유비쿼터스 환경에서의 Usable Security & Privacy 연구 동향: 멀티모달 센싱 시대의 사용자 보안/프라이버시를 고려한 인간 중심 시스템 설계

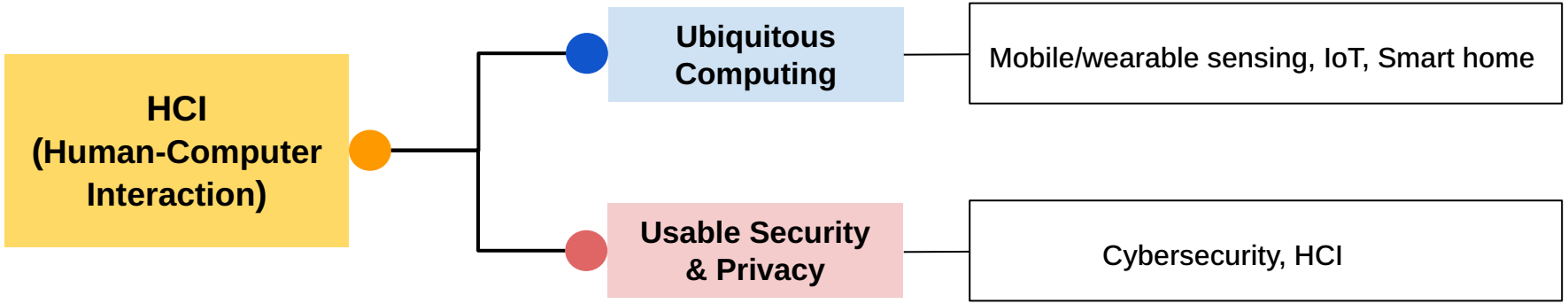
이현수

KCC 2025 신진연구자 세션

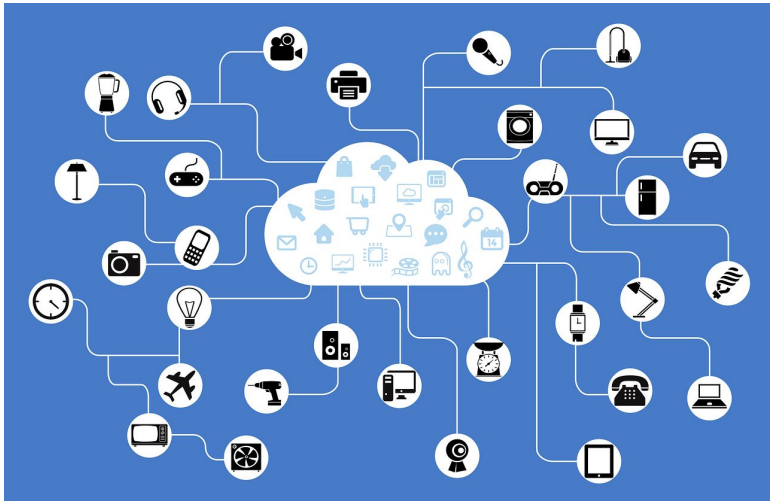
7월 3일 ICC 제주 401B호

목차

Research Area



Research Area

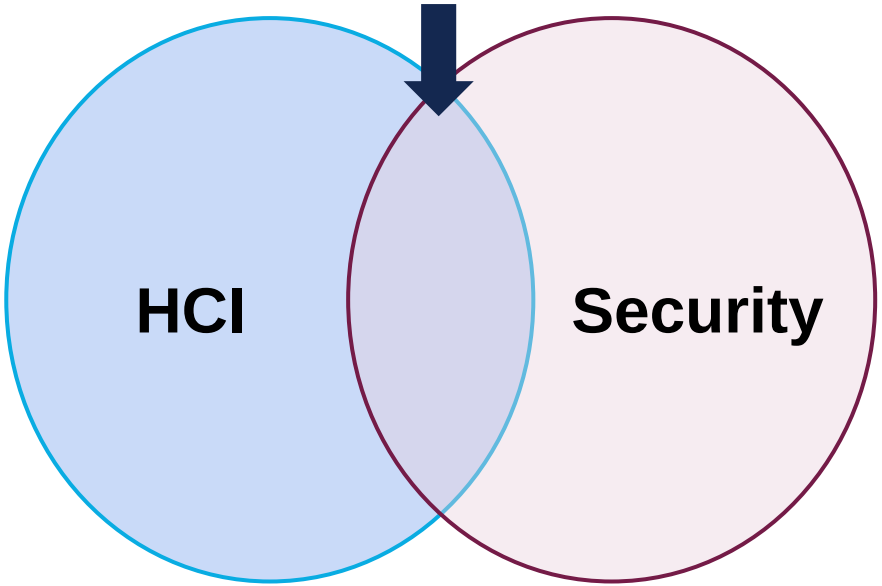


Ubiquitous computing

“Ubiquitous computing, also known as **pervasive computing**, refers to the concept of **embedding computing capabilities into everyday objects and environments**, making technology seamlessly available and accessible anytime and anywhere.”

