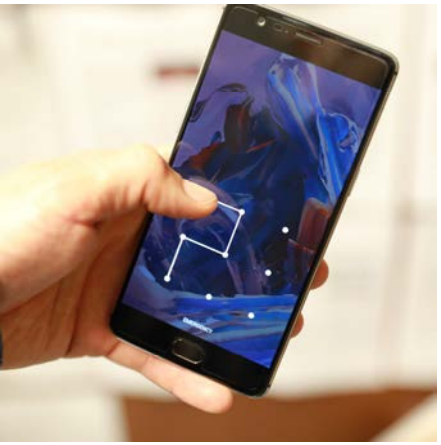
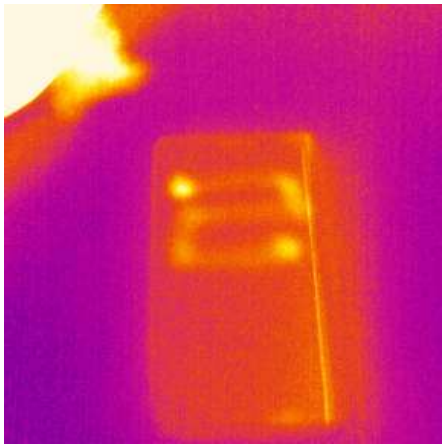
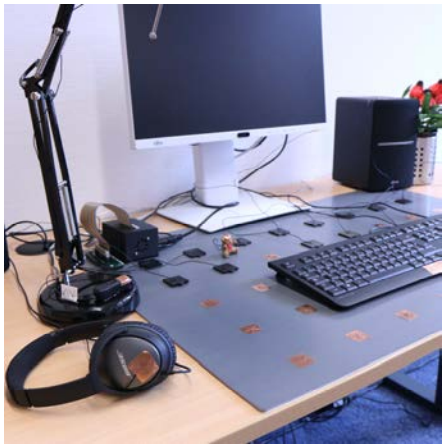
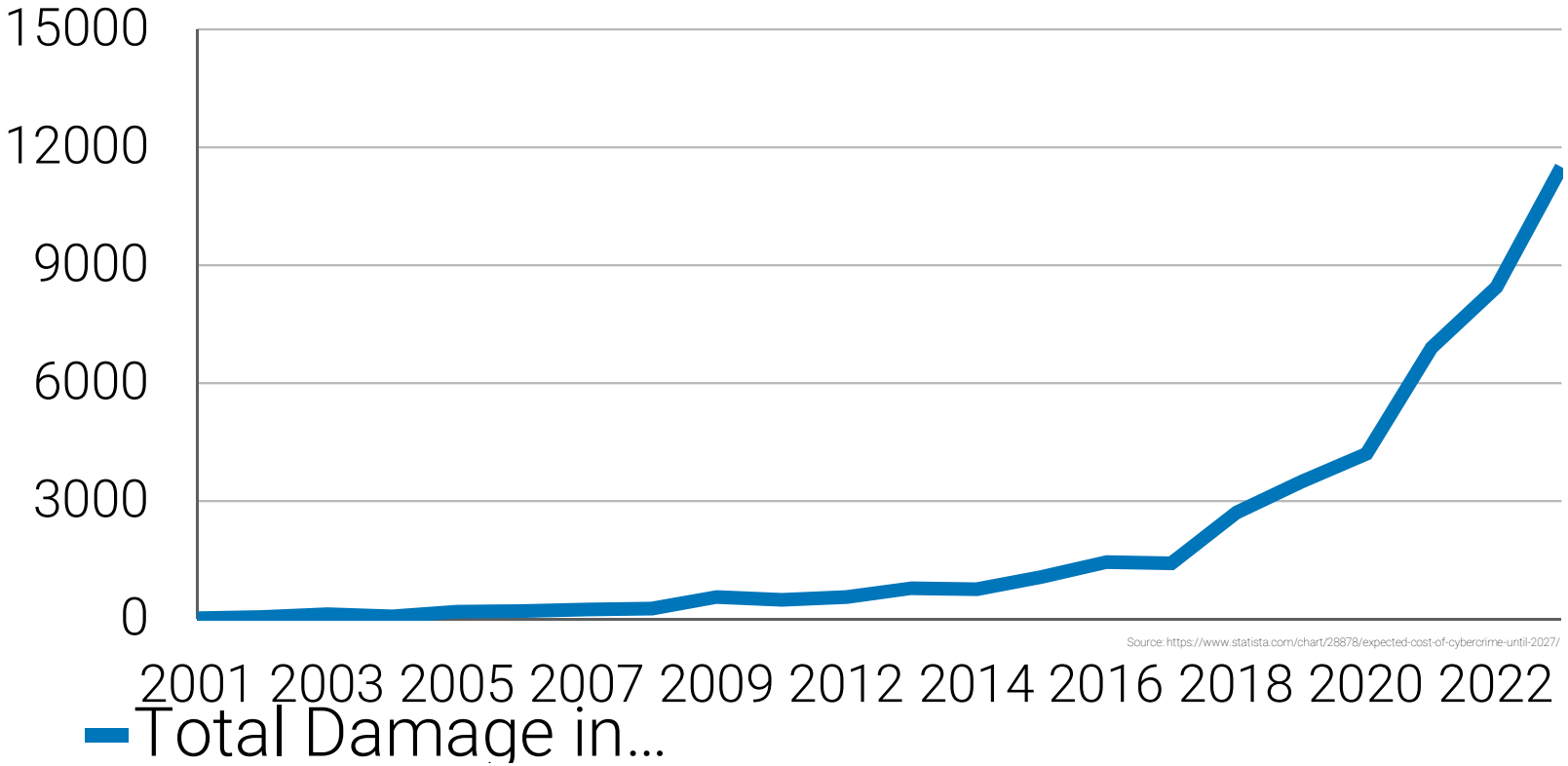



Intelligent Security User Interfaces

Oliver Hein

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



Omnipresent Cyber Attacks

Successful Cyber Attacks on German Universities

in the past 12 months

- 06.10.2023: Uniklinikum Frankfurt
- 02.10.2023: Hochschule Karlsruhe
- 28.09.2023: Universität Göttingen
- 18.09.2023: Hochschule Furtwangen
- 01.07.2023: Universität Düsseldorf
- 09.06.2023: Hochschule Kaiserslautern
- 01.02.2023: TU Ilmenau
- 31.01.2023: Hochschule Ruhr West
- 19.01.2023: Technische Universität Bergakademie Freiberg
- 29.12.2022 HAW Hamburg
- 23.12.2022: FH Zwickau
- 14.12.2022 Universität Duisburg-Essen (again!)
- 27.11.2022 Universität Duisburg-Essen
- 12.11.2022 TH Ulm
- 29.10.2022 Hochschulel Heilbronn

Ransomware, Cybercrime, Data security

Cyberattack against German university claimed by Vice Society

SC Staff January 17, 2023

University of Duisburg-Essen in Germany was hit by a cyberattack in November that has been claimed by the Vice Society ransomware operation, which has also exposed data allegedly stolen from the university, including sensitive details involving its operations, students, and employees, reports BleepingComputer.

UDE, which is having its IT infrastructure overhauled as a result of the attack, emphasized that it will not pay the ransom demanded by Vice Society.

"The university had not complied with the attackers demands and had not paid a ransom," said UDE in a statement.

Further examination of the leaked files by BleepingComputer revealed that Vice Society was able to compromise financial documents, backup archives, student spreadsheets, and research papers although their authenticity could not be verified. Such an attack follows Vice Society's persistent intrusions aimed at the education sector, with the Los Angeles Unified School District, Cincinnati State Technical and Community College, and the Medical University of Innsbruck being attacked by the ransomware operation
year.

HACKERS DON’T BREAK IN —
THEY LOG IN!

TK Keanini (CISCO)

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

Heat Traces

- Social Engineering Attacks
  - (Spear) Phishing
  - Vishing (Voice/Video)
- Reconstruction Attacks
  - Smudge Attacks
  - Thermal Attacks

What are Differences Between HCI and Human-Centered Security?

Security is a Secondary Task

Vs

Goals of the User

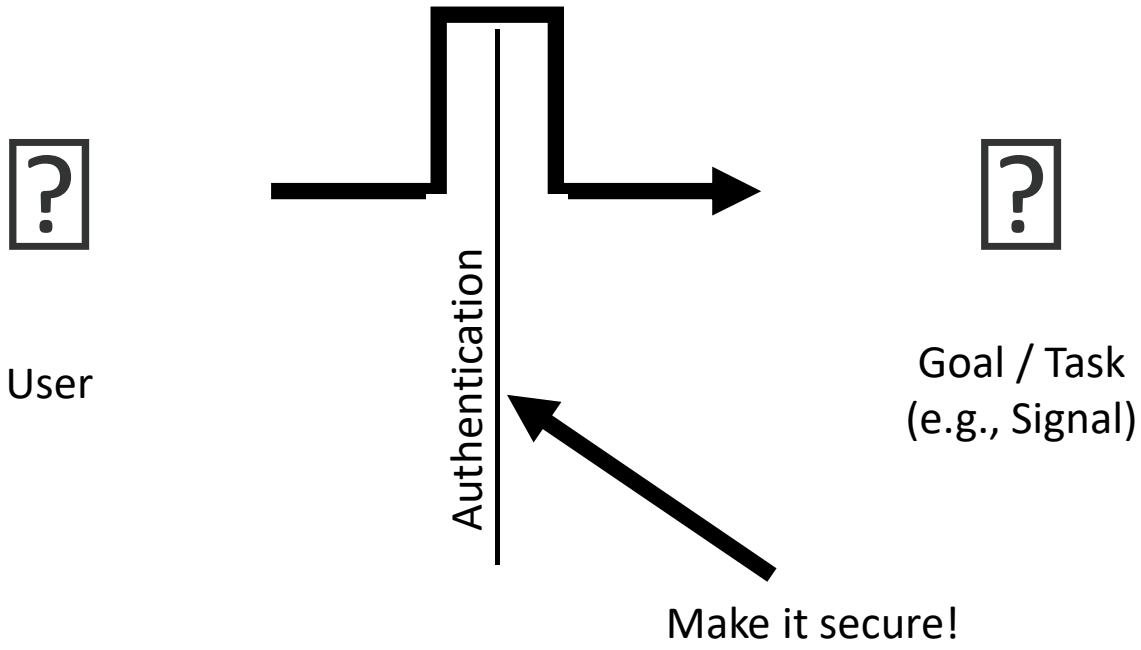
Adams et al., 1999

User

Goal / Task
(e.g., Signal)

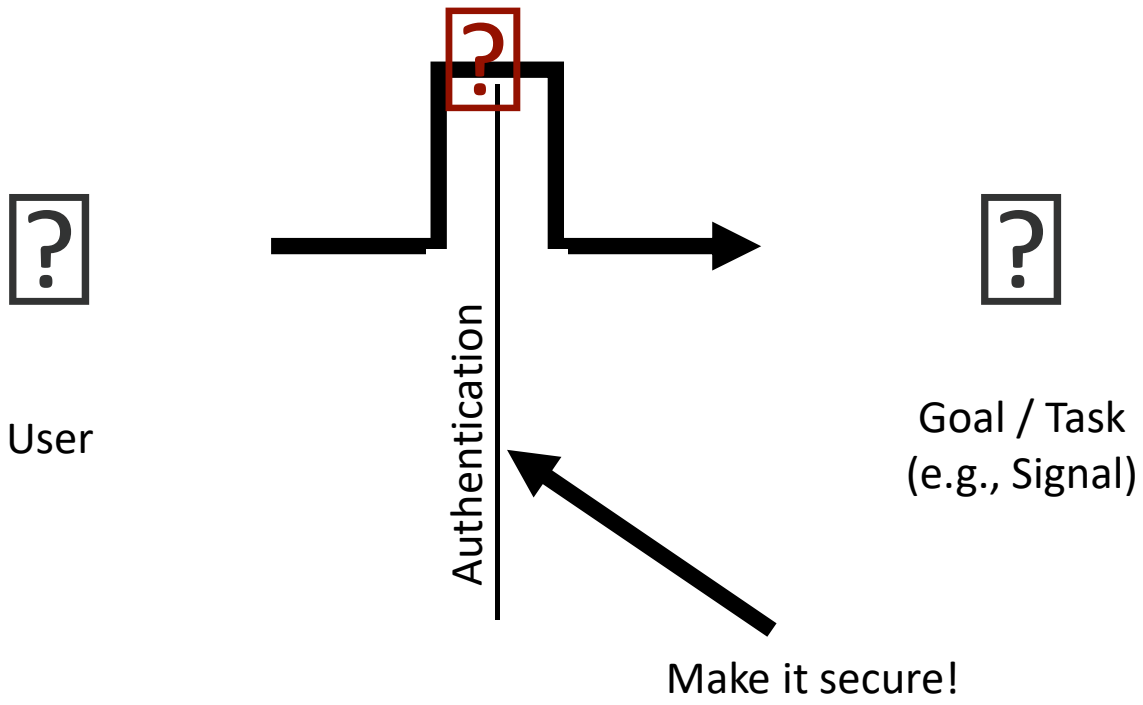
Goals of a Security Expert

Adams et al., 1999



If Mechanisms Are Not Usable They Are Not Secure

Adams et al., 1999



Most Frequent PINs and Passwords

The 25 most frequent PINs

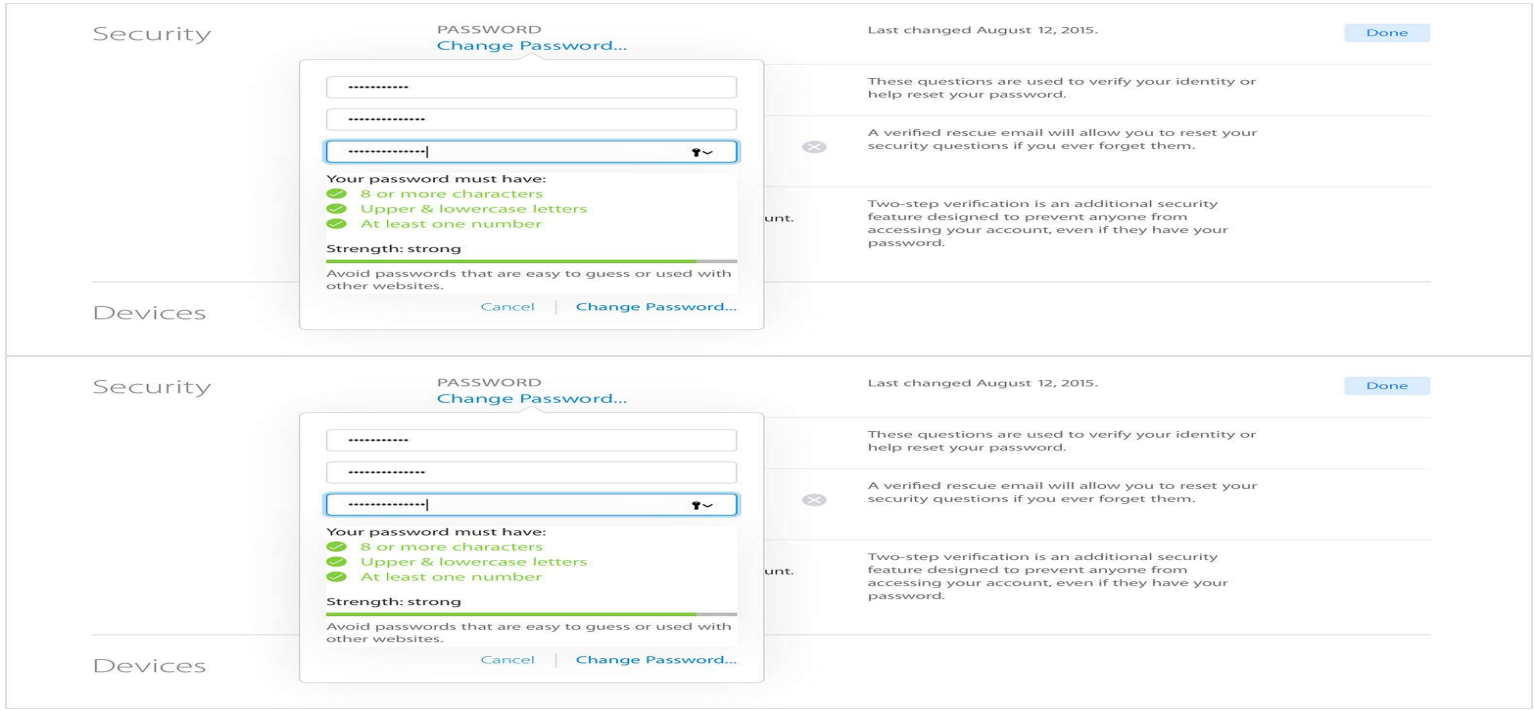
1. 1234
2. 0000
3. 2580
4. 1111
5. 5555
6. 5683
7. 0852
8. 2222
9. 1212
10. 1998
11. 6969
12. 1379
13. 1997
14. 2468
15. 9999
16. 7777
17. 1996
18. 2011
19. 3333
20. 1999
21. 8888
22. 1995
23. 2525
24. 1590
25. 1235

