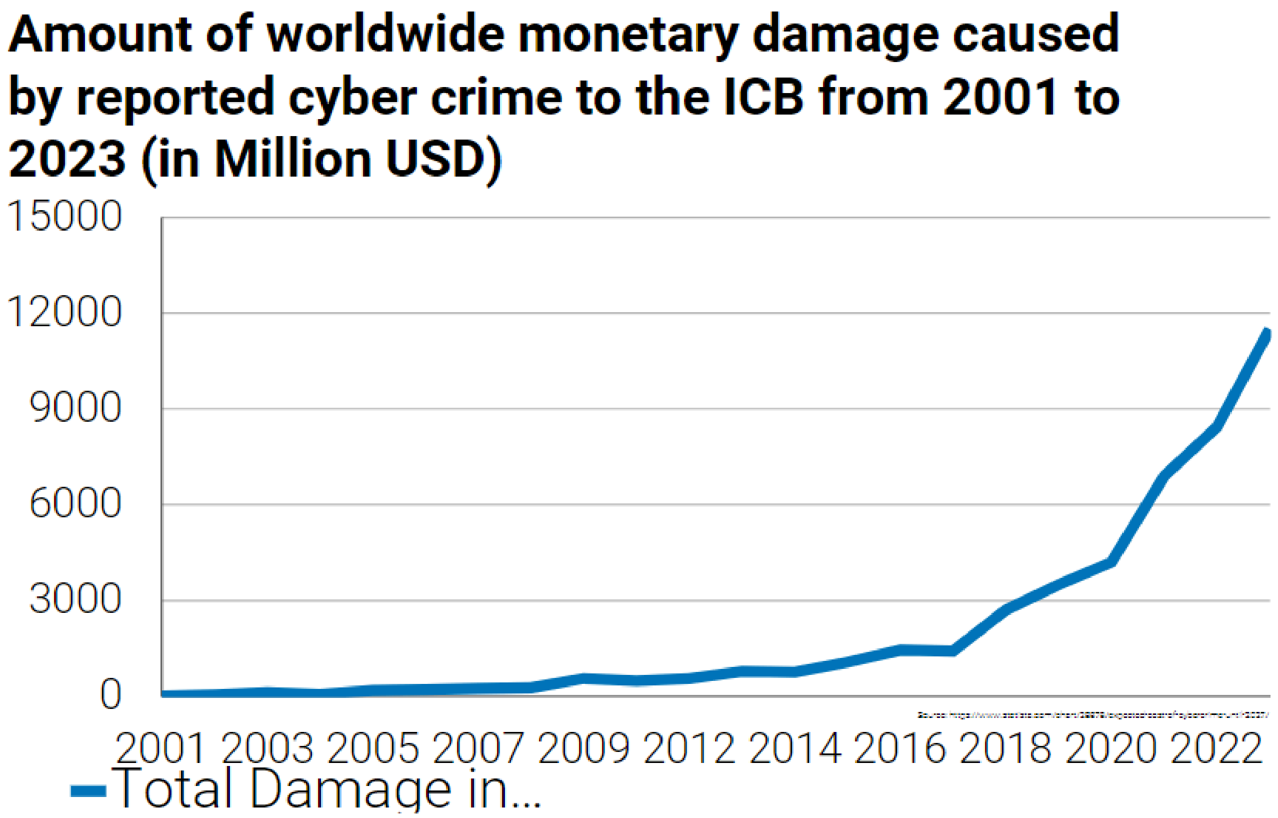
Lecture 8 - Security and Privacy

The Growing Cost of Cybercrime

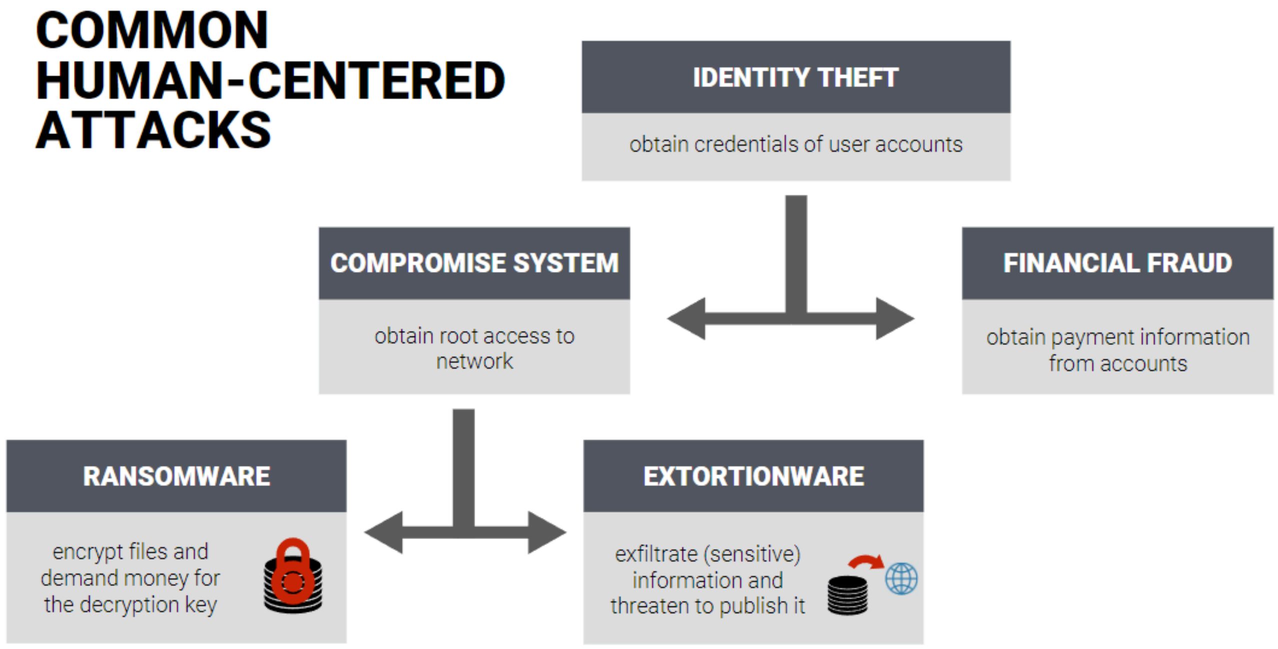


Amount of worldwide monetary damage caused by reported cyber crime to the ICB from 2001 to 2023 (in Million USD)

- Cybercrime costs have increased exponentially, reaching **billions of dollars annually**.
- Successful **cyberattacks on German universities** in recent years highlight the vulnerabilities of institutions.

> **Cybercrime Damage Trends - Statista**
>
> "The financial impact of cybercrime has grown significantly, with expected damages surpassing $10 trillion by 2025."

> **On Hackers, TK Keanini (CISCO)**
>
> "Hackers don't break in — They log in"