Research Area

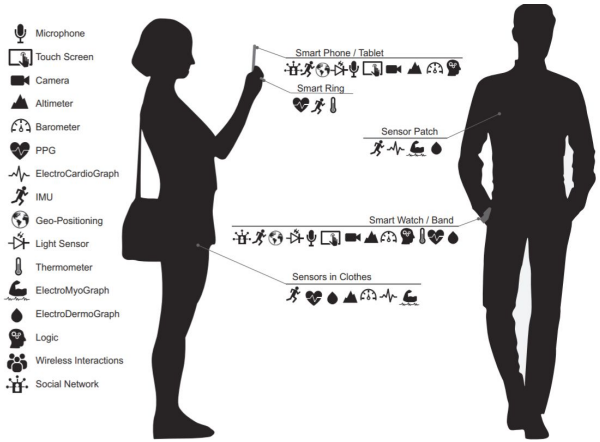
Usable Security & Privacy



"Give end-users **security controls they can understand** and **privacy they can control** for the dynamic, pervasive computing environments of the future."

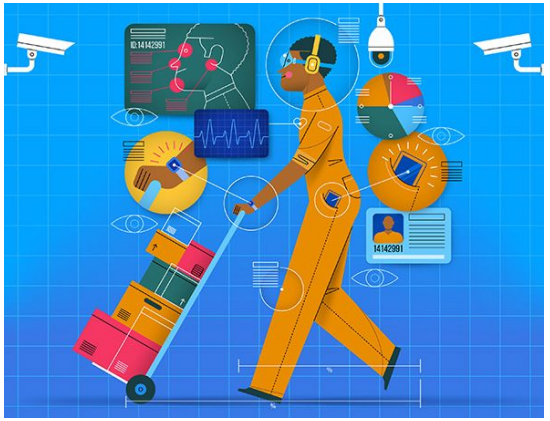
Computing Research Association 2003

Security and Privacy Issues in Ubiquitous Environments



Personal sensing

Smarthome sensing



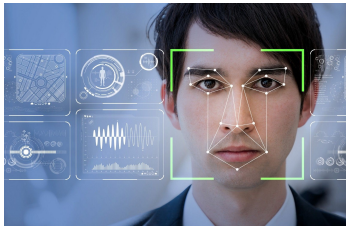
Workplace sensing

[1] Kourtis, Lampros C., et al. "Digital biomarkers for Alzheimer's disease: the mobile/wearable devices opportunity." NPJ digital medicine (2019)
[2] https://ssir.org/articles/entry/the_long_shadow_of_workplace_surveillance

Security and Privacy Issues in Ubiquitous Environments

Personal Profiling & Behavioral Prediction

- Accelerometer data revealing participants' current activities
- Gait recognition data revealing participants' identity



Discrimination & Stigmatization

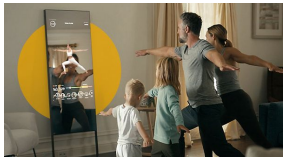
- Drawing health inferences from personal data
- Inaccurate or biased emotion detection algorithms leading to psychological and physical harms (e.g., AI Snake Oil)

[1] Jennifer R Kwapisz, Gary M Weiss, and Samuel A Moore. 2011. Activity recognition using cell phone accelerometers. ACM SigKDD Explorations Newsletter 12, 2 (2011)
[2] Mohammad Omar Derawi, Claudia Nickel, Patrick Bours, and Christoph Busch. 2010. Unobtrusive user-authentication on mobile phones using biometric gait recognition. IEEE (2010)
[3] Skiljic A. The Status Quo of Health Data Inferences. International Association of Privacy Professionals: Privacy Perspectives
[4] Martin Cooney, Sepideh Pashami, Anita Sant'Anna, Yuantao Fan, and Slawomir Nowaczyk. Pitfalls of Affective Computing:How can the automatic visual communication of emotions lead to harm, and what can be done to mitigate such risks. In Companion Proceedings of the The Web Conference 2018

Research landscape

Personal data

Group data



Understanding and analyzing privacy behavior

- Privacy concerns and data sensitivity (UbiComp'22)
- Data collection and sharing preferences (ICMU'21)
- OurData framework (Submitted to UbiComp'25)

Proposing novel concepts and systems

- Dynamic consent for pervasive sensing (IEEE'22)
- Fine-grained privacy control (CHI'24)
- Group data reflection system (CSCW'24)

- [Short-term] Establishing technical framework for group data and explore user perceptions and ethical considerations
- [Long-term] Designing interactive technologies that surface data practices, enhance data literacy, and support both individual and collective privacy decisions in multi-user environments

Research contribution

- End-to-end field trial
- User perception
- User-oriented system design

Research goal

My research will continue to increase users' privacy awareness and provide secure user experience

Privacy Concerns in Multimodal Sensor Data Collection (UbiComp'22)

(1) Collected 31 types of sensor data (N = 100, Four-week)

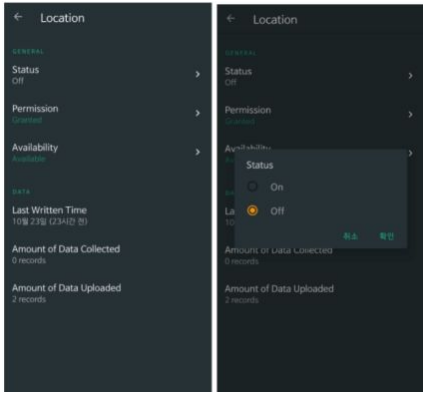
- Collected 31 types of sensor data from 100 college students
- Investigated users' general perception and data sensitivity toward personal data disclosure in multimodal sensing contexts
- Quantitatively analyzed contributing factors toward users' behavioral patterns and privacy-decision making under multimodal sensor data collection (N = 26)