The 25 most frequent passwords

1. password
2. 123456
3. 12345678
4. 1234
5. qwerty
6. 12345
7. dragon
8. pussy
9. baseball
10. football
11. letmein
12. monkey
13. 696969
14. abc123
15. mustang
16. michael
17. shadow
18. master
19. jennifer
20. 111111
21. 2000
22. jordan
23. superman
24. harley
25. 1234567

http://www.netzpiloten.de/die-25-haufigsten-passworter-und-pins/

Password Policies



https://support.apple.com/en-us/HT201303

“Usable” Concepts

Security and Human Factors

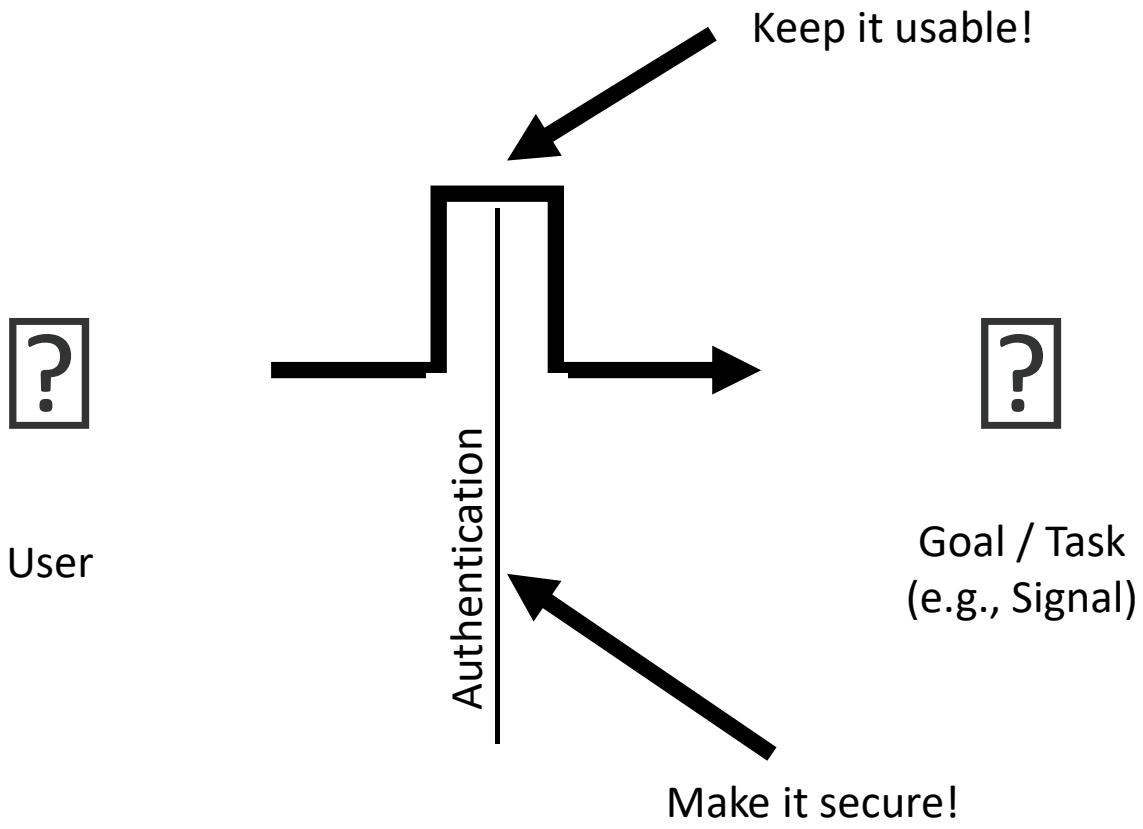
A definition by Jakob Nielson

- “A big lie of computer security is that security improves as password complexity increases. In reality, users simply write down difficult passwords, leaving the system vulnerable. Security is better increased by **designing for how people actually behave**.”

Jakob Nielsen. Security and Human Factors. https://www.nngroup.com/articles/security-and-human-factors/

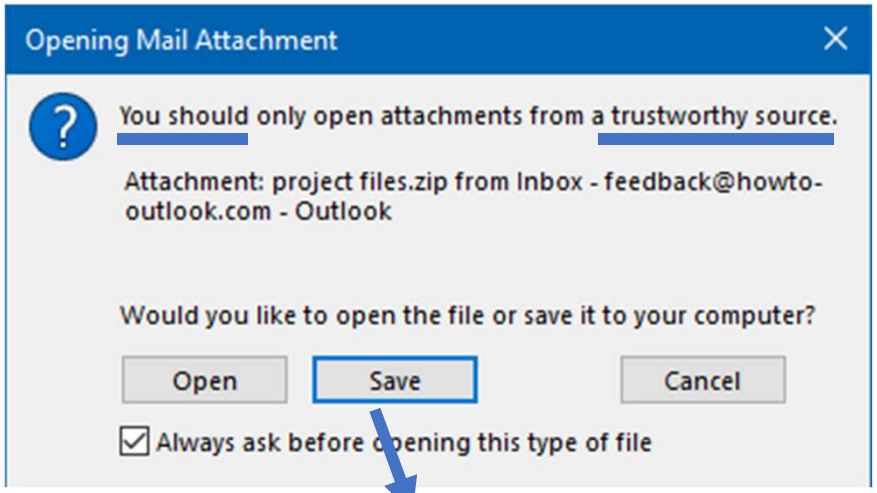
Goals of a Usable Security Expert

Adams et al., 1999



Complex Security Mechanisms

What if I don't?



What makes a source trustworthy?

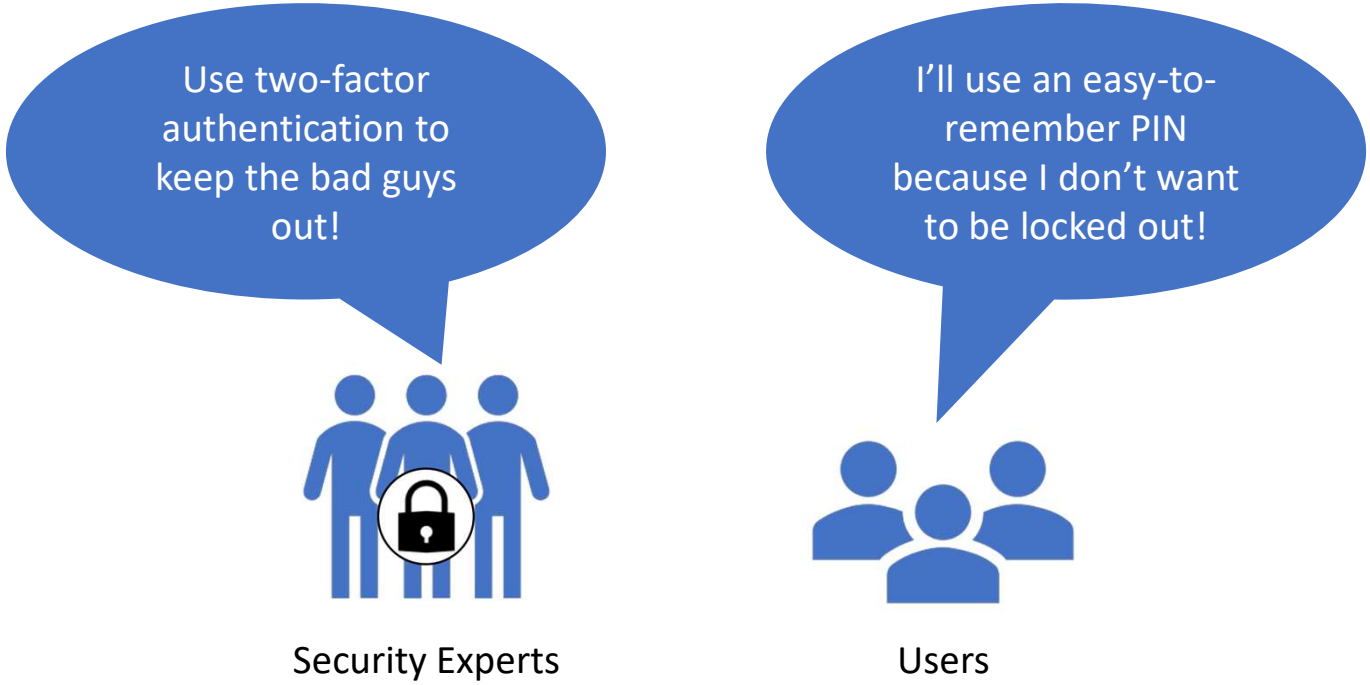
Opening is not okay? I guess this means saving is fine?

Other Examples

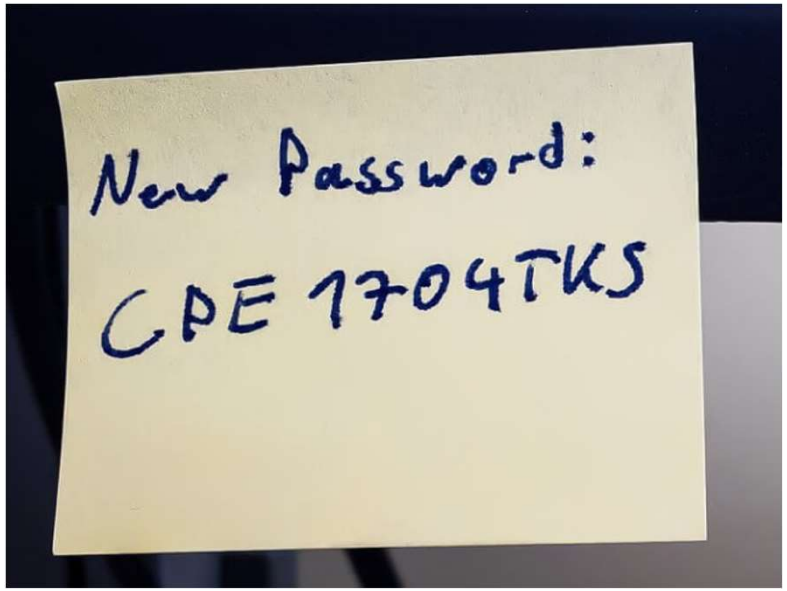
- Virtual Private Networks
- Passwords
  - Secure Password Composition
  - Password Reuse
- Configuration of Smart Home Devies
- Etc.

https://social.technet.microsoft.com/Forums/en-US/f9912914-ad11-4d5c-8b13-756dbca46533/only-open-attachments-from-trustworthy-sources-prompt-popping-up-on-emails-from-people-in-same?forum=outlook

Misaligned Priorities



Limited Capacity of Users



https://techsolvers.com.au/blog/how-to/choose-manage-strong-passwords/

https://me.me/i/changed-all-my-passwords-to-incorrect-so-whenever-i-forget-3419912

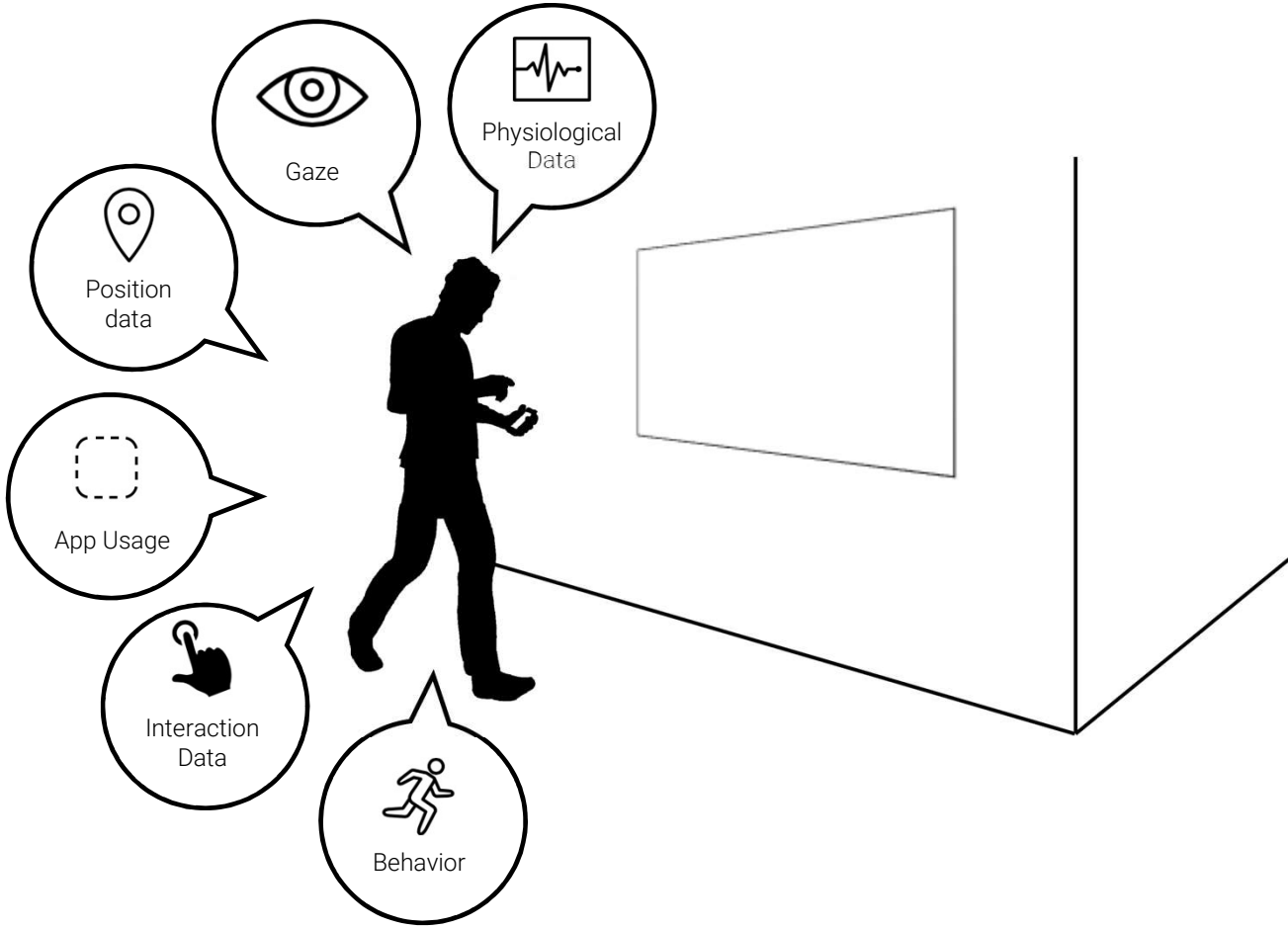
adapted from Lorrie Cranor

Security and Usability Together

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

How to design
security and privacy interfaces
that blend with how we
naturally interact
with computers?

