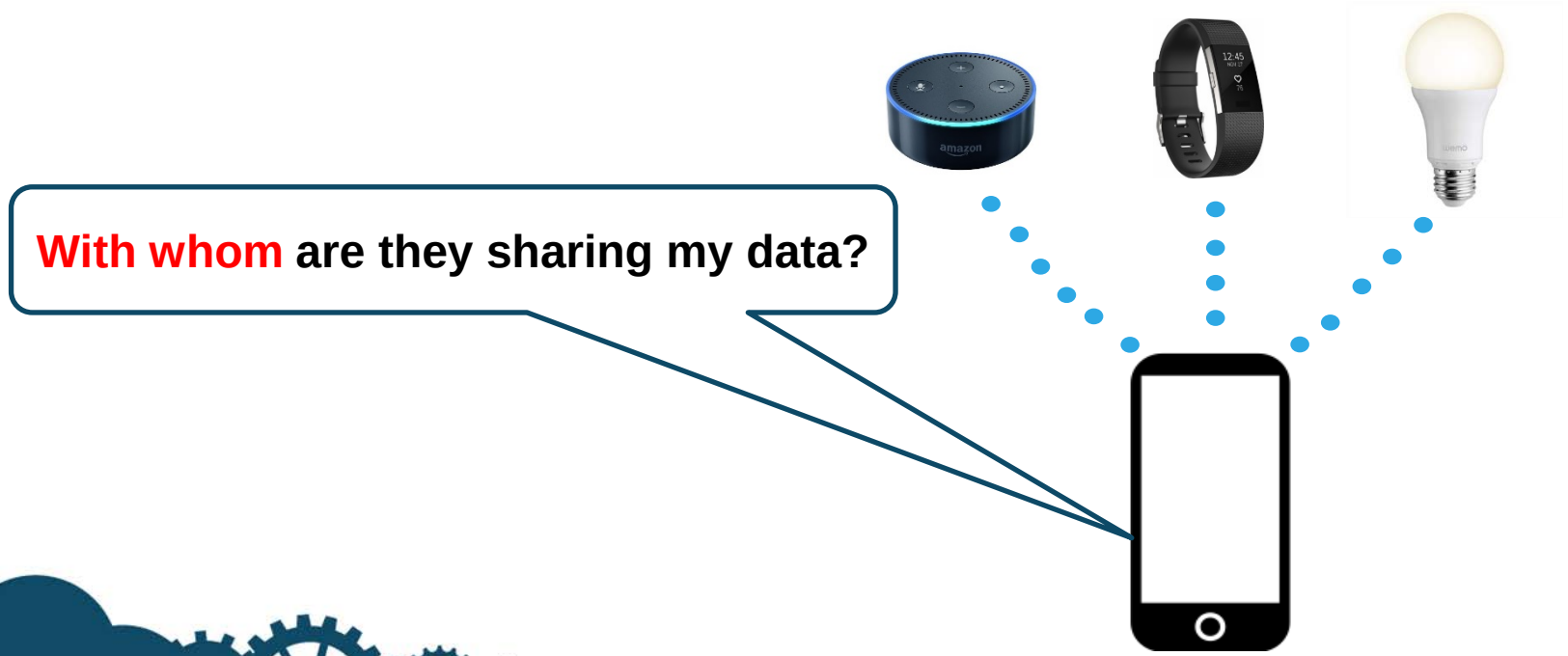
PRIVACYCON

Internet of Things (IoT):

The future privacy assistant:

What are they collecting?

The future privacy assistant:



The future privacy assistant:

Privacy assistant's design goals

Inform people about data collection

- What should we notify people about?

Enable privacy **choices**

- What factors influence privacy decisions?

Automate privacy decision making

- Can we predict privacy preferences accurately?

Vignette study

Asked participants to imagine themselves in hypothetical data collection scenarios

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].

15-minute survey

Recruited 1007 US participants on Mechanical Turk

Each participant shown 14 scenarios + asked questions

- How often would you want your phone to notify you of this data collection?
- How comfortable are you with this data collection?
- Would you allow or deny this data collection?
- …

Interpreting the results

Statistical models that explain relationship between factors explored in vignettes and …

- Users' desire to be notified of data collection
- Users' comfort with data collection
- Users' willingness to allow data collection

Sample of results

What affects preferences to be **notified**?

Data being **shared**

Biometrics data

Beneficial purpose

→ **more likely want to be notified**

→ **less likely want to be notified**

Sample of results

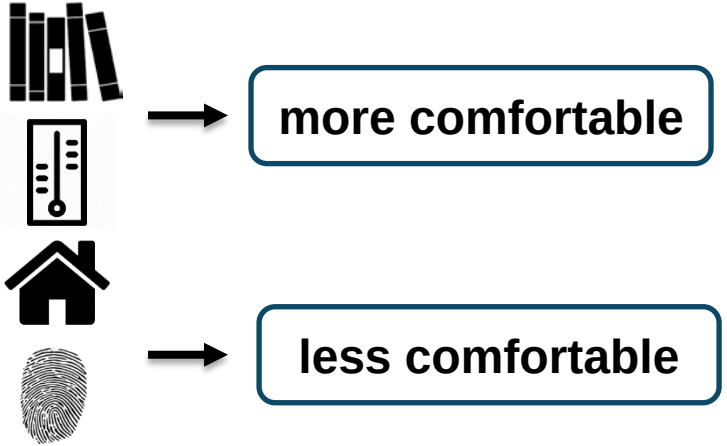
When are users **(un)comfortable** with data collection?

Public location

Environmental data

Private location

Biometrics data



Sample of results

When are users willing to **allow** data collection?

Beneficial purpose

Data being **shared**

→ **more likely want to allow**

→ **less likely want to allow**

What factors matter most to explain privacy preferences?

- Type of data?
- Location of data collection?
- Purpose of data collection?
- Retention time?
- …

What factors matter most to explain privacy preferences?

- ~~Type of data?~~
- ~~Location of data collection?~~
- ~~Purpose of data collection?~~
- ~~Retention time?~~
- ~~…~~

What factors matter most to explain privacy preferences?

Combination of factors matters most!

What factors matter most?

Notification:

Type of data × user-perceived benefit

 × purpose they don’t see as beneficial = more notification

What factors matter most?

Comfort level:

Type of data × happening today

× happening today = comfort

What factors matter most?

Allow/deny:

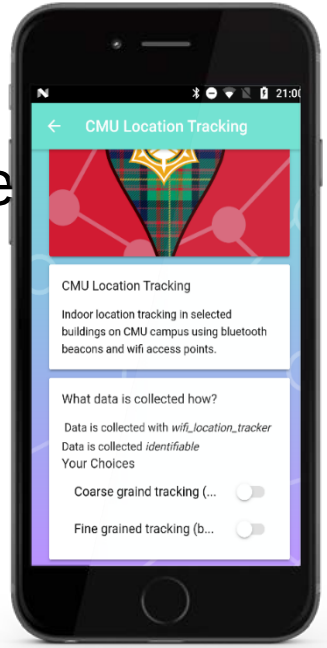
Type of data × location

= deny

Our results → design

Built models to understand people's privacy prefere

Long-term goal: design privacy assistant



P. Emami-Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. Cranor, N. Sadeh. Privacy expectations and preferences in an IoT World. In *Proceedings of the 13th Symposium on Usable Privacy and Security (**SOUPS'17**)*

Carnegie Mellon University

DARPA

PRIVACYCON