COMMON HUMAN-CENTERED ATTACKS

IDENTITY THEFT

obtain credentials of user accounts

COMPROMISE SYSTEM

obtain root access to network

FINANCIAL FRAUD

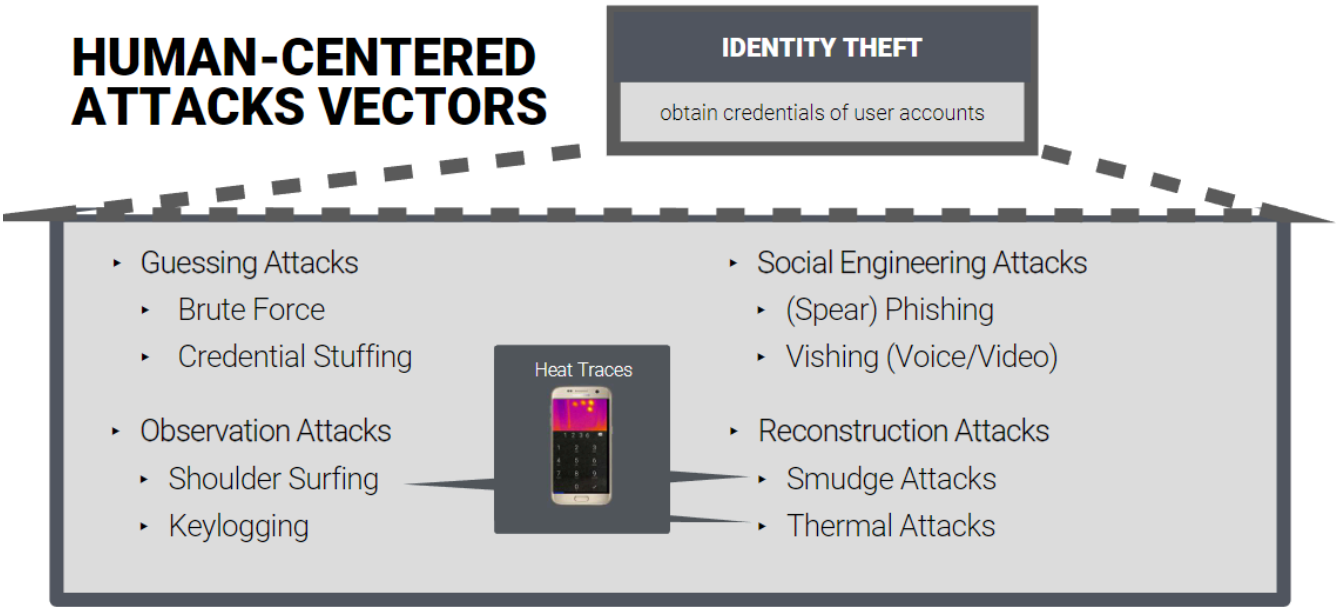
obtain payment information from accounts

RANSOMWARE

encrypt files and demand money for the decryption key

EXTORTIONWARE

exfiltrate (sensitive) information and threaten to publish it



HUMAN-CENTERED ATTACKS VECTORS

IDENTITY THEFT

obtain credentials of user accounts

- Guessing Attacks
  - Brute Force
  - Credential Stuffing
- Observation Attacks
  - Shoulder Surfing
  - Keylogging
- Social Engineering Attacks
  - (Spear) Phishing
  - Vishing (Voice/Video)
- Reconstruction Attacks
  - Smudge Attacks
  - Thermal Attacks

Common Human-Centered Attack Vectors

Attack Type	Description	Example Scenarios
Identity Theft	Stealing credentials to access user accounts	Phishing, credential stuffing
Extortionware	Exfiltrating sensitive data and threatening exposure	Ransom demands
Ransomware	Encrypting files and demanding payment for decryption	Corporate attacks
System Compromise	Gaining root access to a network	Privilege escalation
Financial Fraud	Obtaining payment details for unauthorized transactions	Credit card fraud