4-week field-trial study

- Device - Smartphone, smartwatch, chest band
- Data types - 31
- Data contributor - 100

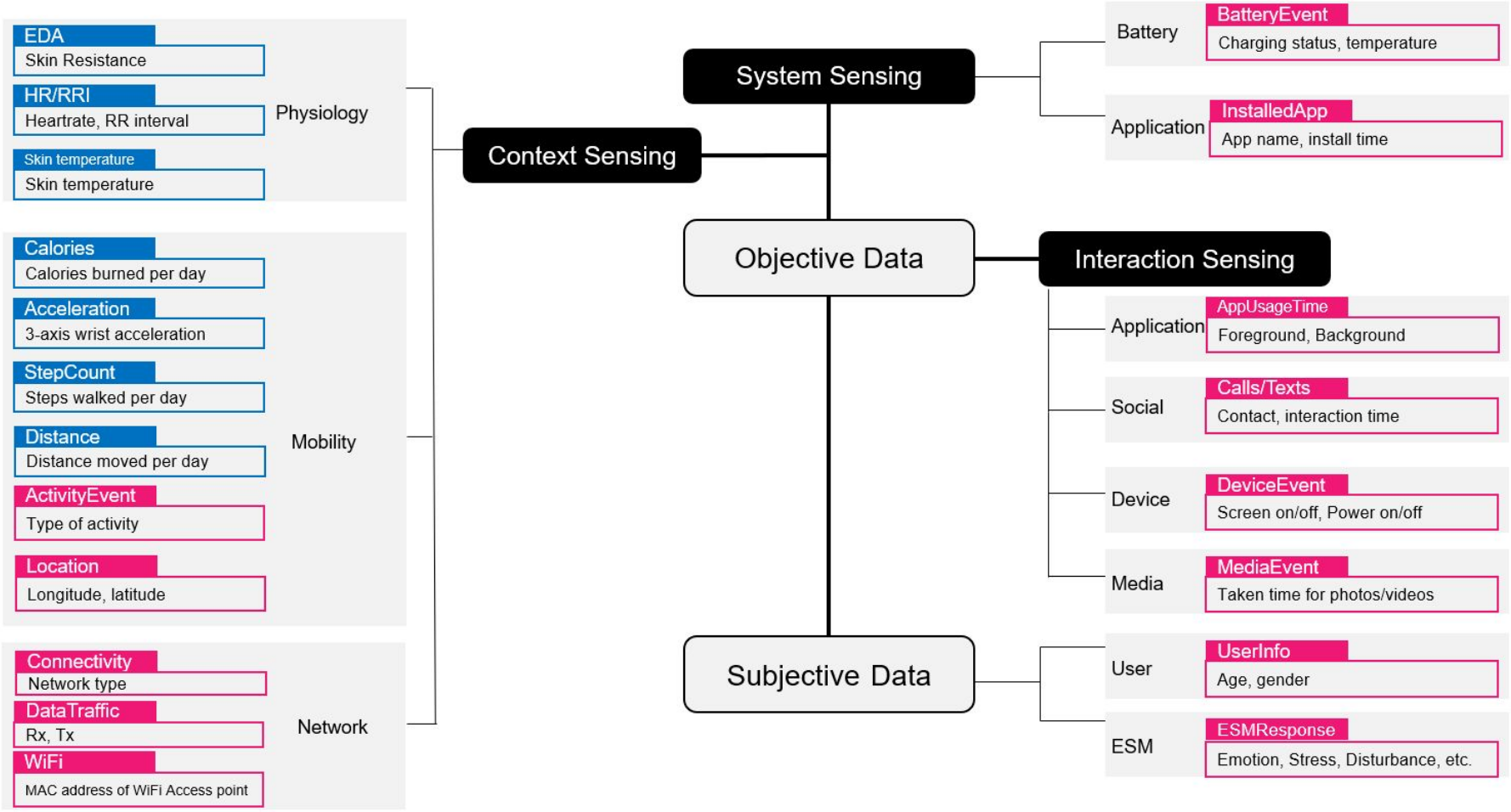
→ Data sensitivity
→ Privacy concerns
→ Risks-Benefits

Apparatus



Sensing platform

Privacy Concerns in Multimodal Sensor Data Collection (UbiComp'22)



Privacy Concerns in Multimodal Sensor Data Collection (UbiComp'22)

(2) Users' general motives and data sensitivity

- Collected 31 types of sensor data from 100 college students
- Investigated users' general perception and data sensitivity toward personal data disclosure in multimodal sensing contexts
- Quantitatively analyzed contributing factors toward users' behavioral patterns and privacy-decision making under multimodal sensor data collection (N = 26)

User perception survey (7-point Likert scale)

Motives	Financial compensation (M = 5.67)
Risk-Benefit Assessment	Personal data protection (M = 6.40)
	Potential benefits (M = 4.68)
Privacy concerns	Behavioral intention (M = 5.15)
	Secondary use (M = 4.50)
Trust	Trust in collected data types (M = 6.16)

Data sensitivity survey (7-point Likert scale)

Calls/texts - App usage - App notification - Camera- GPS (no pre-post statistical difference)