Sensing and actuation moving closer to the human body



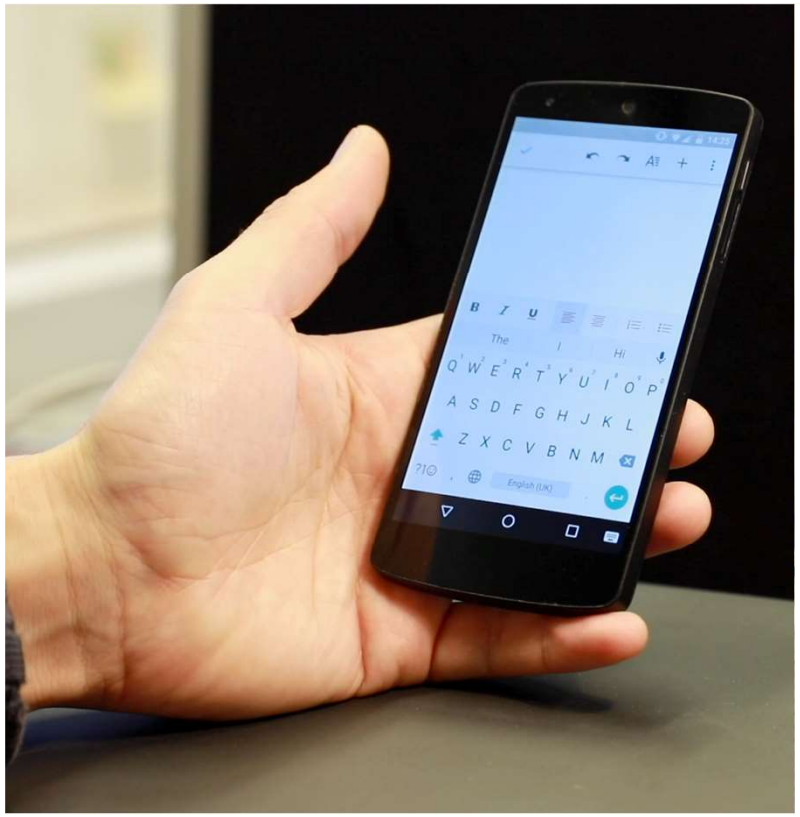
INTELLIGENT AUTHENTICATION

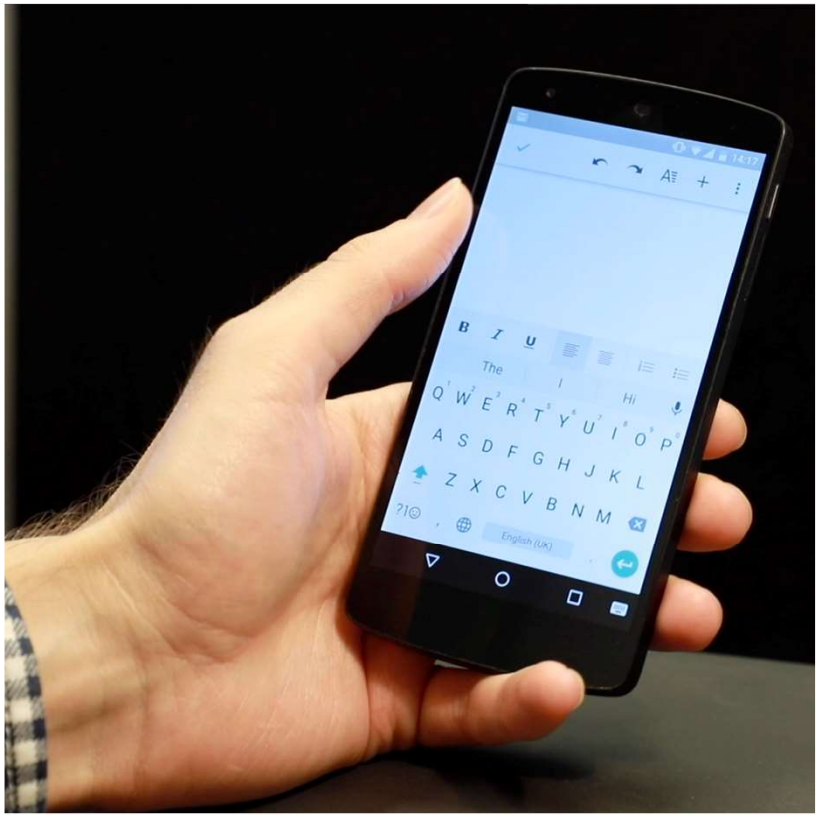
Identifying Users from Behavior

Walking

Identifying Users from Behavior

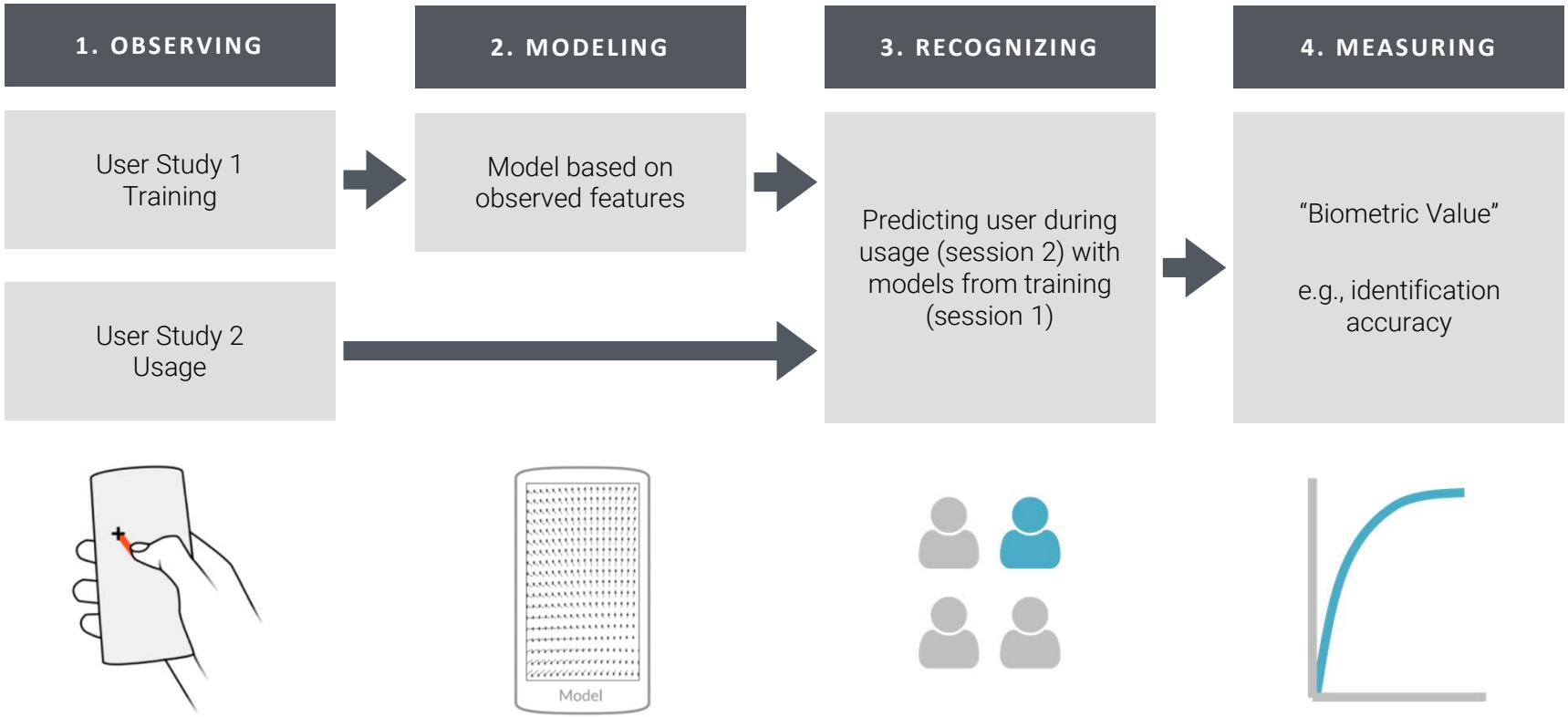
Typing





Typing Biometrics

Building a Behavioral Biometrics System



SHOULDER SURFING

Shoulder Surfing

CHI ’17

Eiband, Khamis, von Zezschwitz, Hussmann, Alt. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers.

- Shoulder surfing exists to a substantial amount in real life but mostly goes unnoticed.
- Observers are opportunistic and rarely act out of reasons other than curiosity and boredom.
- Shoulder surfing affects a broad range of personal information.
- Shoulder surfing leaks personal information about third persons.
- Shoulder surfing puts authentication credentials such as PINs, passwords and patterns at risk.

Understanding Shoulder Surfing in the Wild: Stories from Users and Observers

Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, Florian Alt
Media Informatics Group, LMU Munich, Germany
{malin.eiband, mohamed.khamis, emanuel.von.zezschwitz, hussmann, florian.alt}@ifi.lmu.de

ABSTRACT
Research has brought forth a variety of authentication systems to mitigate observation attacks. However, there is little work about shoulder surfing situations in the real world. We present the results of a user survey (N=174) in which we investigate actual stories about shoulder surfing on mobile devices from both users and observers. Our analysis indicates that shoulder surfing mainly occurs in an opportunistic, non-malicious way. It usually does not have serious consequences, but evokes negative feelings for both parties, resulting in a variety of coping strategies. Observed data was personal in most cases and ranged from information about interests and hobbies to login data and intimate details about third persons and relationships. Thus, our work contributes evidence for shoulder surfing in the real world and informs implications for the design of privacy protection mechanisms.

Author Keywords
Shoulder Surfing; Privacy; Mobile Devices

ACM Classification Keywords
H.5.2 Information Interfaces and Presentation: User Interfaces—*Input devices and strategies*; K.6.5 Computing Milieux: Security and Protection—*Authentication*

INTRODUCTION
At the time of submission of this paper, at least 4640 academic publications indexed on Google scholar are concerned with research on shoulder surfing[1]. The vast majority of these articles (about 4000) have been published since 2007, the year the iPhone entered the market. Not only since then, shoulder surfing – that is the act of observing other people’s information without their consent (see Figure 1) – has served as a fundamental motivation behind much of the work that has been conducted in the area of usable privacy and security. In particular, there is a plethora of work on authentication systems that aim to mitigate shoulder surfing on mobile devices (e.g., [3, 8, 11, 18, 39, 45]).

CHI 2017, May 06 - 11, 2017, Denver, CO, USA

ACM 978-1-4503-4655-9/17/05$15.00
DOI: http://dx.doi.org/10.1145/3025453.3025636

Figure 1. A shoulder surfing situation in a cafe.

At the same time, surprisingly little is known about the phenomenon of shoulder surfing itself. To date, there are no detailed investigations of shoulder surfing incidents and their real-world implications. In fact, findings from Harbach et al. [20] in 2014 showed that only in eleven out of 3410 situations (0.3 %), smartphone users perceived a shoulder surfing risk. Hence, one might wonder, *how much of a threat is shoulder surfing for the user?*

To answer this question, this work contributes the results of an exploratory survey (N=174) that collects actual stories from both perspectives: *users* (the person being shoulder surfed) and *observers* (the shoulder surfer). Stories are not restricted to authentication, but focus on visual privacy in general.

The analysis of the stories revealed that shoulder surfing was mostly casual and opportunistic. There were no stories indicating observation out of malicious intent and/or with technical equipment. Shoulder surfing was most common among strangers, in public transport, during commuting times, and involved a smartphone in almost all cases. Observations uncovered a broad range of mostly personal content, such as information about a user’s interests, hobbies, relationships, sexual preferences, third persons, and login data. Except for two cases, users did not report serious consequences of shoulder surfing. However, both users and observers expressed negative feelings in the respective situation, such as embarrassment and anger or guilt and unease. Users reacted with vari-

[1] https://scholar.google.de/scholar?q=%22shoulder+surfing%22, *accessed 2016/09/20.*

MOBILEHCI 2022

SHOULDER SURFING

—USER PERSPECTIVE

An Investigation of Shoulder Surfing Attacks on Touch-Based Unlock Events

STEFAN SCHNEEGASS, University of Duisburg-Essen, Germany
ALIA SAAD, University of Duisburg-Essen, Germany
ROMAN HEGER, University of Duisburg-Essen, Germany
SARAH DELGADO, University of the Bundeswehr, Germany
ROMINA POGUNTKE, KUKA Deutschland GmbH, Germany
FLORIAN ALT, University of the Bundeswehr, Germany

Fig. 1. User-centered attacks, such as shoulder surfing, are a common privacy threat. They occur in everyday situations; for example, while one is commuting or sitting in a park. We investigate these attacks using an augmented mobile phone system with a fisheye lens to extend the viewport of the front-facing camera capturing the current situation.

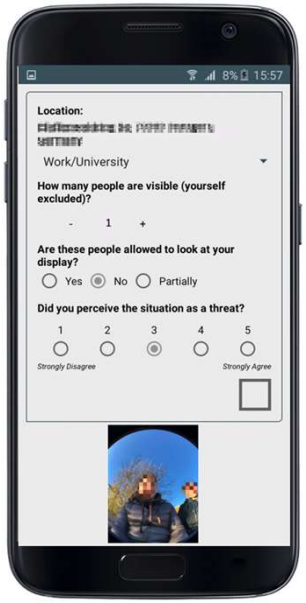
This paper contributes to our understanding of user-centered attacks on smartphones. In particular, we investigate the likelihood of so-called shoulder surfing attacks during touch-based unlock events and provide insights into users' views and perceptions. To do so, we ran a two-week in-the-wild study (N=12) in which we recorded images with a 180-degree field of view lens that was mounted on the smartphone's front-facing camera. In addition, we collected contextual information and allowed participants to assess the situation. We found that only a small fraction of shoulder surfing incidents that occur during authentication are actually perceived as threatening. Furthermore, our findings suggest that our notions of (un)safe places need to be rethought. Our work is complemented by a discussion of implications for future user-centered attack-aware systems. This work can serve as a basis for usable security researchers to better design systems against user-centered attacks.

Authors' addresses: Stefan Schneegass, University of Duisburg-Essen, Schuetzenbahn 70, Essen, Germany, 45127, stefan.schneegass@uni-due.de; Alia Saad, University of Duisburg-Essen, Schuetzenbahn 70, Essen, Germany, 45127, alia.saad@uni-due.de; Roman Heger, University of Duisburg-Essen, Schuetzenbahn 70, Essen, Germany, 45127, roman.heger@uni-due.de; Sarah Delgado, University of the Bundeswehr, Carl-Wery-Str. 20, Munich, Germany, 81739, sarah.delgado@unibw.de; Romina Poguntke, KUKA Deutschland GmbH, Zugspitzstrasse 140, Augsburg, Germany, 86165, Romina.poguntke@hs-kempten.de; Florian Alt, University of the Bundeswehr, Carl-Wery-Str. 20, Munich, Germany, 81739, florian.alt@unibw.de.

2573-0142/2022/9-ART207 $15.00
https://doi.org/10.1145/3546742

Proc. ACM Hum.-Comput. Interact., Vol. 6, No. MHCI, Article 207. Publication date: September 2022.