How to Prevent Phishing

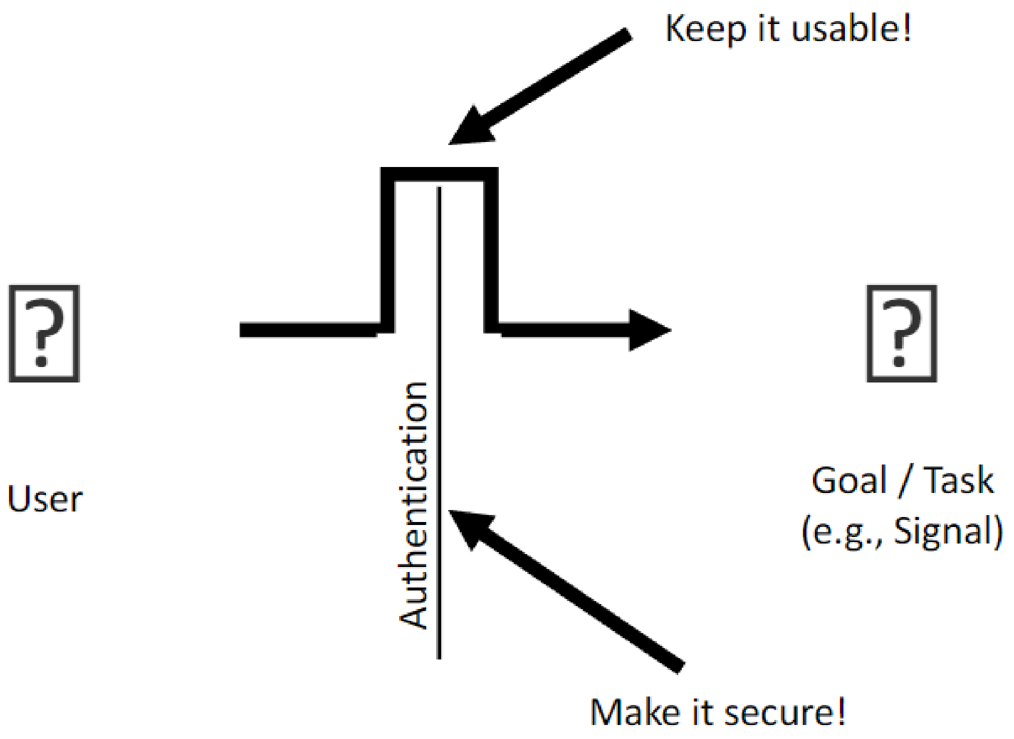
Never click on unexpected email links. Verify sender authenticity and enable multi-factor authentication.

Human-Centered Security Challenges

Security vs. Usability Trade-Off

- Security is often a **secondary task** for users, meaning convenience takes priority.
- **Users want quick access**, while security mechanisms aim to restrict unauthorized entry.
- A study by **Adams et al. (1999)** shows this misalignment between users and security experts.

> **Security vs. Usability - Adams et al. (1999)**
>
> "If security mechanisms are not usable, they are not secure."