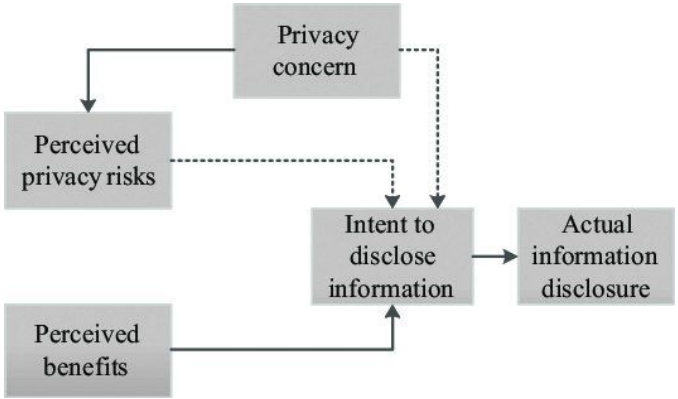
Privacy Concerns in Multimodal Sensor Data Collection (UbiComp'22)

(3) Factors associated with users' privacy decision-making

- Collected 31 types of sensor data from 100 college students
- Investigated users' general perception and data sensitivity toward personal data disclosure in multimodal sensing contexts
- Quantitatively analyzed contributing factors toward users' behavioral patterns and privacy-decision making under multimodal sensor data collection (N = 26)

Types of privacy concerns

- Routine identification	- Judgment
- Surveillance	- Data misuse



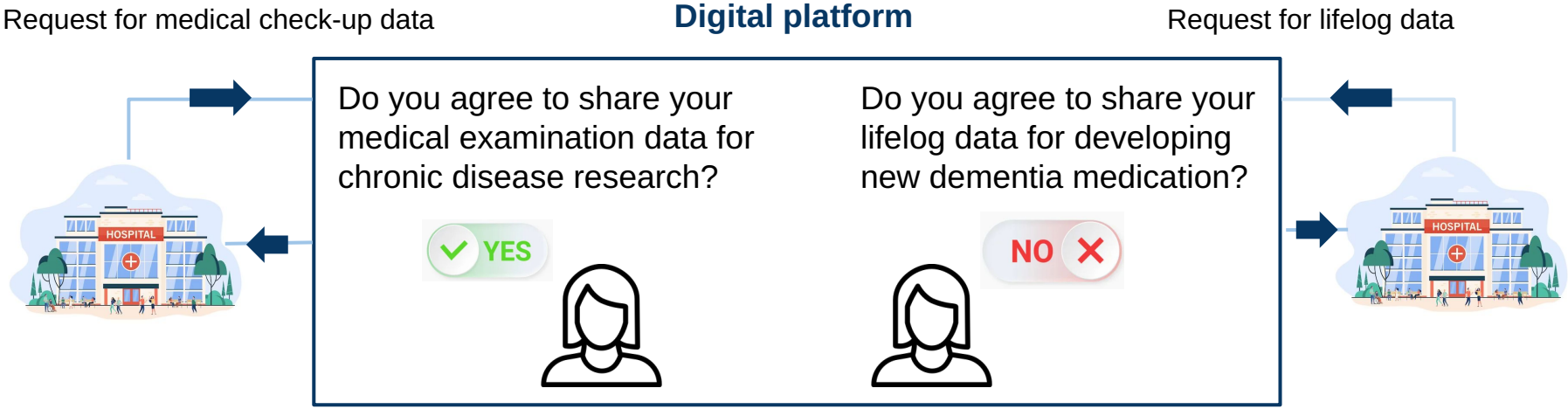
Privacy-Utility Trade-Off

Fine-Grained Privacy Control in Sensor-Driven Research (ACM ICMU'21, IEEE Pervasive Computing'22)

"**Dynamic consent**" in pervasive sensing studies

Definition:

1. **Flexible data consent** (originated from biomedical field) → Patient participation & power to patients
2. **Narrow and specific consent** → engage/withdraw from a new research or give/revoke access to a certain data item



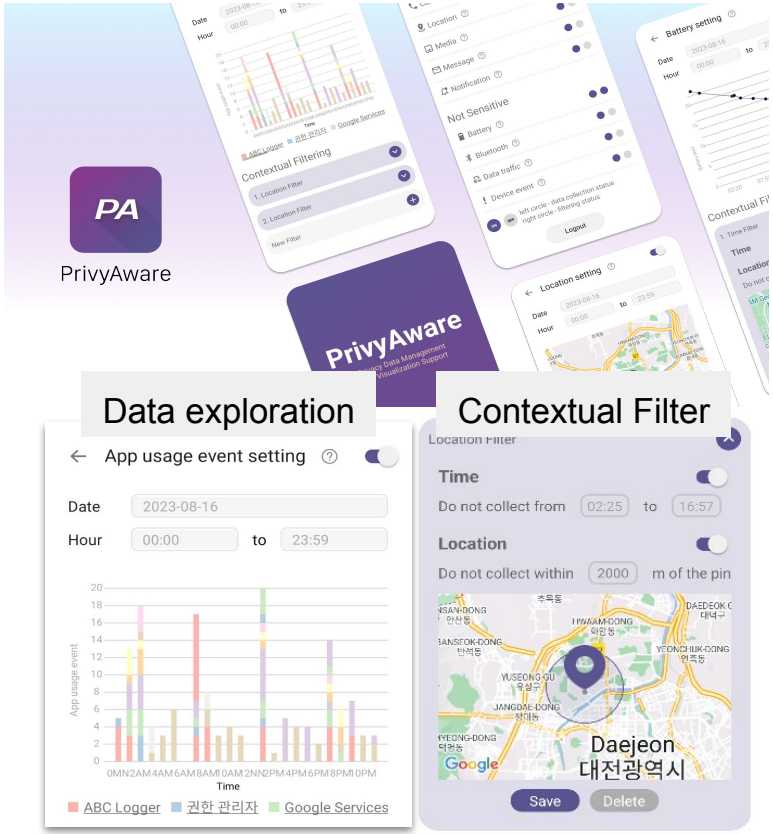
[1] J. Kaye, E. A. Whitley, D. Lund, M. Morrison, H. Teare, and K. Melham, "Dynamic consent: A patient interface for Twenty-First century research networks," Eur. J.Hum. Genet., vol. 23, no. 2, pp. 141–146, 2015.
[2] K. S. Steinsbekk, B. K. Myskja, and B. Solberg, "Broad consent versus dynamic consent in Biobank research:s passive participation an ethical problem?," Eur. J.Hum. Genet., vol. 21, no. 9, pp. 897–902, 2013