Methodology



AVI 2022

SHOULDER SURFING

—OBSERVER PERSPECTIVE

Understanding Shoulder Surfer Behavior and Attack Patterns Using Virtual Reality

Yasmeen Abdrabou
yasmeen.essam@unibw.de
University of the Bundeswehr Munich
University of Glasgow
United Kingdom

Radiah Rivu
sheikh.rivu@unibw.de
University of the Bundeswehr Munich
Germany

Tarek Ammar
tarek.ammar@campus.lmu.de
LMU Munich
Germany

Jonathan Liebers
jonathan.liebers@uni-due.de
University of Duisburg-Essen
Germany

Alia Saad
alia.saad@uni-due.de
University of Duisburg-Essen
Germany

Carina Liebers
carina.liebers@uni-due.de
University of Duisburg-Essen
Germany

Uwe Gruenefeld
uwe.gruenefeld@uni-due.de
University of Duisburg-Essen
Germany

Pascal Knierim
pascal.knierim@unibw.de
University of the Bundeswehr Munich
Germany

Mohamed Khamis
mohamed.khamis@glasgow.ac.uk
University of Glasgow
United Kingdom

Ville Mäkelä
ville.makela@uwaterloo.ca
University of Waterloo
Canada

Stefan Schneegass
stefan.schneegass@uni-due.de
University of Duisburg-Essen
Germany

Florian Alt
florian.alt@unibw.de
University of the Bundeswehr Munich
Germany

ABSTRACT

In this work, we explore attacker behavior during shoulder surfing. As such behavior is often opportunistic and difficult to observe in real world settings, we leverage the capabilities of virtual reality (VR). We recruited 24 participants and observed their behavior in two virtual waiting scenarios: at a bus stop and in an open office space. In both scenarios, participants shoulder surfed private screens displaying different types of content. From the results we derive an understanding of factors influencing shoulder surfing behavior, reveal common attack patterns, and sketch a behavioral shoulder surfing model. Our work suggests directions for future research on shoulder surfing and can serve as a basis for creating novel approaches to mitigate shoulder surfing.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**;

KEYWORDS

Shoulder Surfing, User Behavior, Eye Tracking, Virtual Reality

AVI 2022, June 6–10, 2022, Frascati, Rome, Italy

ACM ISBN 978-1-4503-9719-3/22/06…$15.00
https://doi.org/10.1145/3531073.3531106

ACM Reference Format:
Yasmeen Abdrabou, Radiah Rivu, Tarek Ammar, Jonathan Liebers, Alia Saad, Carina Liebers, Uwe Gruenefeld, Pascal Knierim, Mohamed Khamis, Ville Mäkelä, Stefan Schneegass, and Florian Alt. 2022. Understanding Shoulder Surfer Behavior and Attack Patterns Using Virtual Reality. In *Proceedings of the 2022 International Conference on Advanced Visual Interfaces (AVI 2022), June 6–10, 2022, Frascati, Rome, Italy.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3531073.3531106

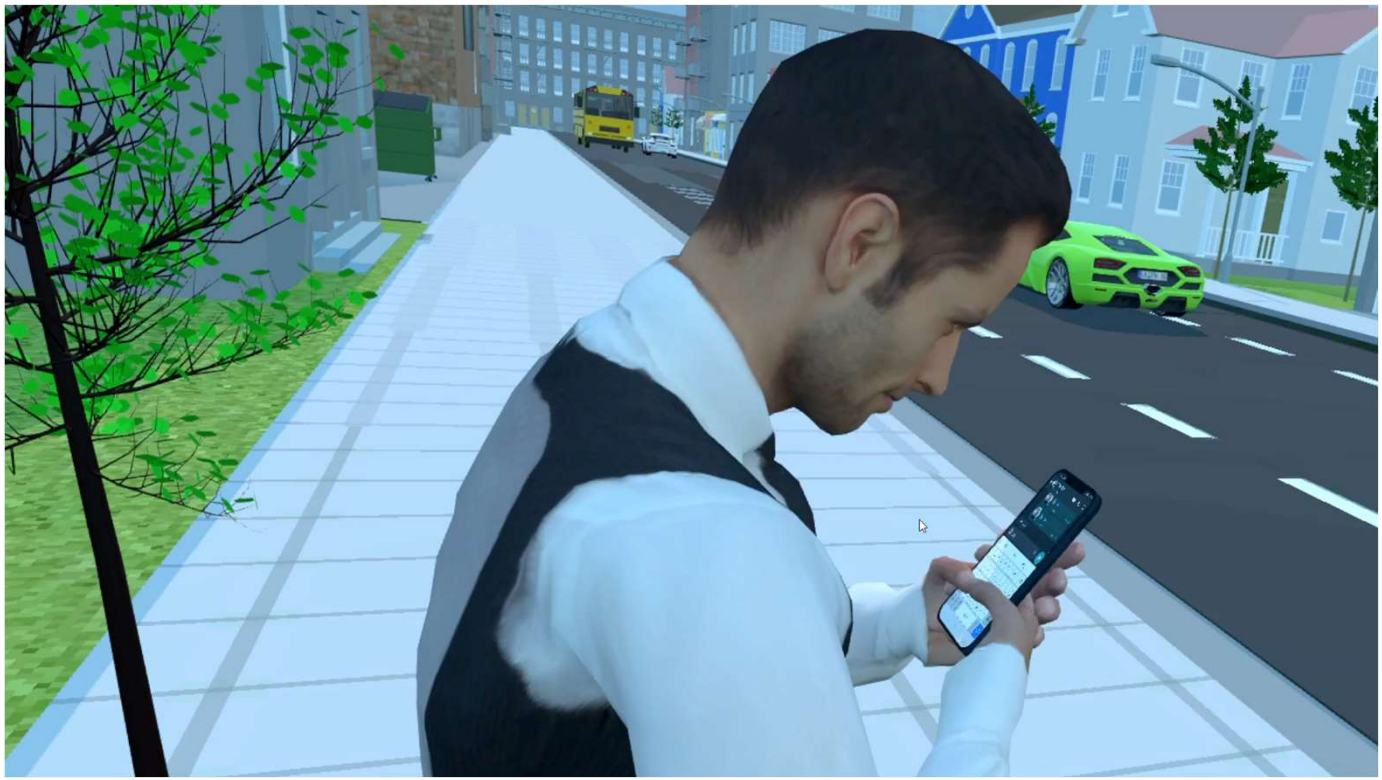
1 INTRODUCTION

Shoulder surfing is the act of observing the device screen of other people without their permission [12]. It can occur anywhere and at anytime, making it a common threat to users. Shoulder surfing has received considerable attention from the HCI and usable security communities [7, 12, 31, 34]. Shoulder surfing occurs in various situations and it has considerable negative implications on users [12, 19]. At the same time, we are currently missing an in-depth understanding of how attacks happen and what strategies attackers follow in their attempts. Answering these questions will help designers and practitioners create solutions that can counteract shoulder surfing attacks, providing users with better protection.

Shoulder surfing behavior is difficult to investigate in the real world because it frequently occurs in complex scenarios. Furthermore, from an ethical perspective, undertaking such in-the-wild studies is challenging [39]. Researchers attempted to address this in different ways. For example, Eiband et al. *asked people* about their shoulder surfing behavior in an online survey [12]. Marques et al. *collected stories* from people to learn how they feel about unauthorized access to their smartphones [19]. Although such research

Methodology

VIRTUAL REALITY STUDY



Shoulder Surfing

VALIDATION IN THE REAL WORLD

Technology

Task and Environment

Increasing User Awareness

Figure 3. DSSytem interface in case of shoulder surfing: LED flash light is on(Left), a preview of the front camera appears (second to left) , vibration(second to right) and icon overlay (right)

Communicating Shoulder Surfing Attacks to Users

Alia Saad[1,2], Michael Chukwu[2], Stefan Schneegass[2]
[1]German University in Cairo, Cairo, Egypt, Alia.khaled@guc.edu.eg
[2]University of Duisburg-Essen, Essen, Germany, stefan.schneegass@uni-due.de

ABSTRACT
Since mobile interaction takes place in almost every context, shoulder surfing attacks are becoming more and more a threat to user's privacy. While several approaches exist to prevent these attacks for the authentication process, protecting the actual interaction has not yet been in the main focus of research. In this work, we present the concept of communicating shoulder surfing attacks to the user. This should create awareness on the user side and help preventing this type of privacy invasion. We present out shoulder surfer detection mobile application, called DSSytem, and report on a focus group that helped to design this system. We also report on the results of a user study in which we compare four different notification methods, namely, vibro-tactile, front LED, on-screen icon, and video preview feedback. Vibro-tactile feedback results in the lowest reaction time of the participants and is also favoured throughout the follow-up semi-structured interviews.

CCS Concepts
•**Security and privacy** → **Usability in security and privacy;**

Author Keywords
Shoulder Surfing; Notification; Usable Security and Privacy.

INTRODUCTION
Mobile devices are essential in modern day life. They are used to handle private information, communicate with family and friends, and store pictures of recent life events. While classical desktop computers are mainly used at home, mobile devices are used in various public situations. This results in novel challenges for protecting the user's content since unauthorized bystanders can peek on the mobile's display. These so called shoulder surfing attacks [24] can be used to gain insights on the user's passwords but also on other private information. Thus, shoulder surfing is considered to be one of the most severe threats to an individual's privacy [12].

Most of the recently introduced countermeasures are directed towards protecting the user authentication process since it is one of the most crucial moments from a security perspective. These previous solutions varied from gaze-based passwords, graphical unlock patterns, gestures for authentication to the deployment of external hardware [2, 7, 12, 15]. While such approaches are efficient in preventing the shoulder surfer from capturing and figuring out the authentication credentials, they do not protect the entire interaction of the user.

MUM '18, November 25–28, 2018, Cairo, Egypt

ISBN 978-1-4503-6594-9/18/11…$15.00
DOI: https://doi.org/10.1145/3282894.3282919

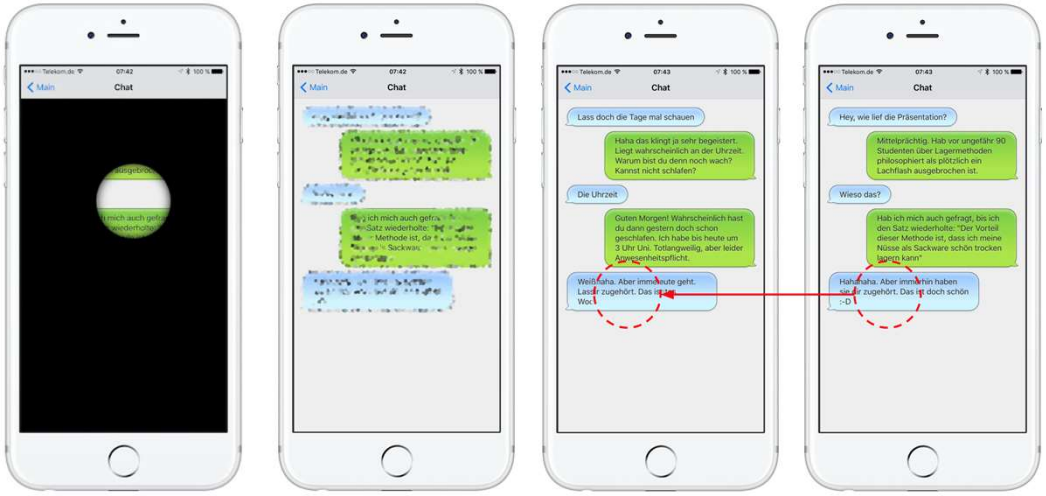
Figure 1. An attacker is shoulder surfing while a user is interacting with the phone.

In this work, we investigate how we can protect the entire interaction of a user with the mobile phone from shoulder surfing attacks. One of the main challenges of preventing shoulder surfing attacks is to perceive that attacker. This is challenging when the attacker is positioned at a blind spot, either at the back or at the sides of the user. To tackle this challenge, we present DSSytem, a system that detects shoulder surfers and notifies the user on such an attack. It uses the front facing camera of the mobile device to detect shoulder surfers peeking from behind the user and notifies the user using four different feedback methods, namely, vibro-tactile feedback, front LED blinking, iconic screen overlay, and live video stream. We report on the user-centered design process of DSSytem and an evaluation comparing the different feedback methods.

CONTRIBUTION STATEMENT
The contributions of the paper are presented as follows:

1. The design and implementation of a notification system that detects and communicates the event of shoulder surfing to users.
2. A comparison between four notification approaches to define the most suitable form of communication of shoulder surfing incidents, following users' preferences.

Shoulder Surfing Protection



Article

EyeSpot: Leveraging Gaze to Protect Private Text Content on Mobile Devices from Shoulder Surfing

Mohamed Khamis[1,2,*], Malin Eiband [1], Martin Zürn [1] and Heinrich Hussmann [1]

[1] Media Informatics Group Ludwig Maximilian University of Munich, 80337 München, Germany; malin.eiband@ifi.lmu.de (M.E.); martin.zuern@campus.lmu.de (M.Z.); heinrich.hussmann@ifi.lmu.de (H.H.)
[2] Glasgow Interactive Systems Section School of Computing Science University of Glasgow, Glasgow, G12 8RZ, Scotland
* Correspondence: mohamed.khamis@ifi.lmu.de; Tel.: +49-163-485-6721

Received: 10 June 2018; Accepted: 25 July 2018; Published: date

Abstract: As mobile devices allow access to an increasing amount of private data, using them in public can potentially leak sensitive information through shoulder surfing. This includes personal private data (e.g., in chat conversations) and business-related content (e.g., in emails). Leaking the former might infringe on users' privacy, while leaking the latter is considered a breach of the EU's General Data Protection Regulation as of May 2018. This creates a need for systems that protect sensitive data in public. We introduce EyeSpot, a technique that displays content through a spot that follows the user's gaze while hiding the rest of the screen from an observer's view through overlaid masks. We explore different configurations for EyeSpot in a user study in terms of users' reading speed, text comprehension, and perceived workload. While our system is a proof of concept, we identify crystallized masks as a promising design candidate for further evaluation with regard to the security of the system in a shoulder surfing scenario.

Keywords: mobile devices; privacy; gaze; eye tracking; security

1. Introduction

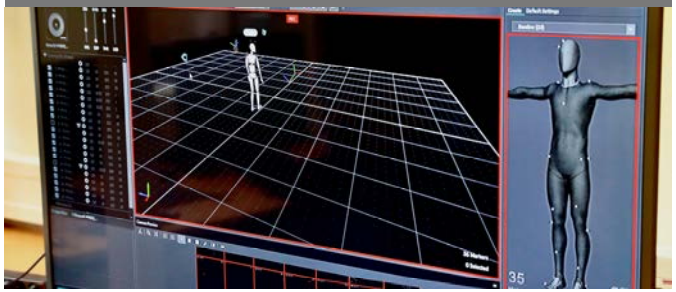
Users interact with their mobile devices in different contexts, ranging from private spaces, such as homes and offices, to public areas such as public transport, transit areas, and workplaces. However, the convenience of being able to access sensitive data anywhere comes with the risk of exposing private information to bystanders through shoulder surfing. A survey by Eiband et al. revealed that interactions on mobile devices are often observed by bystanders which may leak sensitive private information about, for example, the user's personal relationships, interests and plans [1]. These problems may potentially become more prominent with the increased popularity of larger screens of smartphones and tablets where the content that users are not interacting with is unnecessarily exposed. Leaking business-related third-person data when working on the go, such as information about customers and employees, is even deemed a breach of the EU's General Data Protection Regulation as of May 2018 [2]. Furthermore, with growing tendency and expectations by employers and society to be always accessible, employees are more likely to engage in acts that compromise privacy, such as reading sensitive emails on the train.

This creates a need for systems that protect users' "visual privacy" [3,4] in public. While prior work presented various approaches to mitigate the shoulder surfing of credentials [5–7], the protection of other data is relatively underexplored with the exception of few works that we discuss further in Section 2 [4,8]. This work focuses on protecting sensitive text that is normally shown on screens, and hence, visible to bystanders.

We introduce EyeSpot, a technique inspired by prior work on visual privacy protection [4,9] and privacy protection with eye tracking [8,10,11]. EyeSpot utilizes the user's gaze to protect their visual privacy when interacting with a handheld mobile device. As illustrated in Figure 1, the on-screen content is hidden through overlaid masks while revealing the "spot" the user is gazing at. This allows

Research Areas

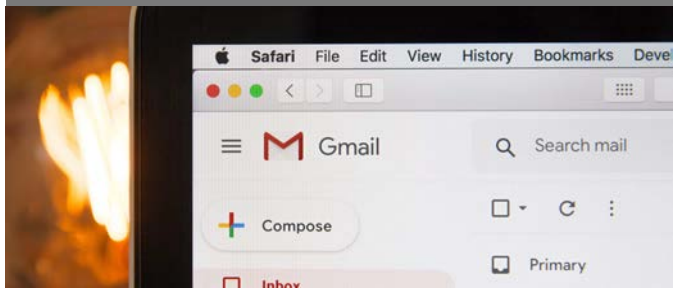
Behavioral Biometrics



Physiology-based Security UIs

Mixed Reality Privacy & Security

Social Engineering



Security & Privacy in Smart Homes

Tangible Human-Centered Security

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

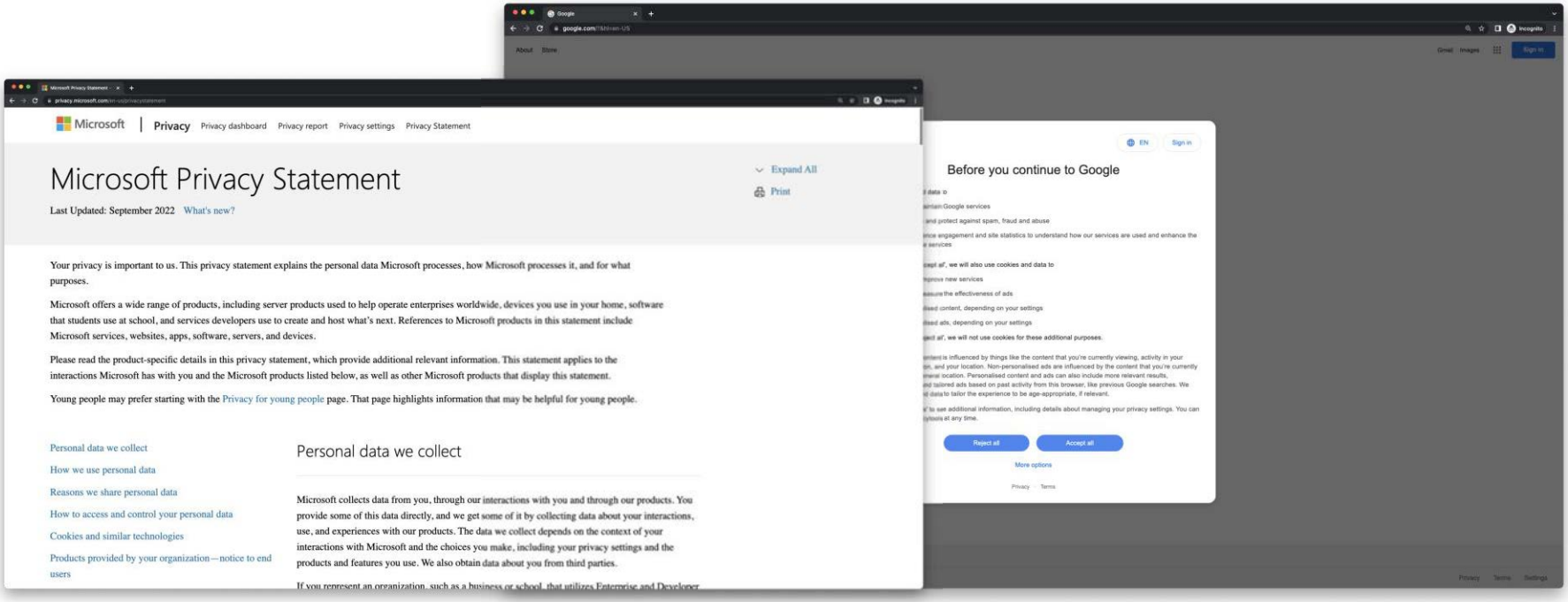
Media Informatics Group

Human-Centered Privacy in Intelligent Environments

Maximiliane Windl

IUI, 11th of December 2024

While we Have Measures Online…



… We Lack Mechanisms for Intelligent Environments

Toward Privacy-Preserving Intelligent Environments

Understanding people’s concerns in smart environments.