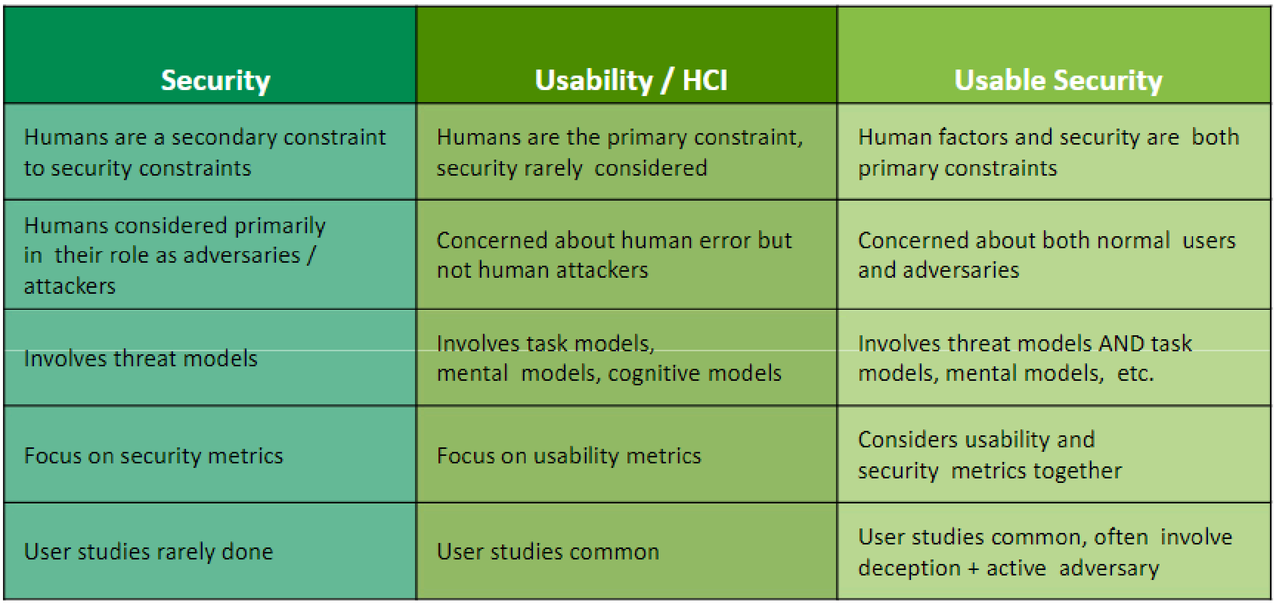


Frequent Authentication Weaknesses

- **Common PINs & Passwords**: Users often pick predictable credentials.
- **Shoulder Surfing & Smudge Attacks**: Observers can reconstruct passwords from traces left on screens.
- **Brute Force & Credential Stuffing**: Automated attempts to guess passwords.
- **Social Engineering**: Manipulating users into revealing credentials.

Why Password Complexity Fails

Users who are forced to create complex passwords **often write them down**, reducing security effectiveness.

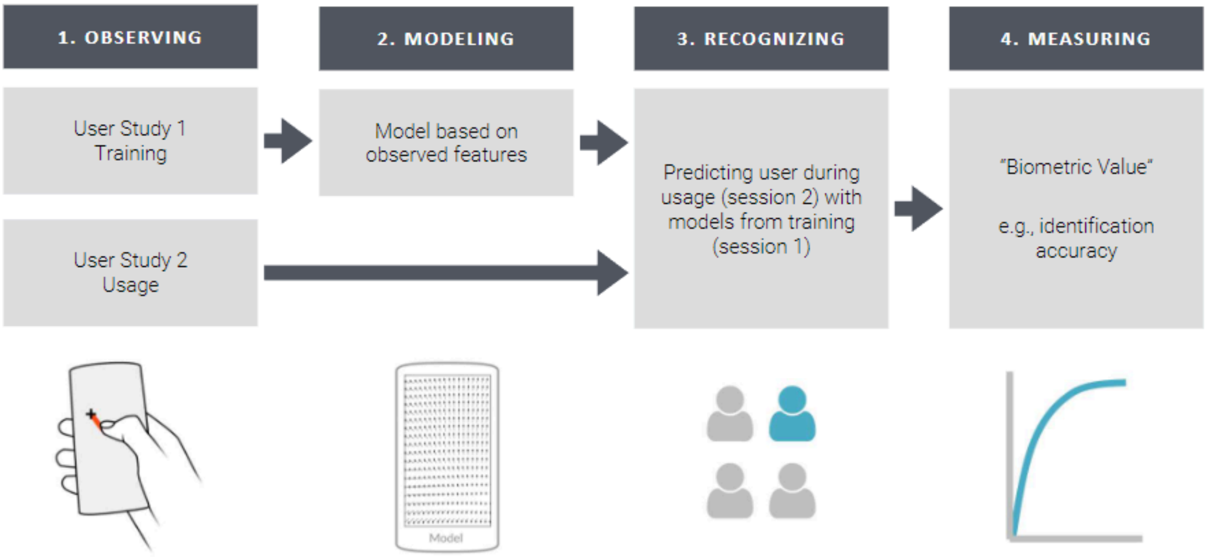


Security	Usability / HCI	Usable Security
Humans are a secondary constraint to security constraints	Humans are the primary constraint, security rarely considered	Human factors and security are both primary constraints
Humans considered primarily in their role as adversaries / attackers	Concerned about human error but not human attackers	Concerned about both normal users and adversaries
Involves threat models	Involves task models, mental models, cognitive models	Involves threat models AND task models, mental models, etc.
Focus on security metrics	Focus on usability metrics	Considers usability and security metrics together
User studies rarely done	User studies common	User studies common, often involve deception + active adversary

