Designing Meaningful Privacy Choice Experiences for Users

Yuanyuan Feng, Yaxing Yao, and Norman Sadeh
School of Computer Science
Carnegie Mellon University
“Notice and Choice”

Privacy Notices  Data Subject  Data Practices

Privacy Choices
Privacy choices are often difficult to find, overly simplified, and even manipulative.

Difficult to find on user interfaces

Overly simplified into binary choices

Manipulative using “dark patterns”
“Dark Patterns” in Privacy Choice Design

By clicking Sign Up, you agree to our Terms, Data Policy and Cookies Policy. You may receive SMS Notifications from us and can opt out any time.

Sign Up

→ hidden privacy choices

This website uses cookies
We use cookies to make our website safer, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media and analytics partners who may combine it with information that you’ve provided to them or that they’ve collected from your use of their services.

☐ Necessary  ☑ Preferences  ☑ Statistics  ☑ Marketing  Show details  OK

→ choice pre-selection
Lack of Guidance for Practitioners
Effectiveness

Neutrality

Efficiency

Meaningful Privacy Choices

Comprehensiveness

User Awareness
A Design Space for Privacy Choices

A technology review

A user-centered analysis
A Design Space for Privacy Choices

- **Type**
  - Binary choice
  - Multiple choices
  - Contextualized choices
  - Privacy rights-based choices

- **Functionality**
  - Presentation
  - Enforcement
  - Feedback

- **Timing**
  - At setup
  - Just in time
  - Context-aware
  - Periodic
  - On-demand
  - Personalized

- **Channel**
  - Primary
  - Secondary
  - Public

- **Modality**
  - Visual
  - Auditory
  - Haptic and other sensory
  - Machine-readable
  - Combined
A Design Space for Privacy Choices

Use Case: Designing a privacy choice platform for deployed Internet of Things (IoT) - the IoT Assistant app
A Design Space for Privacy Choices

Use Case: Designing a *privacy choice platform* for deployed Internet of Things (IoT) - the **IoT Assistant** app
Lab Location Tracking

Description
The Mobile Commerce Lab has a bluetooth beacon-based location tracking service for registered lab members. It can track if a lab member is in the lab room (TCS Hall 431) and share their location info with other lab members. Registered lab members can opt out of data collection or data sharing by this service.
A Design Space for Privacy Choices

Use Case: Designing a privacy choice platform for deployed Internet of Things (IoT) - the IoT Assistant app
Type

- binary choice
- multiple choices
- contextualized choices
- privacy rights-based choices
A Design Space for Privacy Choices

Use Case: Designing a privacy choice platform for deployed Internet of Things (IoT) - the IoT Assistant app.
Functionality

- Presentation (of privacy choices)
- Enforcement (of privacy decisions)
- Feedback (of privacy choice status)
A Design Space for Privacy Choices

Use Case: Designing a privacy choice platform for deployed Internet of Things (IoT) - the IoT Assistant app
Timing

- at setup
- just in time
- context-aware
- periodic
- on-demand
- personalized
A Design Space for Privacy Choices

Use Case: Designing a *privacy choice platform* for deployed Internet of Things (IoT) - the **IoT Assistant** app
Channel

- Primary
- Secondary (an app)
- Public (QR codes)

Discover and control IoT data collected about you

IoT Privacy Assistant
A Design Space for Privacy Choices

Use Case: Designing a *privacy choice platform* for deployed Internet of Things (IoT) - the **IoT Assistant** app
Modality

- Visual
- Auditory
- Haptic and other sensory
- Machine-readable
- Combined
A Design Space for Privacy Choices

Use Case: Designing a privacy choice platform for deployed Internet of Things (IoT) - the IoT Assistant app
Summary of Contributions

- A conceptual framework and a taxonomy for meaningful privacy choices
- A comprehensive guide to design meaningful privacy choices experiences for users