Approaches to mitigate concerns in smart home environments.

Approaches to mitigate concerns for advanced and emerging technologies.

The Skewed Privacy Concerns of Bystanders in Smart Environments

Maximiliane Windl and Sven Mayer

Hypotheses

H1: Different devices pose different privacy concerns.

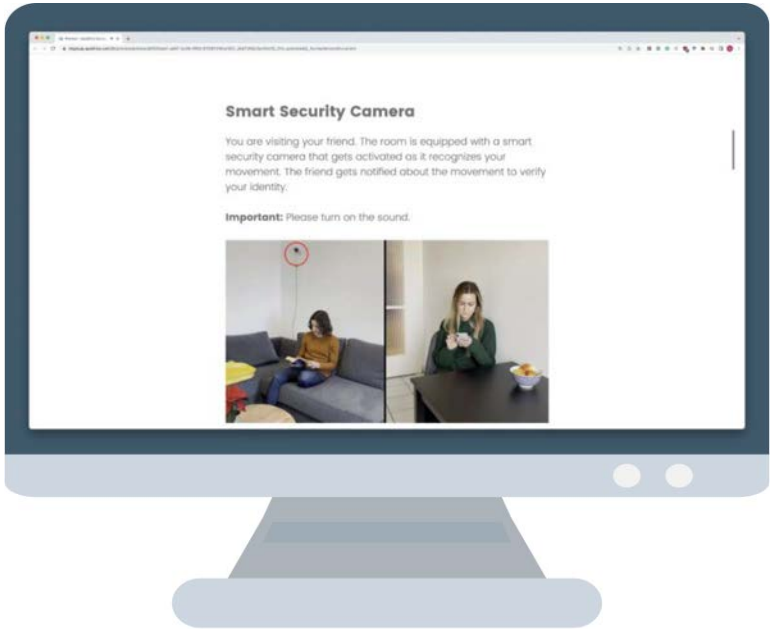
H2a: Bystanders perceive smart home devices as generally more privacy-concerning than personal computing devices.

H3: A stronger social relationship with a device owner reduces privacy concerns.

H4: Bystanders' privacy concerns increase the more intimate the usage location is.

H5: Ownership reduces privacy concerns.

Method



- Online Survey (N=170)
- 10 Devices
- 5 social relationships
- Videos to showcase interactions
- Rating on a 100 point scale

The 10 Devices

Smart Display

Smart Speaker

Smart Doorbell

Smart Security Camera

Smart Lights

Laptop

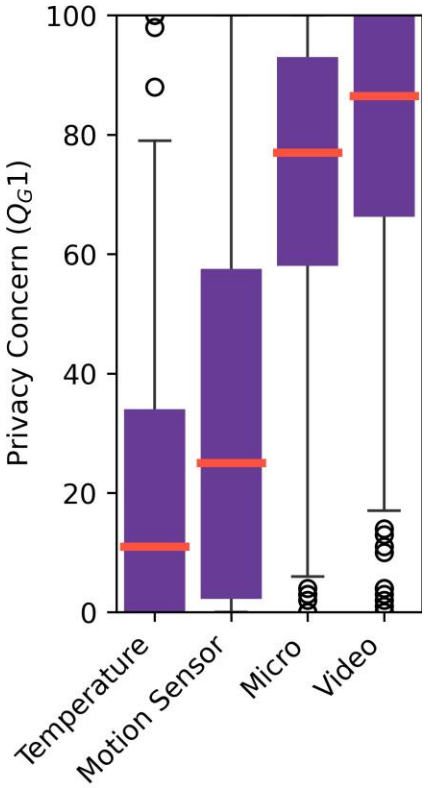
Smartwatch

Personal Computer

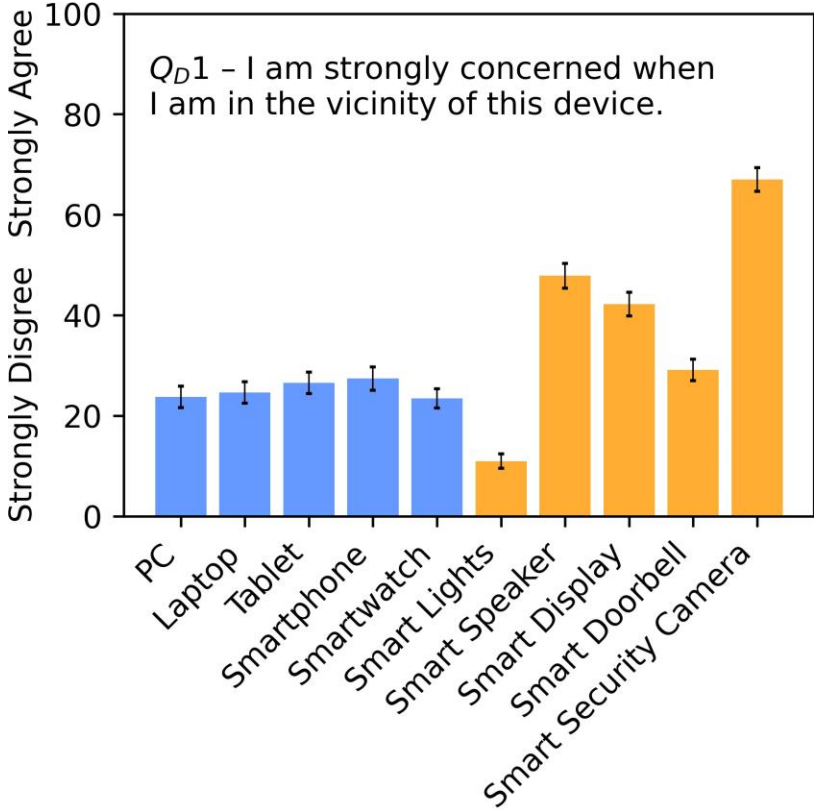
Smartphone

Tablet

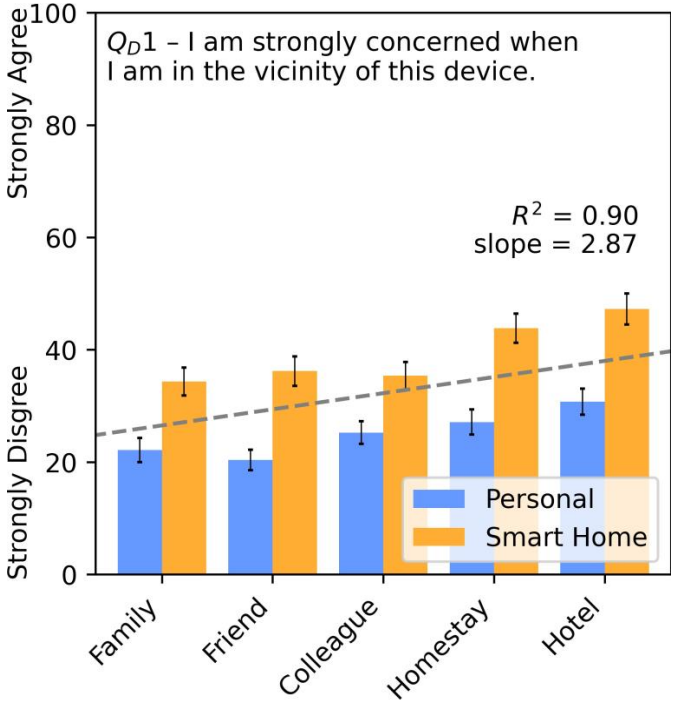
H1: Different devices pose different privacy concerns



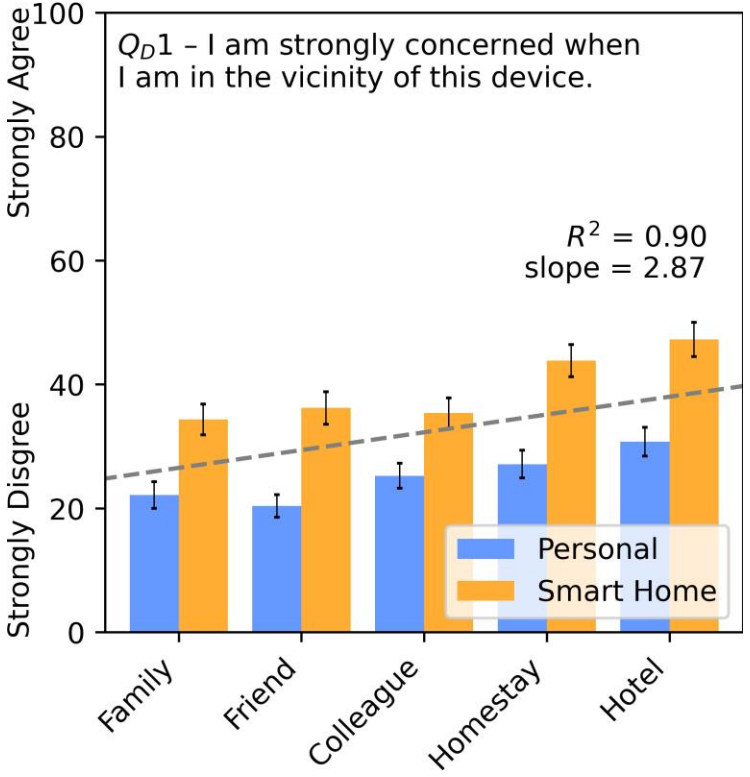
H1: Different devices pose different privacy concerns



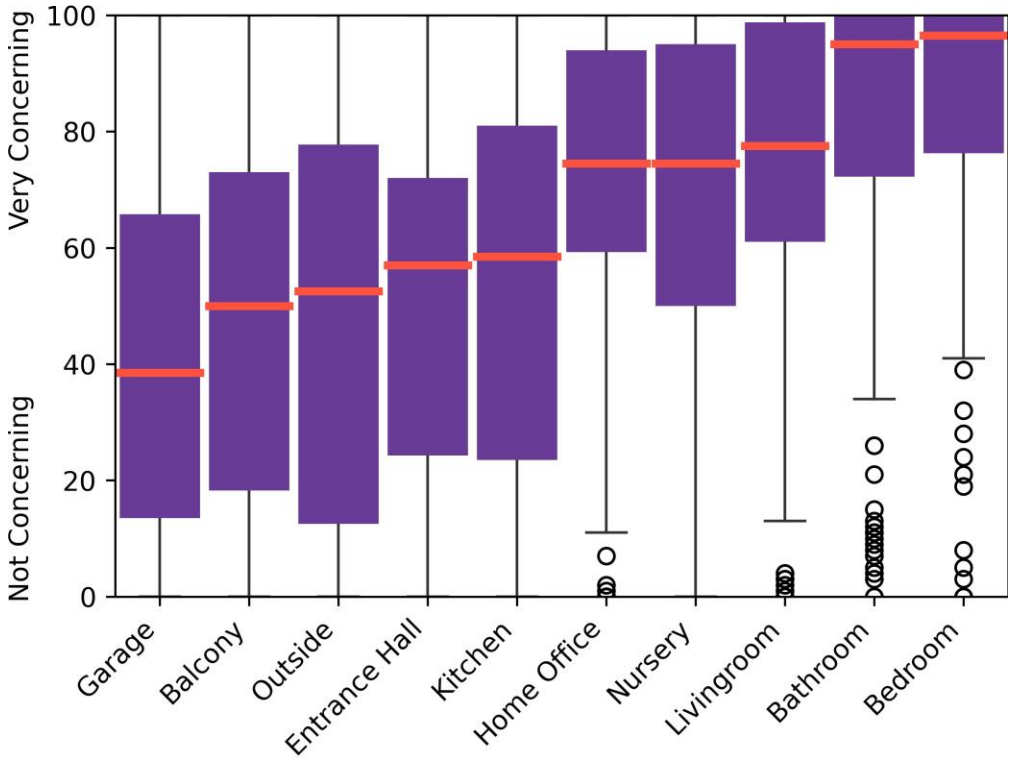
H2a: Bystanders perceive smart home devices as generally more privacy concerning than personal computing devices



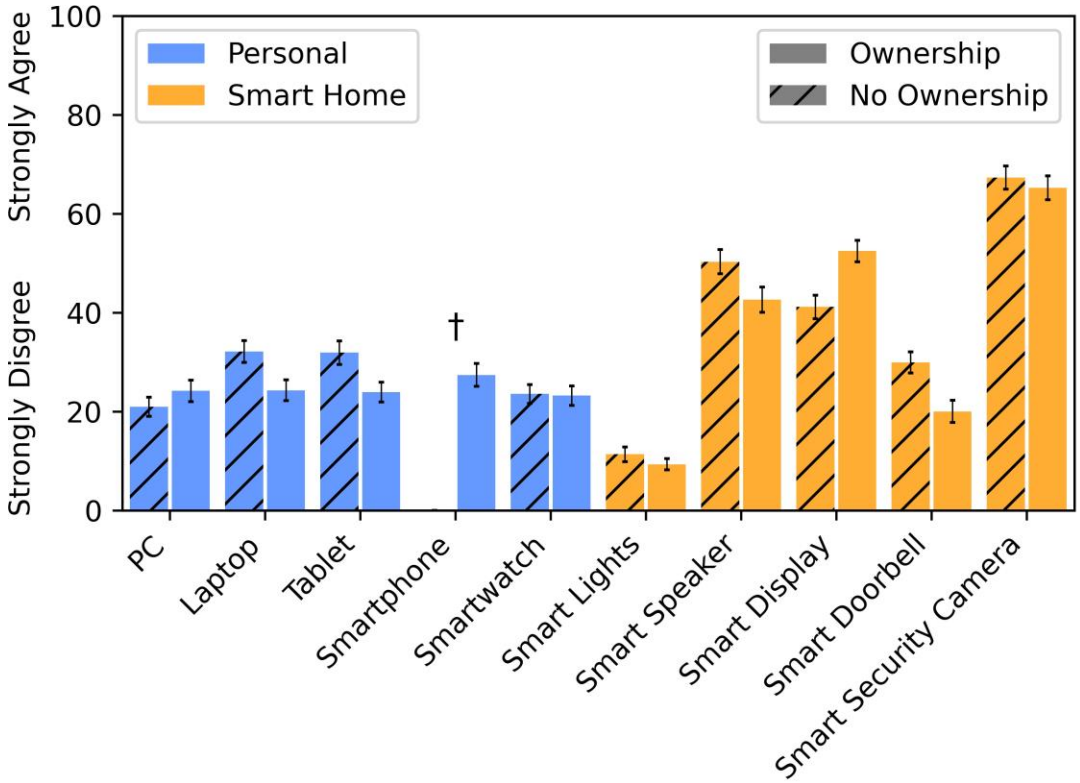
H3: A stronger social relationship to a device owner reduces privacy concerns



H4: Bystanders' privacy concerns raise the more intimate the usage location is



H5: Ownership reduces privacy concerns



Takeaways

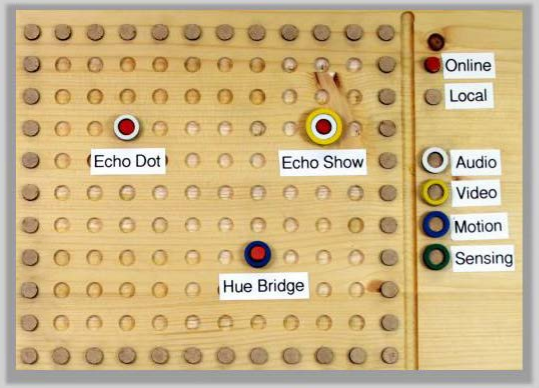
Bystanders should be notified about the presence of devices, especially those with microphones and cameras.