Authentication Methods

Behavioral Biometrics

- Users can be identified based on **unique behavioral traits**, such as:
    - **Typing biometrics** (e.g., flight time, hold time)
    - **Gait recognition** (e.g., walking patterns)
    - **Interaction data** (e.g., app usage, touch dynamics)


1. OBSERVING
2. MODELING
3. RECOGNIZING
4. MEASURING
User Study 1 Training
Model based on observed features
Predicting user during usage (session 2) with models from training (session 1)
"Biometric Value"
e.g., identification accuracy
User Study 2 Usage
Model

> 🔍 **Behavioral Biometrics:**
> Unlike passwords, behavioral biometrics continuously authenticate users **without requiring explicit actions**.

Intelligent Authentication Systems

- Security interfaces are integrating **machine learning** to detect anomalies.

- Continuous authentication monitors user behavior to **detect unauthorized access**.
- Example: A system detects unusual typing speed and flags potential impostors.

Privacy Concerns & Transparency

Factors Influencing Privacy Perception

Privacy Concern	Explanation
Device Type	Smart home devices raise more concerns than personal computing devices.
Social Context	People are more comfortable sharing data with close contacts.
Location Sensitivity	Privacy concerns increase in intimate settings (e.g., bedrooms).

Privacy vs. Convenience

Users will trade **privacy for convenience** if benefits outweigh perceived risks.

Transparency & User Control

- Providing **privacy dashboards** enhances user trust.
- Field studies show that users **rarely engage with fine-grained controls** unless actively encouraged.
- Transparency without control **may increase privacy concerns** rather than reduce them.

> **Transparency vs. Control - MobileHCI 22**
>
> "Users prefer having control, but they rarely use it unless directly prompted."

Designing Usable Security & Privacy Interfaces

Balancing Security & Usability

Approach	Benefit	Challenge
Two-Factor Authentication	Adds an extra layer of security	Inconvenient for frequent logins
Password Managers	Reduces password fatigue	Users must trust the tool
Biometric Authentication	Quick & user-friendly	Privacy concerns over data storage

Fine-Grained Privacy Controls

- Traditional **binary permission models** (Allow/Deny) are **too rigid**.
- **Privacy Sliders** allow users to **adjust data sharing levels** dynamically.

> 🔍 **Privacy Sliders:**
> Instead of all-or-nothing permissions, sliders enable users to fine-tune access **based on context and**

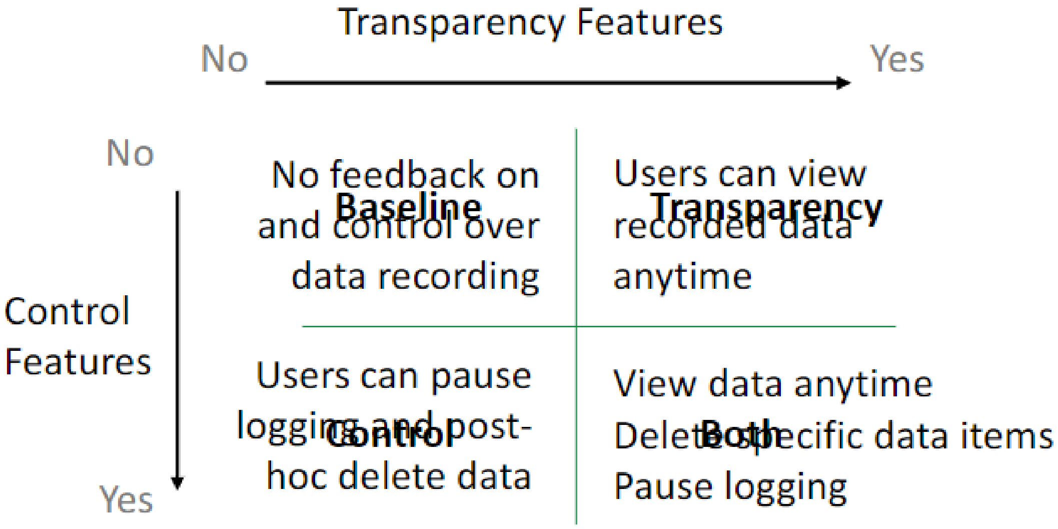
necessity.