User-Friendly Privacy Support in Multimodal Sensing (CHI'24)

(1) Design and implementation of PriviAware

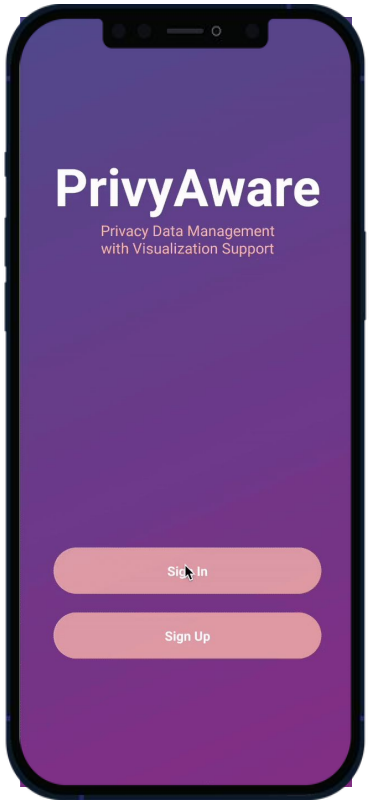
- Designed and implemented **PriviAware** - a mobile intervention app for promoting participants' proactive data collection consent and privacy management

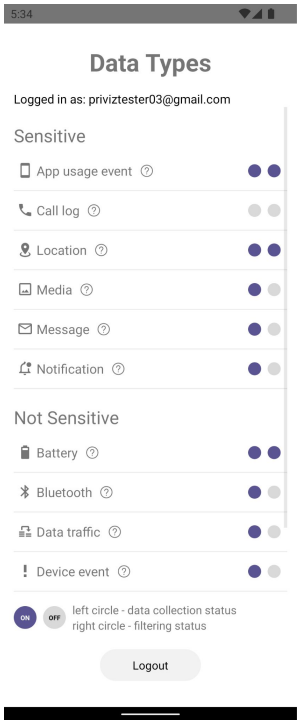
- Performed user study on how PriviAware's different intervention conditions have a different effect on participants' perceived level of privacy concerns and awareness