Bystanders should be notified about the presence of devices in all social contexts.

Bystanders should be notified about devices before entering intimate spaces, for example, already in the entrance hall.

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Media Informatics Group



Investigating Tangible Privacy-Preserving Mechanisms for Future Smart Homes

Maximiliane Windl, Albrecht Schmidt, Sebastian S. Feger

Method

Study I:
Focus Group

Study II:
Conference Workshop

Study III:
In-the-Wild

Study I: Focus Group

- Eight participants with different backgrounds and professions
- Speculative artifacts
- Co-design sessions

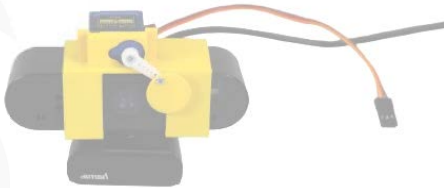
Study I: Results

Clear device status

Cumbersome

Automation

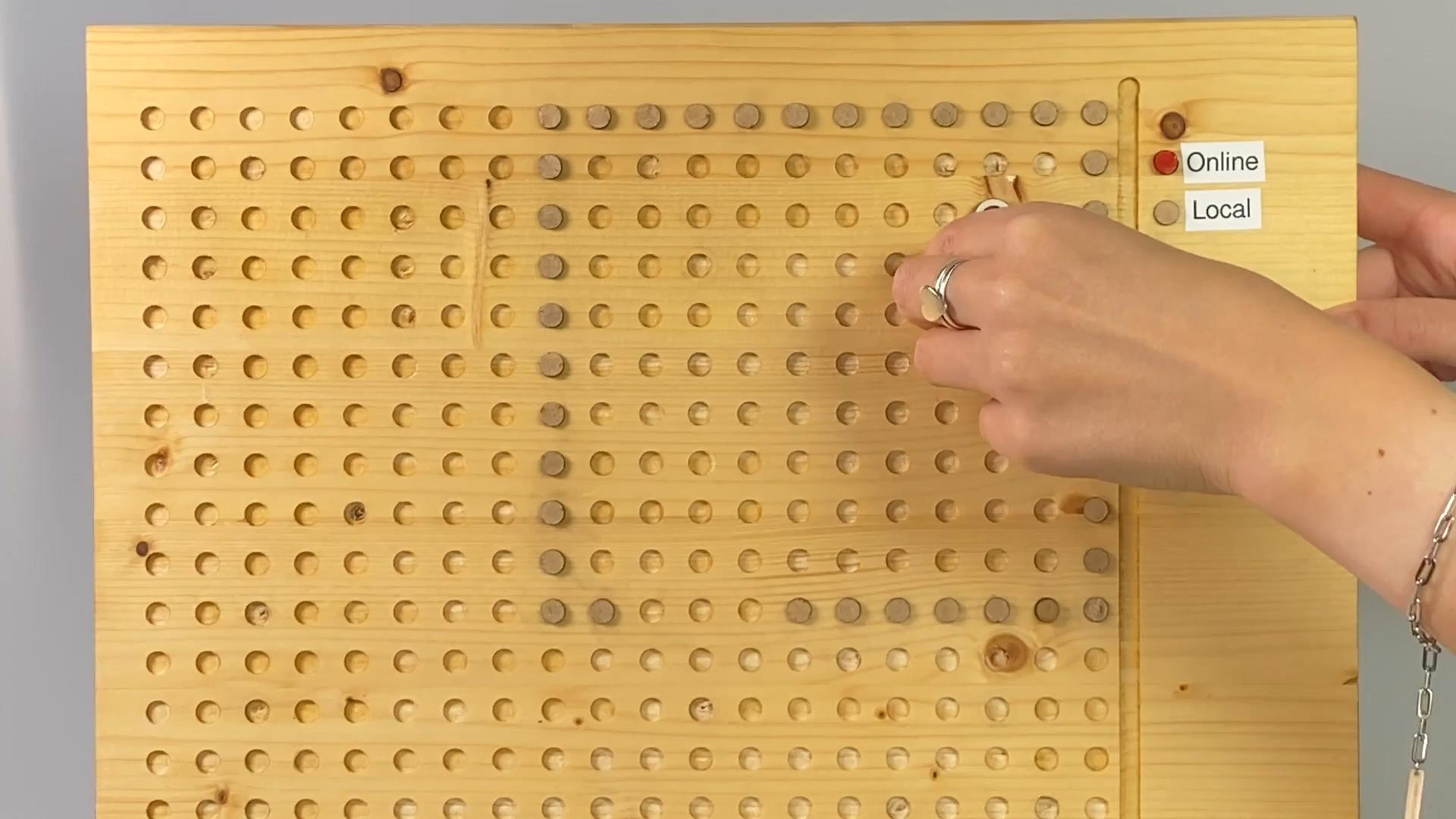
Security risk



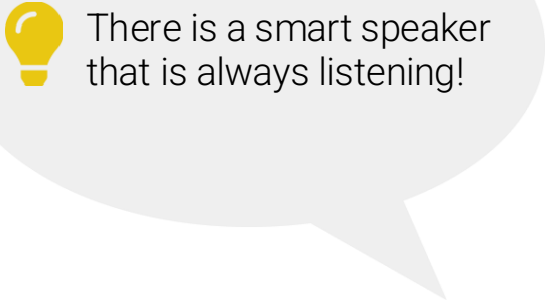
- Control hub with floor plan
- Focus: Awareness
- Differing opinions regarding control

Study III: In-the-Wild

- Six households and 12 participants
- Six weeks study duration
- Static tangible dashboards
- Goal: Investigating visitors' reactions and gaining insights into privacy negotiations
- Method: Interviews and diary study


Online
Local

Study III: Results

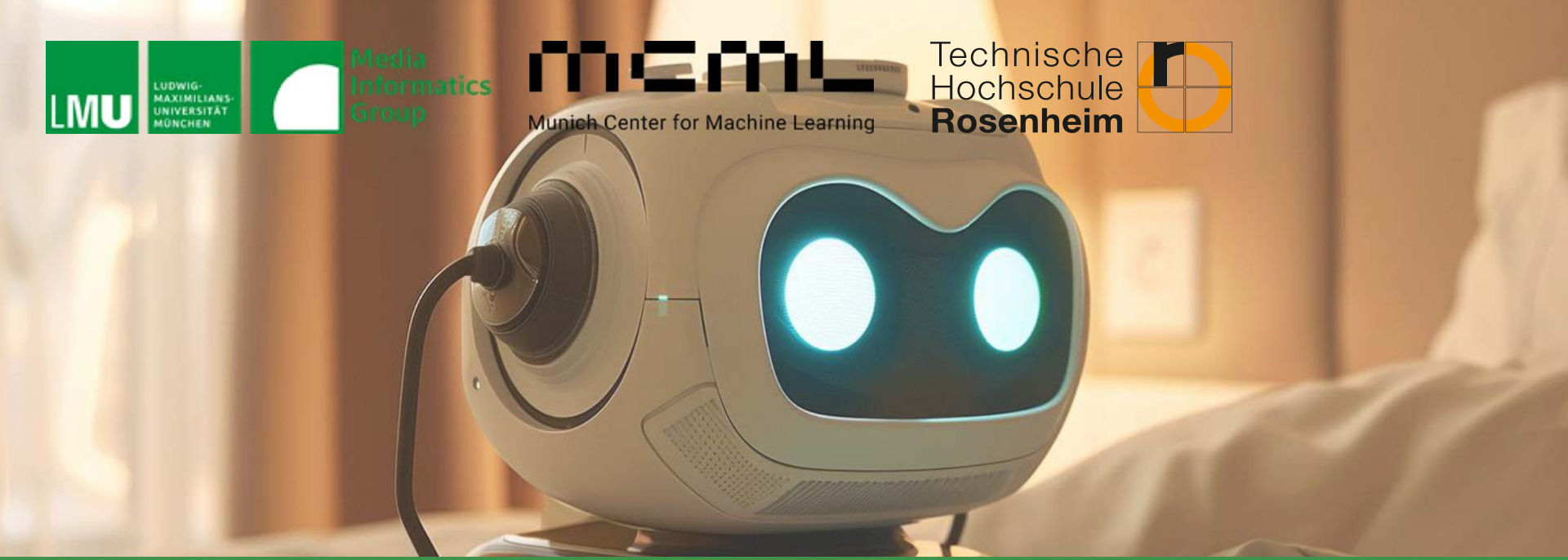


Takeaways

There is a need for tangible smart home control mechanisms, not only on the sensor level but across the entire tangible privacy spectrum.

Future systems have to be designed for both awareness and control rather than focusing on a single dimension.

Tangibility can act as a driver for inclusive privacy.



Privacy Communication Patterns for Domestic Robots

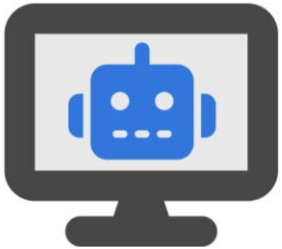
Maximiliane Windl, Jan Leusmann, Albrecht Schmidt, Sebastian S. Feger, Sven Mayer

Research Questions

RQ1	How do privacy concerns change with increasing levels of **locomotion** and **interaction** capabilities?
RQ2	Which **patterns** should domestic robots employ to communicate their privacy-relevant functionalities to users?
RQ3	Which communication patterns perform best regarding **trust**, **privacy**, **understandability**, **notification qualities**, and **general user preference**?

Method

Study I (RQ1): Online Survey on Privacy Concern (N=90)



Study II (RQ2): Focus Groups on Communication Patterns (N=22)

Study III (RQ3): Communication Patterns Evaluation (N=1720)

Study I: Method

- Online survey on Prolific (N=90)
- 3 Interaction levels: Passive, limited, full
- 4 locomotion levels: Stationary, linear, planar, world
- Every participant rated all 12 combinations

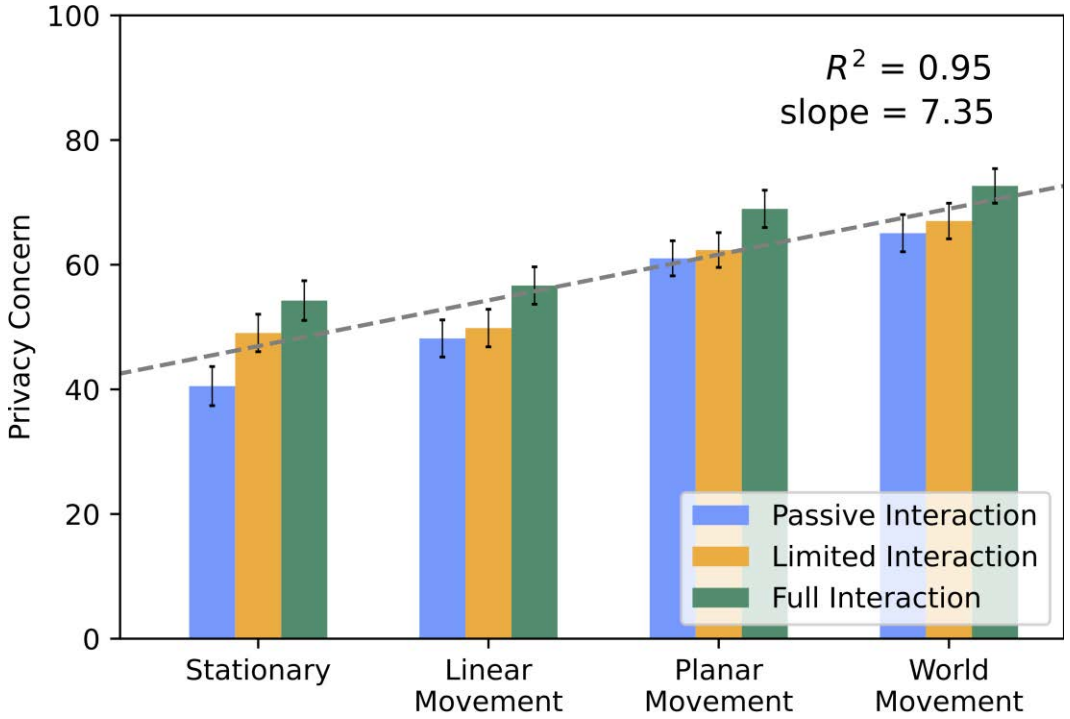
ht tps: / /www.not ebooksbilliger.de/ ama zon+echo +show+ 5+2+ generat ion+20 21+71 8987

ht tps: / /www.eur ekafor bes.com/ vacuum- cleaner s/fo rbes-ro bo-l-vac

ht tps: / /gad gets.fu tureca ndy.com/ gadget s/a mazon-ast ro

ht tps: / /ro botsgu id e.com/ robo ts/ atlas201 6

Study I: Quantitative Results



"I am strongly concerned about my privacy due to the presence of the smart assistant."
Asked on 100-point visual analogue scale

Study I: Qualitative Results

"[I have] full control on what it sees." (P66)

Concerns Rooted in Interaction

"It can probably open doors and enter areas in times where I don't want it to." (P43)

"It's hard to avoid it popping up unexpectedly, isn't it?" (P56)

Concerns Rooted in Locomotion

"Due to its limitation to one floor I might feel a bit safer with my privacy, I can move downstairs or upstairs." (P43)

Additional User Concerns

Microphone

"It might be recording conversations." (P27)

Camera

"I don't like to be watched." (P57)

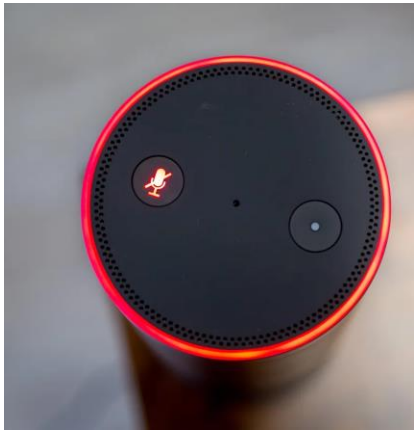
Internet Connectivity

"I always question if the assistant passes what it perceives to a third party or a remote server." (P46)

Study II

Study II: Method

- 3 focus groups (N=22)
- Task: Developing communication patterns for **internet connectivity**, **camera**, and **microphone**


Study II: Results

… faces the wall to signal that the camera is off.

Awareness Mechanisms

… plays distinct audio feedback to signal that it is disconnected from the internet.

86 Communication Patterns

… removes the microphone's cable to physically prevent the microphone from recording.

… enters physical confinement to physically prevent all functionality.

Study II: Results

... faces the wall to signal that the camera is off.

Awareness Mechanisms

... plays distinct audio feedback to signal that it is disconnected from the internet.

86 Communication Patterns

... removes the microphone's cable to physically prevent the microphone from recording.

Interventions

... enters physical confinement to physically prevent all functionality.

