On the Design of a Privacy-focused Data Lifecycle for Smart Living Spaces

(Redacted Version)

Joseph Bugeja
Andreas Jacobsson
✓ Over 20 billion Internet of Things (IoT) devices by 2020

✓ Internet-connected devices will outnumber people at least 2:1

✓ Global market size of about $457B by 2020

✓ Applications range from domestic to industry scenarios
SOME EXAMPLES OF PRIVACY HARMs

- Discrimination
- Identity theft
- Unsolicited ads

On the Design of a Privacy-focused Data Lifecycle for Smart Living Spaces  IFIPSC 2019
Amazon Workers Are Listening to What You Tell Alexa

A global team reviews audio clips in an effort to help the voice-activated assistant respond to commands.

Recordings are transcribed and annotated

Source: https://bloom.bg/2D6kQbq
1890: Warren and Brandeis identified privacy as “the right to be let alone”

1968: Westin described privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”

1975: Altman conceptualizes privacy as a boundary regulation process whereby people optimize their accessibility depending on a context

2009: Nissenbaum proposed the theory of Contextual Integrity that argues for a consideration of information flow in context
On the Design of a Privacy-focused Data Lifecycle for Smart Living Spaces
**IoT EXTERNAL ENTITIES**

- **Data subject:** The human entity that generates the original raw data

- **Data curator:** Typically the organization, that collects, stores, processes, and releases the data

- **Data users:** Signifies the entities who access the released data
Data attacker
**Data generation:** Activity where the data subject interacts with the IoT system to create personal data.

**Data collection:** Acquiring personal data from data subjects, including external sources.

**Data processing:** The IoT analyses the stored data to provide the smart services.

**Data disclosure:** Disseminating, making available or transmitting personal data for external use by third-parties.
OTHER PRIVACY THREATS

✓ **Privacy-violating interaction and presentation**: Exposing personally identifiable information to individuals who are not supposed to have access to it

✓ **Inventory attacks**: Unauthorized collection of information about the existence and characteristics of personal things

✓ **Lifecycle transitions**: Disclose private information during changes of control spheres in their lifecycle
THANK YOU FOR YOUR ATTENTION!

joseph.bugeja@mau.se