Field Study Insights on Security UI Adoption

- **Users prioritize ease of access over security settings.**
- **Warning fatigue** reduces the effectiveness of security prompts.
- **Default settings** strongly influence user behavior.

> **How to Reduce Warning Fatigue**
>
> Use **adaptive security prompts** that trigger only under high-risk scenarios.

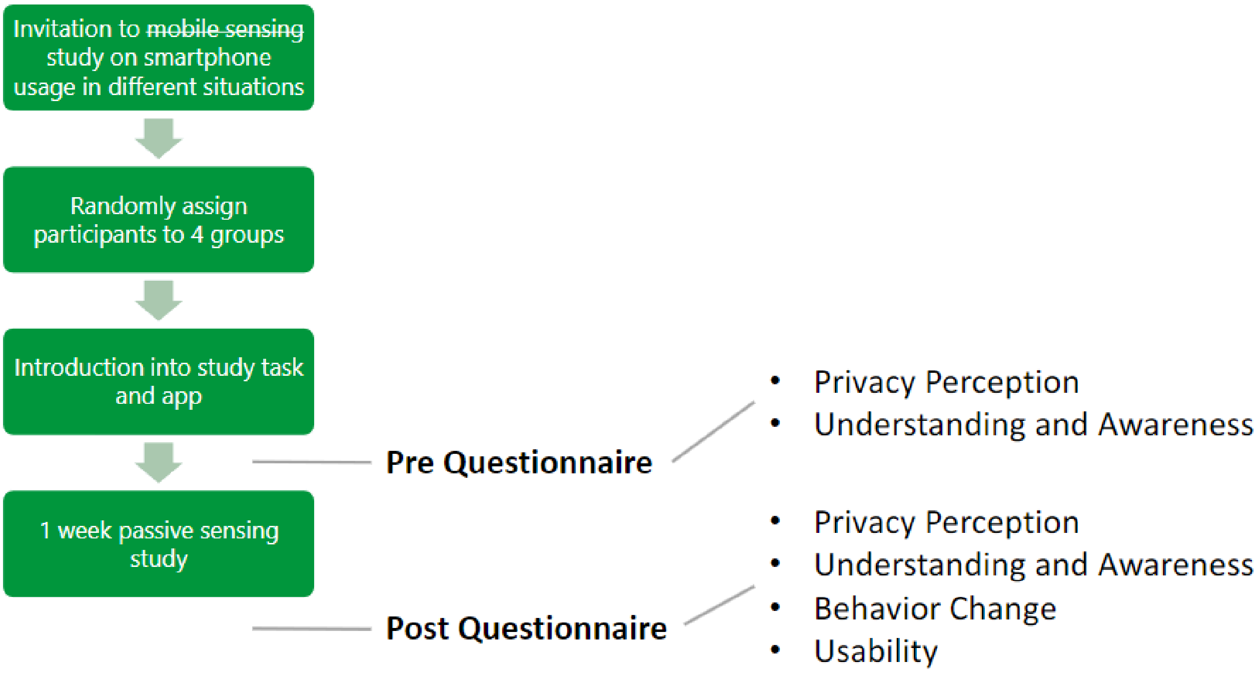
Transparency and Control in Mobile Sensing Apps



Transparency Features

Control Features

	No	Yes
No	**Baseline** No feedback on and control over data recording	**Transparency** Users can view recorded data anytime
Yes	**Control** Users can pause logging and post-hoc delete data	**Both** View data anytime Delete specific data items Pause logging