Study II: Results

"We thought about a lock from the outside so the robot [...] itself can't reopen it." (P15)

"If you tell it: Just go away! That doesn't work if it's still doing a task." (P20)

Trust

"I think that self-destruct is useful. When your robot has so many capabilities, you also need very strong limitations." (P11)

Usability

"It is fun. Like it's something that is trying to mimic me, but it's not me." (P7)

"If it looks like a human we start having human like expectations." (P13)

Humanoid vs. Non-Humanoid

"If a robot is covering its eyes I would be like: What's wrong with you? Just turn off your camera, dude!" (P5)

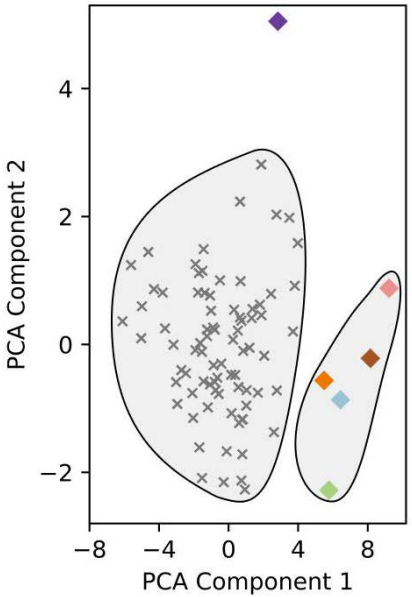
Study III

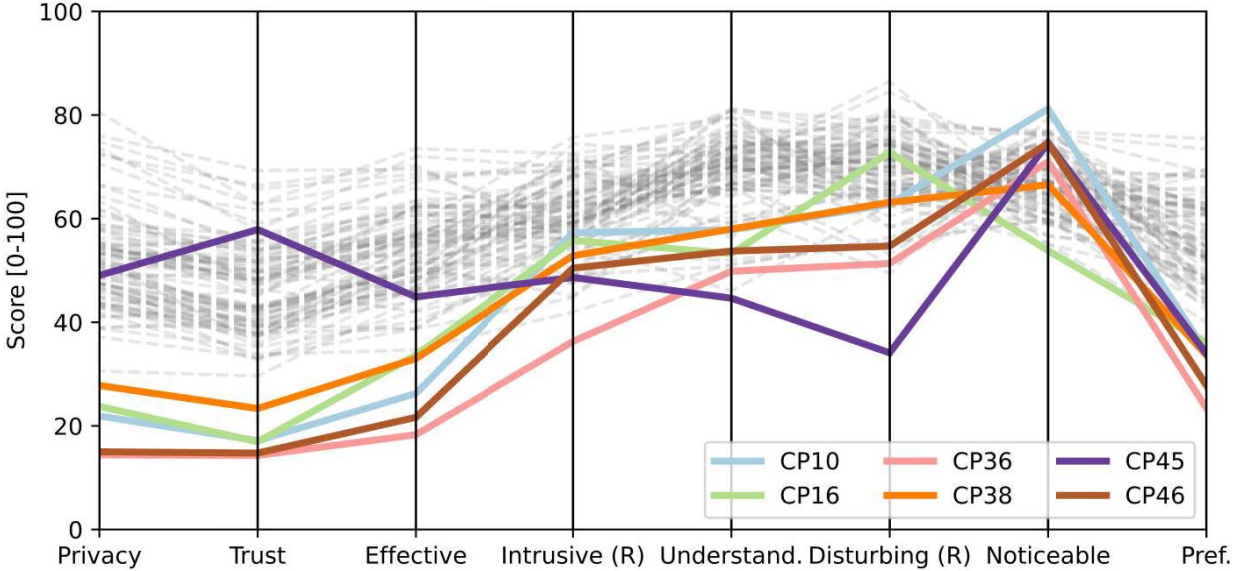
Study III: Method

- Online survey on Prolific (N=1720)
- 20 ratings per communication patterns
- We asked for perceived
    - Privacy protection
    - Trust
    - Effectiveness
    - Intrusiveness
    - Noticeability
    - Understandability
    - Disturbance
    - Preference

Study III: Results

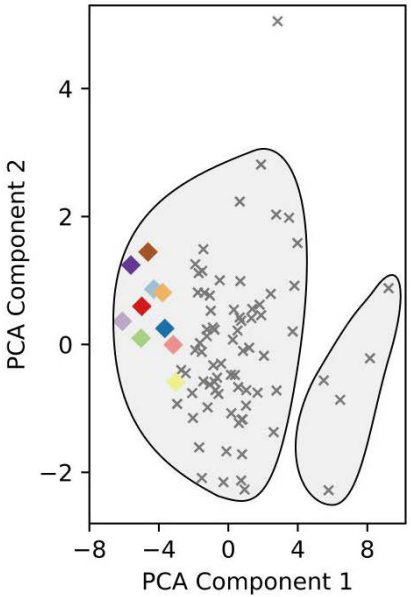
CP10: The robot covers its ears with its hands to prevent audio recording
CP36: The robot faces the wall to prevent audio recordings
CP46: The robot parks against a pillow to prevent the microphone from recording
CP45: The domestic robot kills itself to physically prevent all functionality

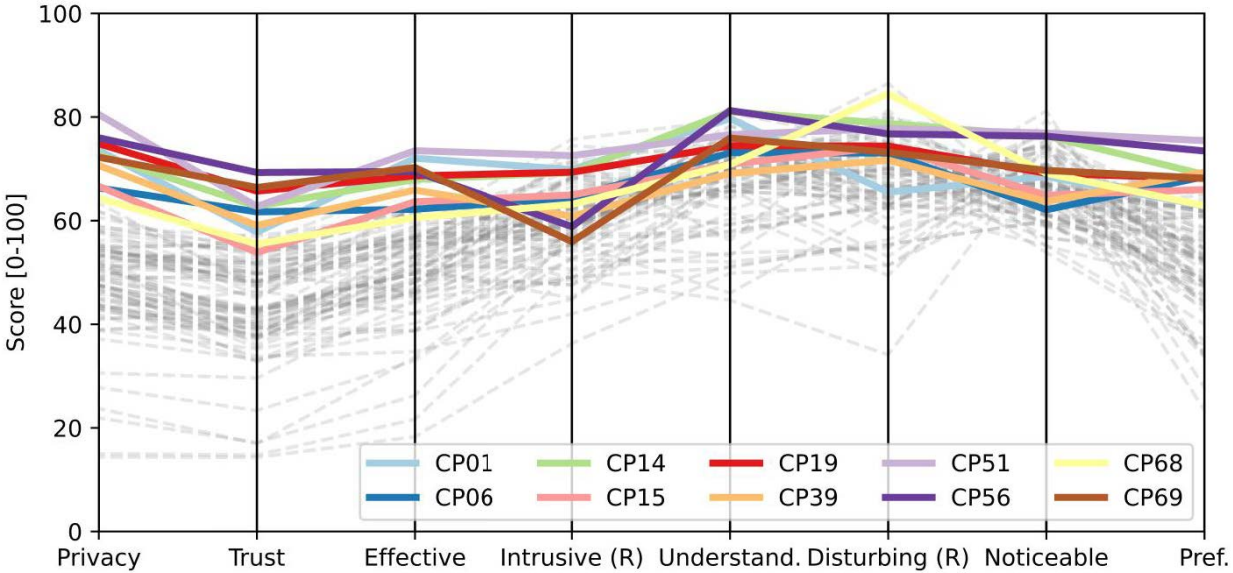




Study III: Results

CP1: The robot detaches its memory card to prevent all functionality
CP51: The robot puts a physical cover over its camera to prevent camera recordings
CP39: The robot goes to its docking station to prevent all functionality at once
CP19: The robot detaches the microphone to prevent audio recordings





Takeaways

Familiarity fosters understandability, trust, and general user preference.

Be careful when employing anthropomorphism to convey privacy states.

The right communication pattern depends on the requirements of a situation.

Overall Takeaways

As our environment becomes increasingly intelligent, it brings greater convenience but also introduces new privacy risks.

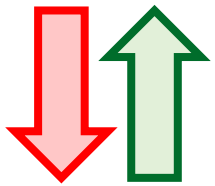
Users express privacy concerns and wish to be informed and exert privacy control.

Developers and researchers should prioritize privacy considerations when designing innovative, intelligent interfaces and devices.


PRIVACY
SUCH AN EXCITING TOPIC
imgflip.com

The Service – Privacy Fit

Users evaluate the ratio of…

Privacy Implications  **Obtained Benefits**

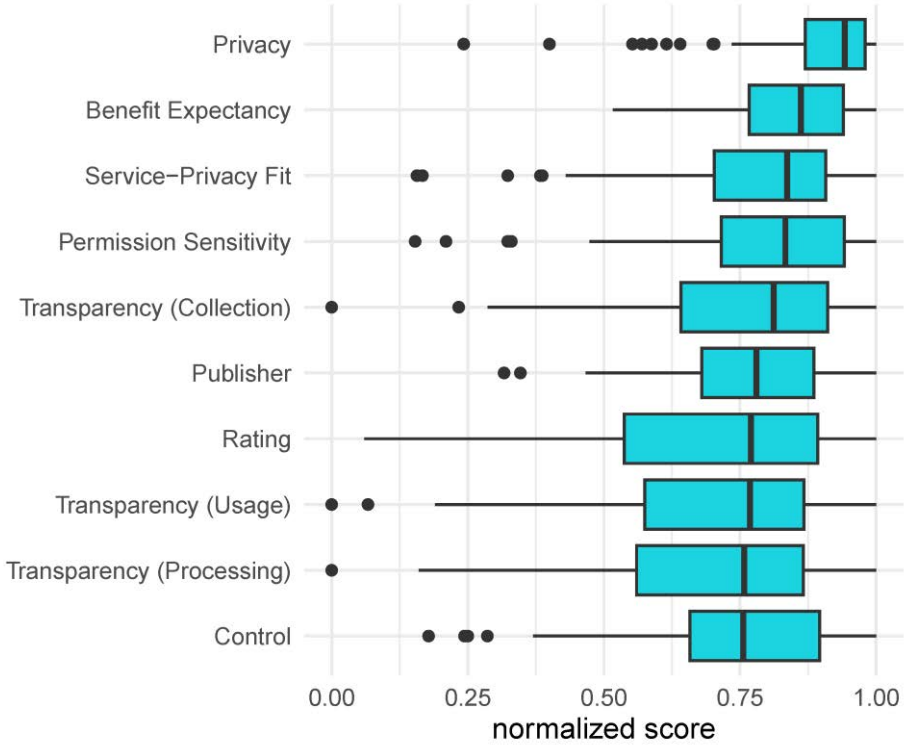
… to make a decision for or against an app

Results

Part 2: General Factors of App Adoption

Perceived Privacy significantly more relevant than all others, except *Benefit Expectancy*
$X2$ (9, N = 100) = 128.21, p < .0001).

The Ratio of Privacy and Benefits Mainly Decides App Adoption Behavior



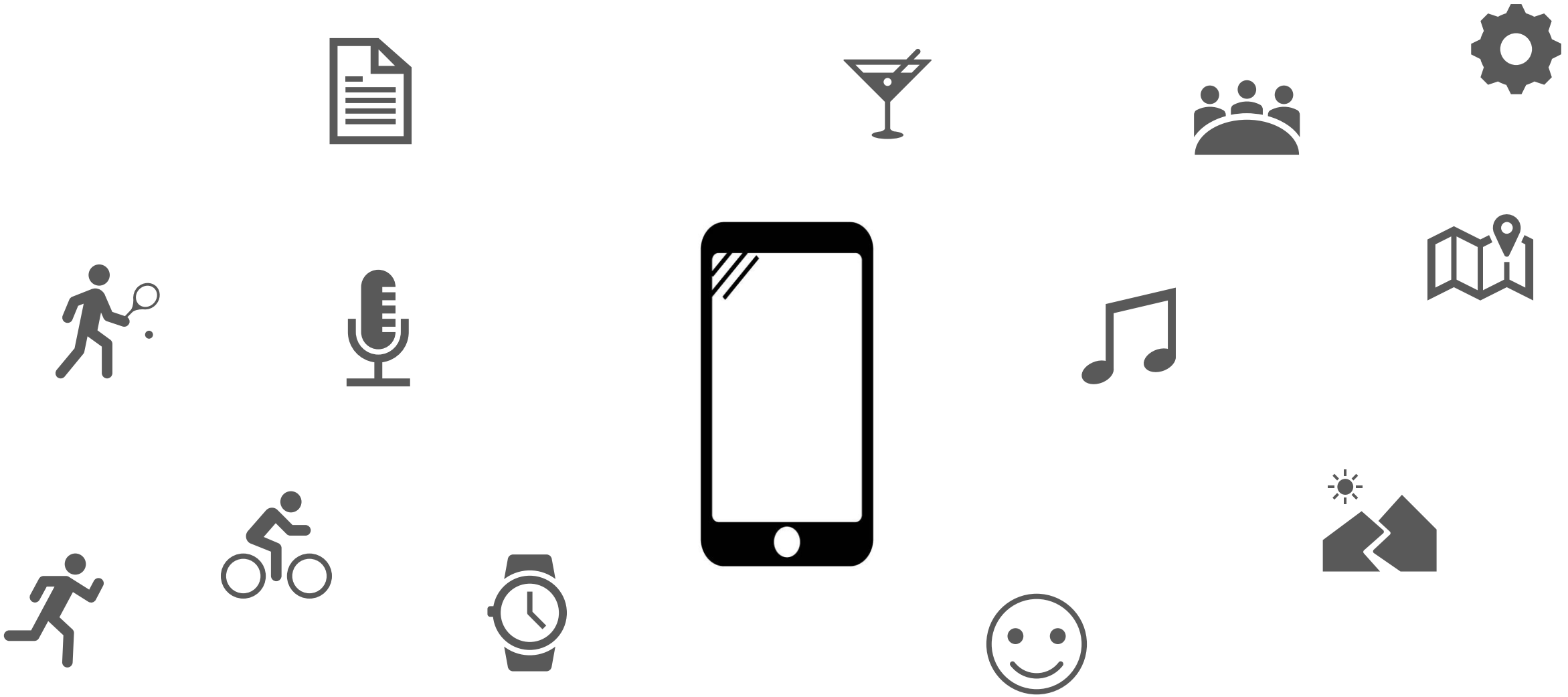
Bemmann & Mayer 2024[104]

People tend to neglect your system if they perceive privacy concerns.

Smartphones Are Different

They are **omnipresent** and **always-connected**.

Crossler et al. 2020[104]



Voices on Smartphone Data Usage

"On the whole, I find it generally bad that data are collected." (P12)

"There is the discomfort of not knowing how it will be used […]." (P19)

Voices on Smartphone Data Usage

“Doing as little as possible. That's the main protection.” (P2)

Users

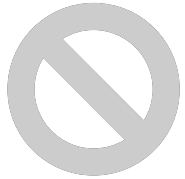
perceive concerns and fears

Feel out of control

Use systems less

App Publishers and OS Developers

Face app security issues



Impose access restrictions to data

Users

perceive concerns and fears

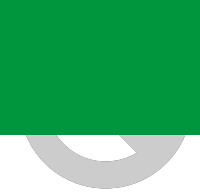
Feel out of control

Use systems less

Gained Benefits From Mobile Sensing Systems are Obstructed by Privacy Barriers

App Publishers and OS Developers

security issues



restrictions to data

Context Awareness:
Understanding the User

Users' In-Depth Privacy Concerns with Smartphone Data

Methodologies

- 📚 Literature Based
- ❓ Survey
- 💬 Interviews
- 🆎 Qualitative Analysis

Contribution

- 👫 Understanding People

What Concerns Arise From Mobile User Quantification?

Concerns, fears, and envisioned mitigation measures that users have regarding sensing-based smartphone apps

What is people's level of **knowledge regarding privacy and security** practices of the data collected through their smartphones?

What are people's **detailed privacy concerns and feared real-world consequences** of smartphone privacy issues?

What are **solutions to mitigate** privacy concerns from the users' perspective?

- What is people's level of **knowledge regarding privacy and security** practices of the data collected through their smartphones?
- What are people's **detailed privacy concerns and feared real-world consequences** of smartphone privacy issues?
- What are **solutions to mitigate** privacy concerns from the users' perspective?