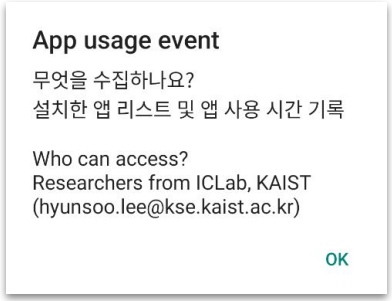
Final System Design

- Main page

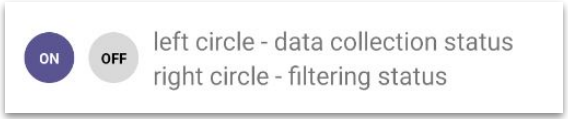




Help Dialog Messages

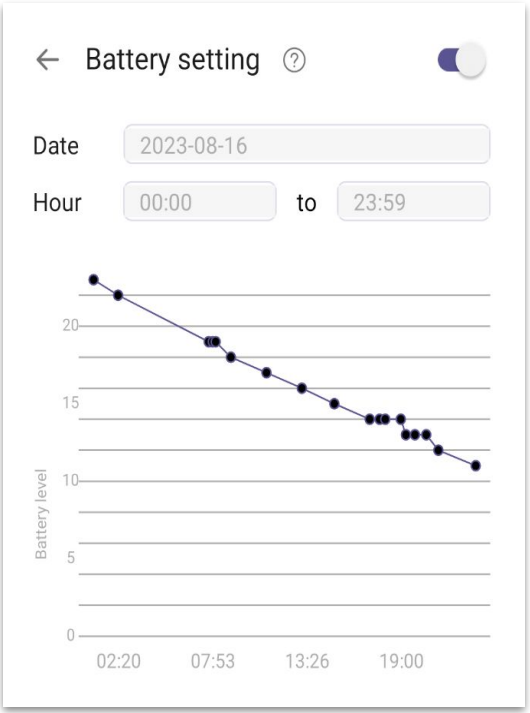


Collecting Status

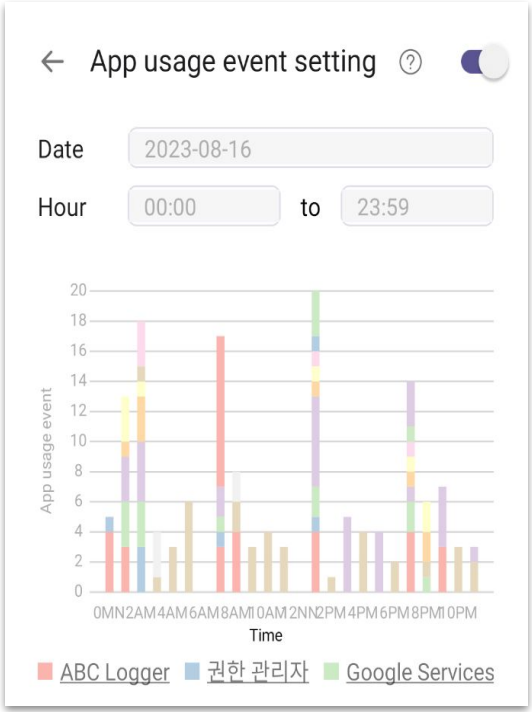


Final System Design

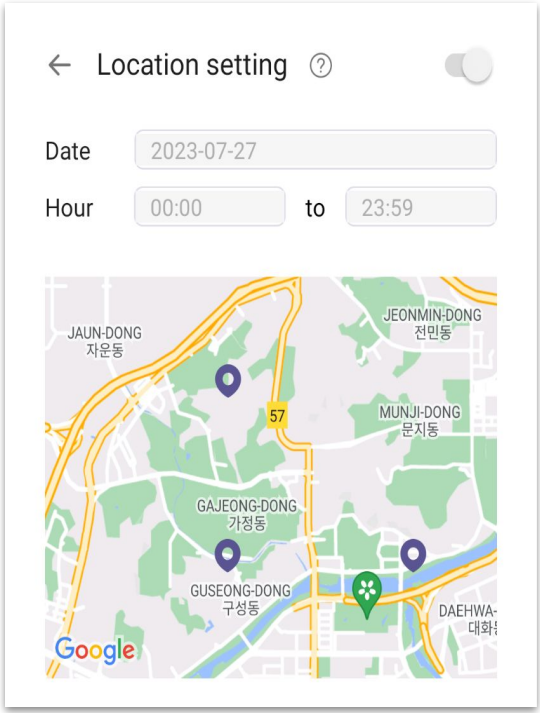
- Key Feature #1. Data exploration: Data visualization of collected data



Numeric data view



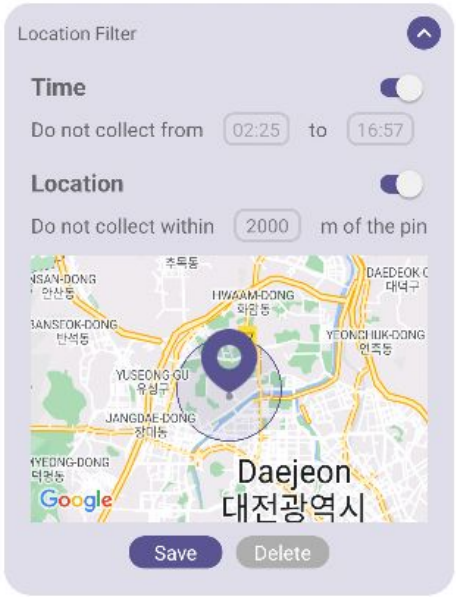
Categorical data view



Location data view

Final system design

- Key Feature #2. Data control: Contextual filtering



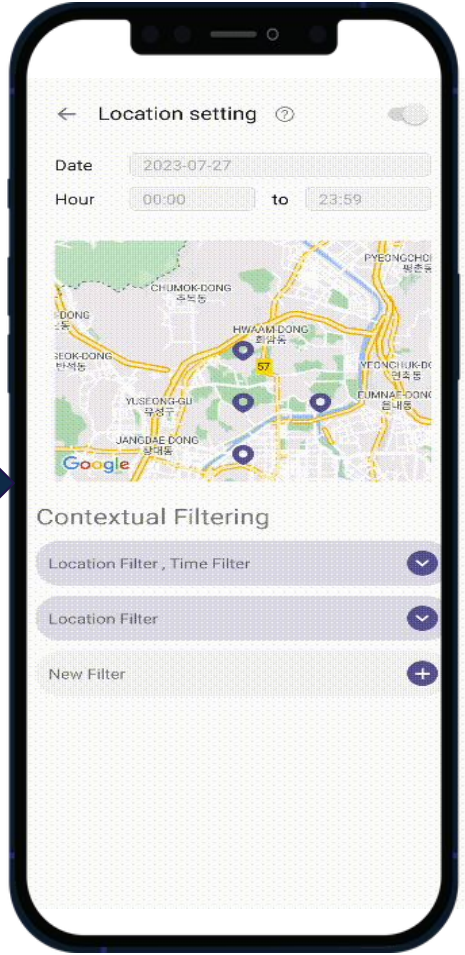
Contextual filtering: Disable data collection

1. Time Filter

- By setting the time range (start-end), users can apply time filter

2. Location Filter

- By moving the pin on map, users can select center of filtering area

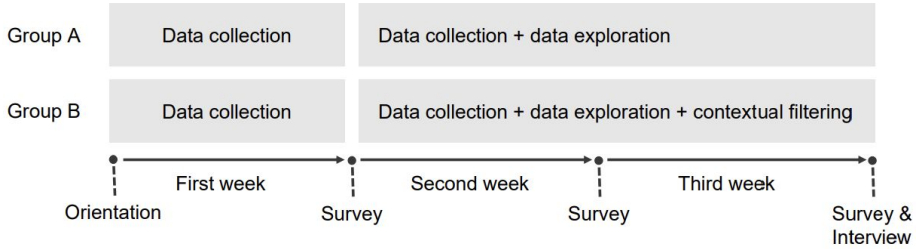


User-Friendly Privacy Support in Multimodal Sensing (CHI'24)