Invitation to ~~mobile sensing~~ study on smartphone usage in different situations

Randomly assign participants to 4 groups

Introduction into study task and app

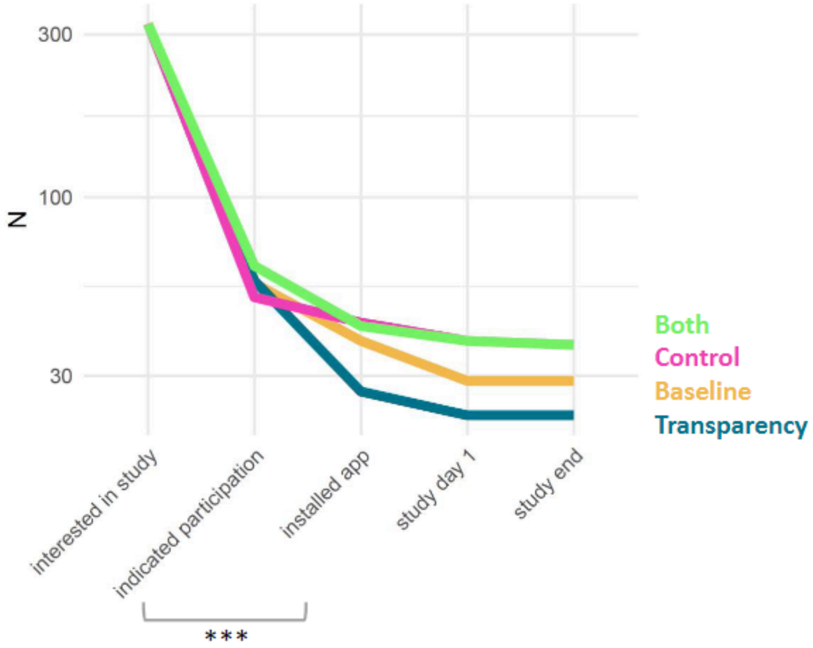
1 week passive sensing study

Pre Questionnaire
- Privacy Perception
- Understanding and Awareness

Post Questionnaire
- Privacy Perception
- Understanding and Awareness
- Behavior Change
- Usability

- **Field Study Design:** A 2x2 factorial design study compared four conditions: baseline, transparency only, control only, and both transparency and control.

- **Findings:** Users provided with transparency features initially showed higher understanding of data logging. However, transparency alone did not significantly improve adoption rates; control features are critical to enhancing user trust.
- **User Behavior:** Despite the availability of control mechanisms, users tend to use them sparingly, indicating that such features should be intuitive and accessible on-demand.



Users in condition *Control* installed the app more likely (84.3%) than *Transparency* users (47.4%)***

$\chi_2(3) = 16.557$, p = .0009 Chi-Square test with post-hoc tests

- **Understanding**- What happens with my data?
  - In the beginning, Transparency users had higher understanding than others
  - Understanding of Transparency users decreased, while the others' increased
- Awareness – What data is logged?
  - Slightly higher knowledge about what is logged for Transparency users
  - Slight improvements during the study period

Importance of Combining Transparency with Control

Ensure that any transparency feature is paired with an easy-to-use control mechanism to help users feel secure without overwhelming them.

Fine-Grain Privacy Control and the Privacy Slider Concept

- **Limitations of Binary Permissions:** Traditional permission systems force users into yes/no decisions, which can be overly restrictive or too permissive.
- **Privacy Slider Concept:**
  - A privacy slider allows users to adjust their data sharing preferences along a continuum rather than making binary choices.
  - Studies indicate that users prefer interfaces that mirror the natural structure of the data (e.g., sliders for continuous values).
- **User Feedback:** While the privacy slider enhances perceived control and transparency, designers must be wary of warning fatigue, where too many alerts can lead to desensitization.