(2) User study on PriviAware system design (N = 60, Three-week)

- Designed and implemented **PriviAware** - a mobile intervention app for promoting participants' proactive data collection consent and privacy management

- Performed user study on how PriviAware's different intervention conditions have a different effect on participants' perceived level of privacy concerns and awareness



Quantitative analysis

1) Perceived usability of PriviAware features (SUS Scale)
   - Data exploration: 73.3
   - Contextual filter: 73.1

2) Decreased privacy concern level for both groups (Mixed-Anova)
   - 1st week vs. 2nd week
   - 1st week vs. 3rd week

User-Friendly Privacy Support in Multimodal Sensing (CHI'24)

(2) User study on PriviAware system design (N = 60, Three-week)

- Designed and implemented **PriviAware** - a mobile intervention app for promoting participants' proactive data collection consent and privacy management

- Performed user study on how PriviAware's different intervention conditions have a different effect on participants' perceived level of privacy concerns and awareness

Qualitative analysis (N = 20)

1) **Behavioral pattern**

- **Data exploration → Contextual filter → Daily check-up on personal data collection & management**

- Contextual filtering configuration:
  - Regular filtering for daily contexts
  - One-time filtering for special occasions

2) **Decrease in privacy concerns**

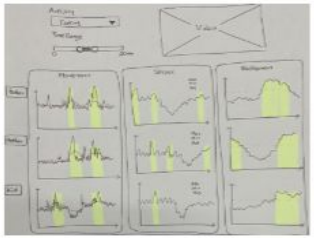
- Increased data literacy
- Increased trust in data handling

Group data privacy in multimodal sensing environment (CSCW'24)

(1) FamilyScope system design

- Designed and implemented **FamilyScope** - sensor data collection and exploration tool for family's emotional health and wellbeing at smart home

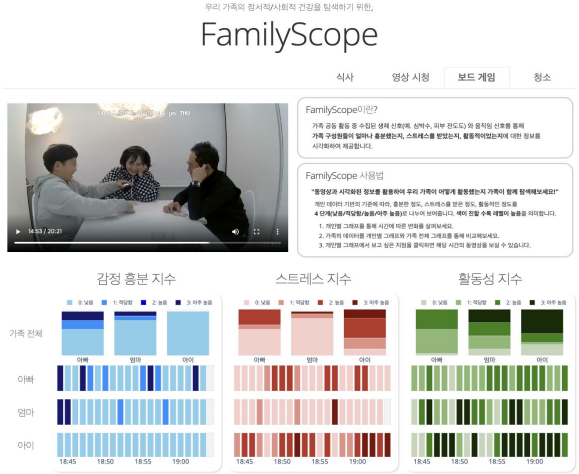
- User study on FamilyScope system design
  - Data collection
  - Interpersonal data privacy concerns
  - Design requirements

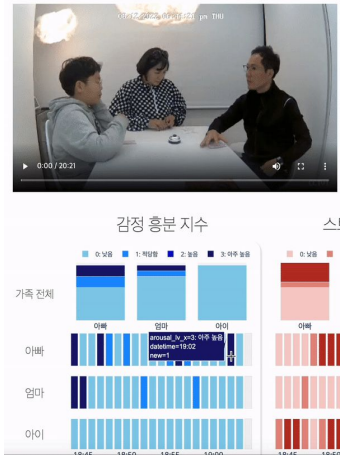


(a) Initial prototype

(b) Second prototype

(c) Third prototype



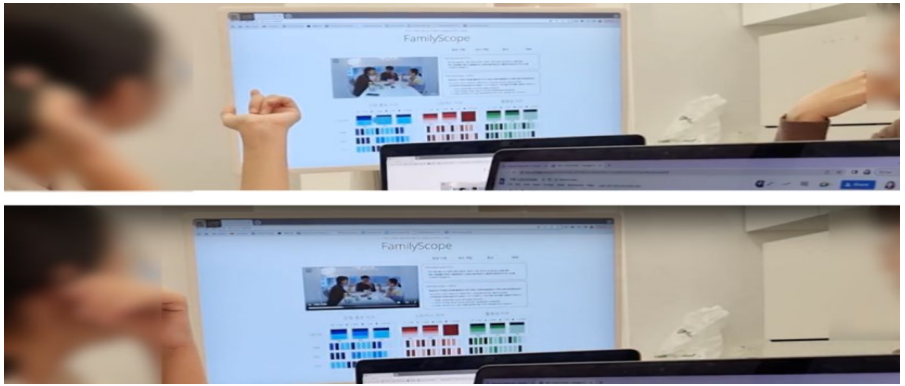


Group data privacy in multimodal sensing environment (CSCW'24)

(2) User study on FamilyScope system design (N = 30, 10 families)

- Designed and implemented **FamilyScope** - sensor data collection and exploration tool for family's emotional health and wellbeing at smart home

- User study on FamilyScope system design
  - Data collection
  - Interpersonal data privacy concerns
  - Design requirements

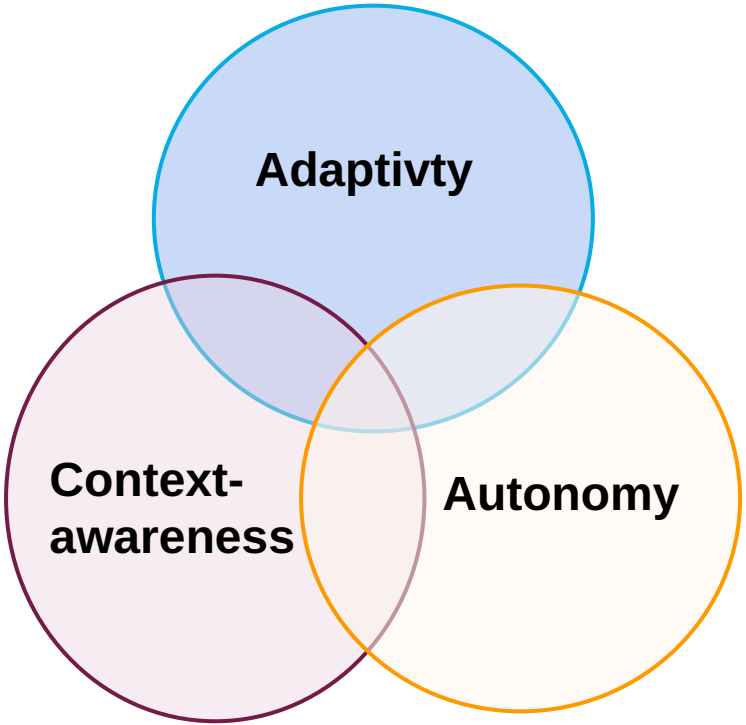


User perceptions & Privacy concerns

Positive	**Family data = "common asset"**
Negative	**Sensor data literacy**
	Data access/grant issue
	Data boundary

Designing for Human-Centered Security and Privacy

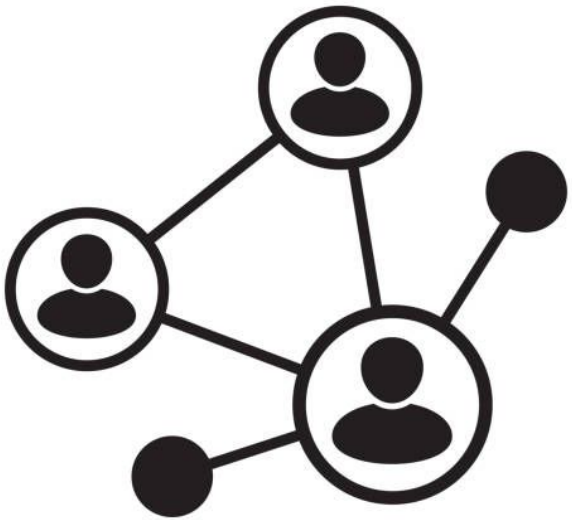
#1. Security & Privacy is not a static setting—it's a dynamic, context-sensitive challenge



- **Implication**
  - Permission toggles alone are insufficient → need for context-aware, adaptive interfaces
- **Research directions**
  - Real-time consent flows based on user context

Designing for Human-Centered Security and Privacy

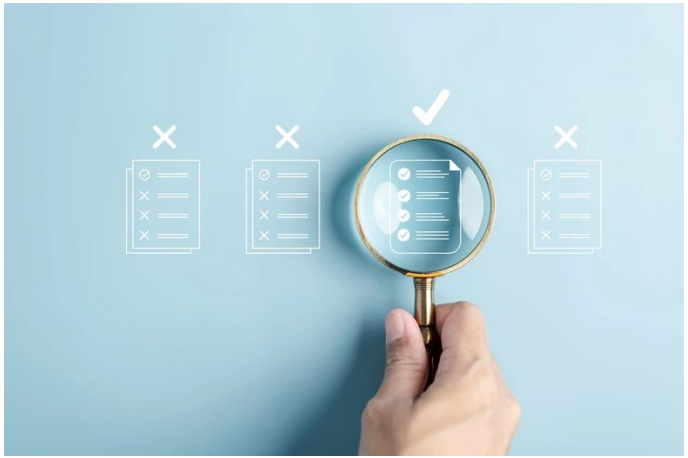
#2. Security & Privacy decisions often involve multiple users—data is relational



- **Implication**
  - Shared data (e.g., family, teams) demands **multi-user privacy design patterns**
- **Research directions**
  - Interfaces for negotiating access across social boundaries
  - Sociotechnical components for coordinating shared privacy preferences
  - Tools for managing group-level data conflicts

Designing for Human-Centered Security and Privacy

#3. Transparency and controllability are essential for building trust



- **Implication**
  - Sensor- or AI-driven systems must visualize invisible data flows and support **user agency**
- **Research directions**
  - Understandable visualizations of sensed data and system inference
  - Feedback loops combining data tracking with actionable controls

Designing for Human-Centered Security and Privacy

#4. Security & Privacy design should shift from protection to participation

- **Implication**
  - Security & Privacy behavior is not just about risk avoidance, but about **user empowerment and active engagement**
- **Research directions**
  - Participatory interfaces that support user-driven data decisions
  - Lightweight, usable interaction models that require minimal cognitive effort

유비쿼터스 환경에서의 Usable Security & Privacy 연구 동향: 멀티모달 센싱 시대의 사용자 보안/프라이버시를 고려한 인간 중심 시스템 설계

이현수

KCC 2025 신진연구자 세션

7월 3일 ICC 제주 401B호