Study I

Online Survey (N=100)

Study II

Semi-structured Interviews (N=20)

Qualitative Online Survey + Interviews

Study Design and Sample

Understanding Users‘ Concerns:

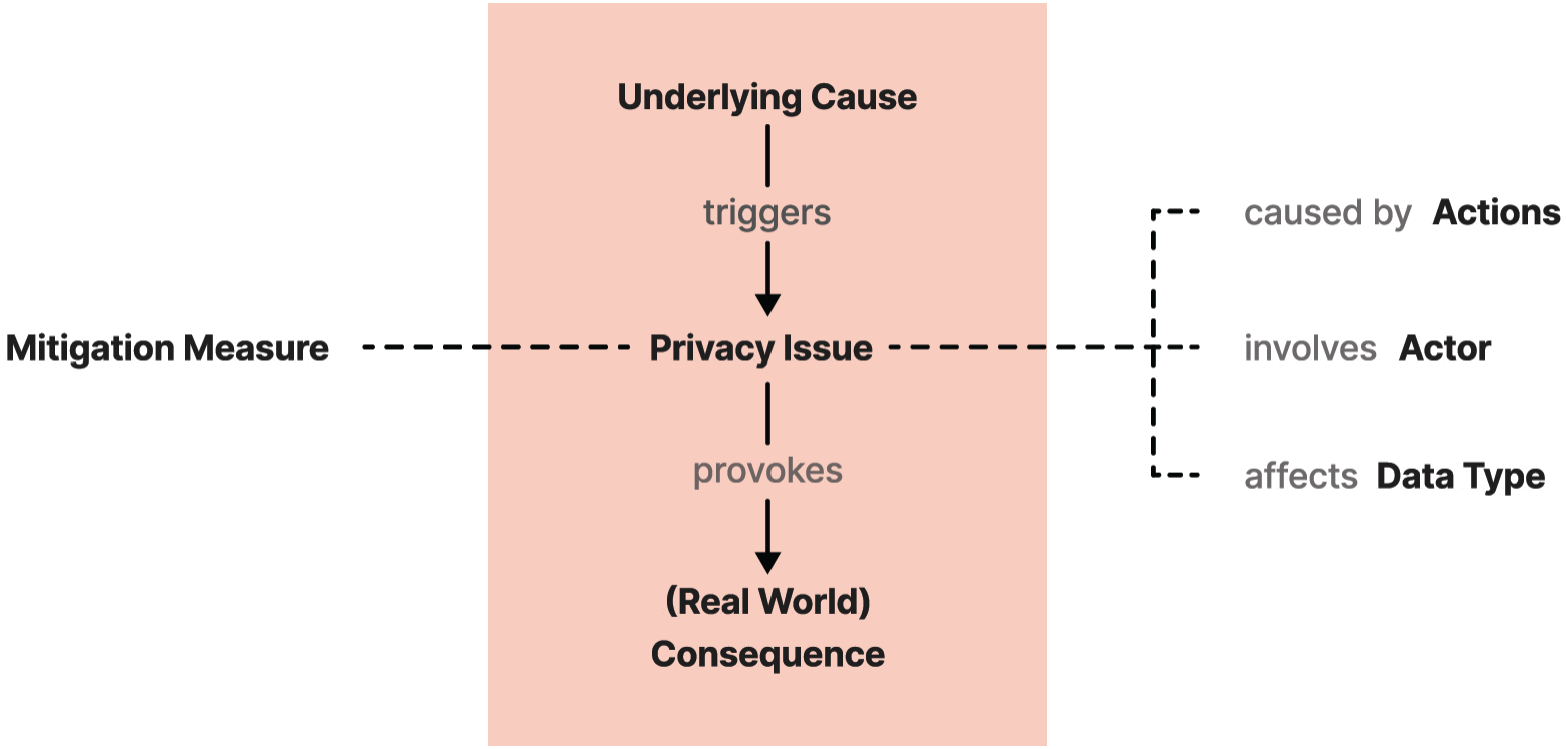
- Open questions
- Asking for details on one specific concern:
  - Outcome
  - Situation
  - Datatypes
  - Actors
  - Mitigation measures

374
codes

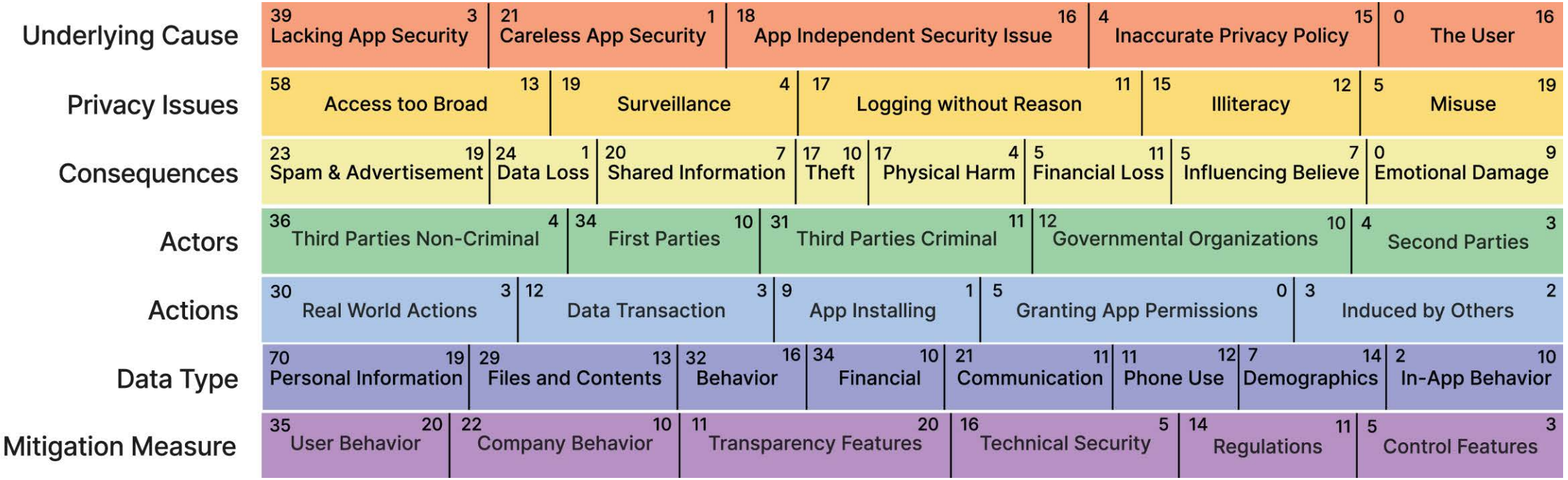
53
code groups

7
themes

A Privacy Concern Model



RQ What are people's detailed privacy concerns and feared real-world consequences of smartphone privacy issues?



# of mentions in online survey (N=100)

17 Theft 10

# of mentions in interviews (N=20)

The qualitative code

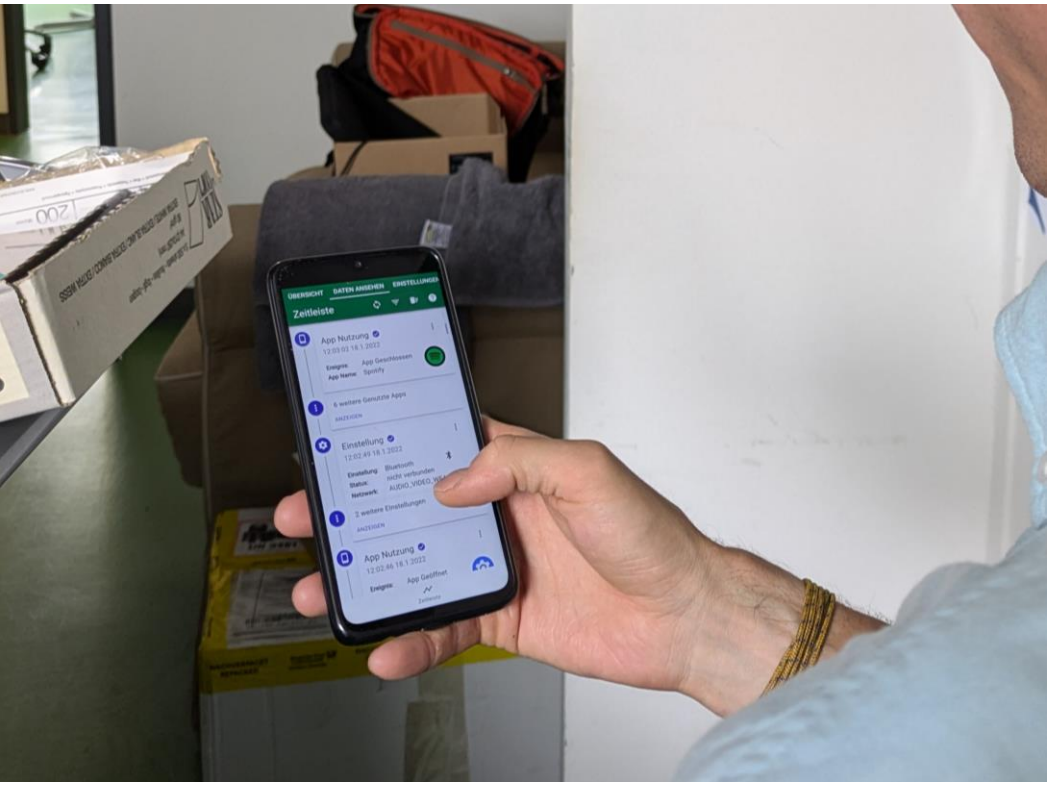
Privacy Enhancing Technologies Are Not User-Centered

TAKE AWAYS

Qualitative Survey and Interviews

- more people having access to their data than intended
- impacts on their real-world lives
- Users lack an understanding of what happens with their data
- Users do not feel in control of data collection and processing
- The perceived service-privacy fit mainly influences users privacy decision
- Technical security measures hardly mitigate concerns

Users lack **transparency** and **control** over their data.



The Influence of Transparency and Control on the Willingness of Data Sharing in Adaptive Mobile Apps

EICS 2020

Methodologies

📊 Field Study

⏱️ Quantitative Analysis

Contribution

👫 Understanding People

📱 Interface Concept

The Effects of Transparency and Control

Research Questions

How do **transparency** and **control** in a privacy dashboard …

RQ1 …affect the **number of users adopting and dropping out** of a passive mobile sensing app?

RQ2 …affect the **awareness** of and **knowledge** about the data logging?

RQ3 …induce **behavior change and self-reflection** and thus the logged data of a passive mobile sensing app?

RQ4 …affect a passive mobile sensing system user's **privacy concerns and trust**?

Field Study Design

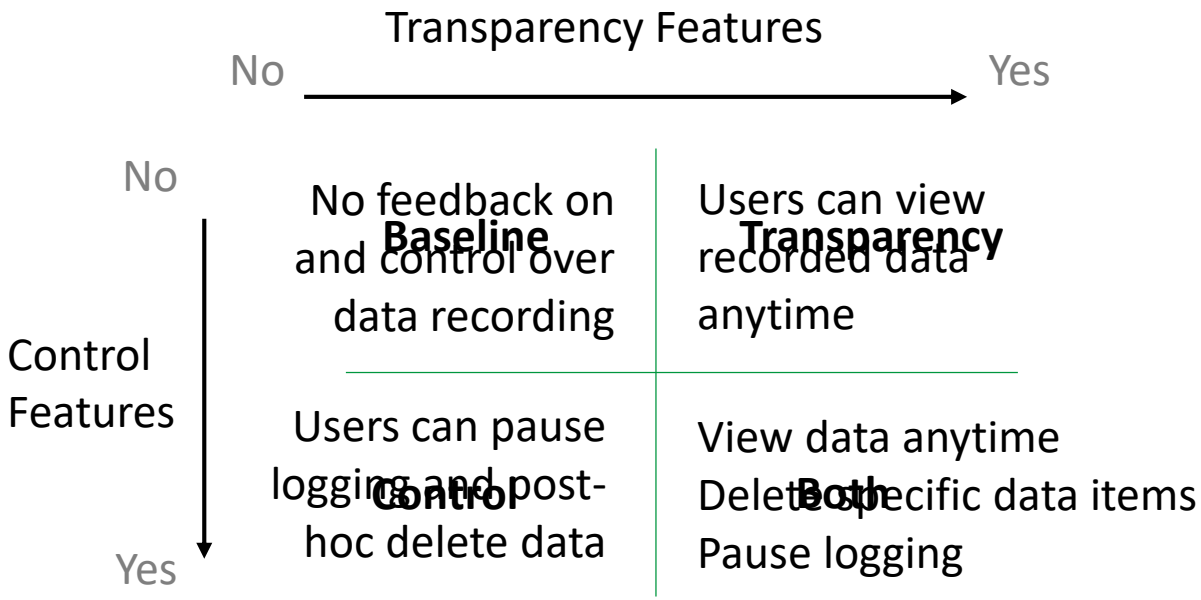
The Effects of Transparency and Control

- Assess people‘s willingness to install a mobile sensing app
- Different variants, with and without (a) transparency and (b) control features

- App scenario: Mobile sensing field study
- Transparency and control features incorporated through a privacy dashboard Raschke et al. 2018[337]

Field Study Design

The Effects of Transparency and Control



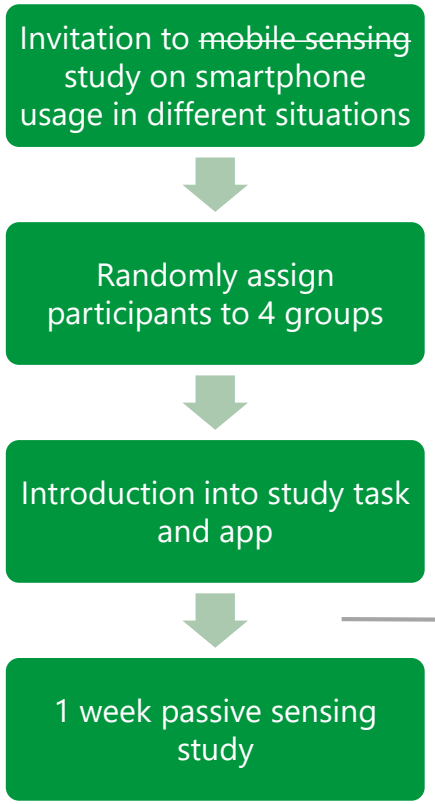
2x2 Factorial Design

Between Subject

N=227

Field Study Design

Tracking of participation rates + usage statistics through all stages

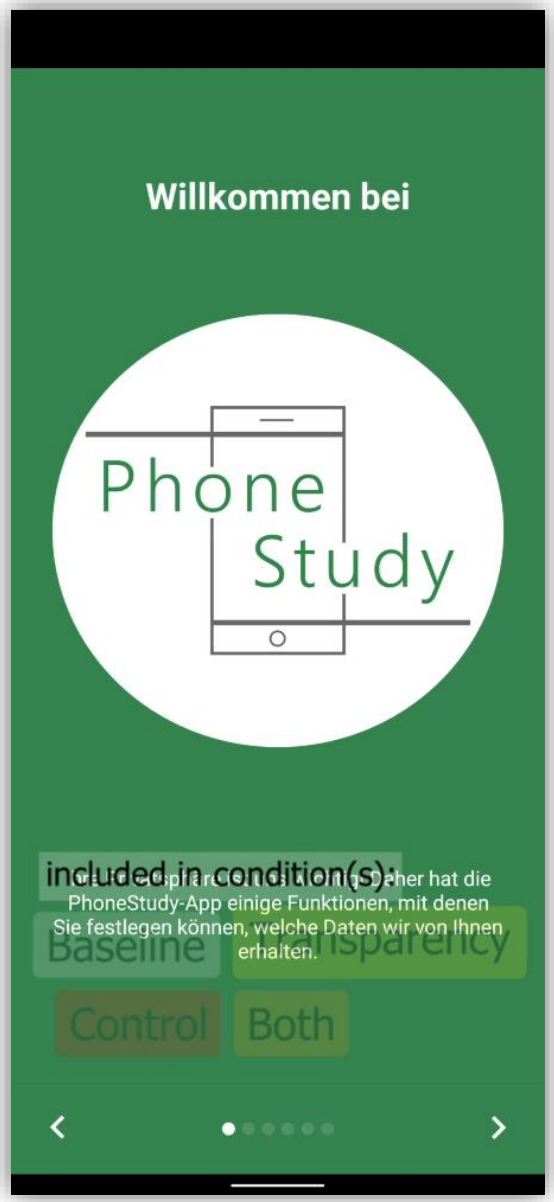


Pre Questionnaire

- Privacy Perception
- Understanding and Awareness

Post Questionnaire

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

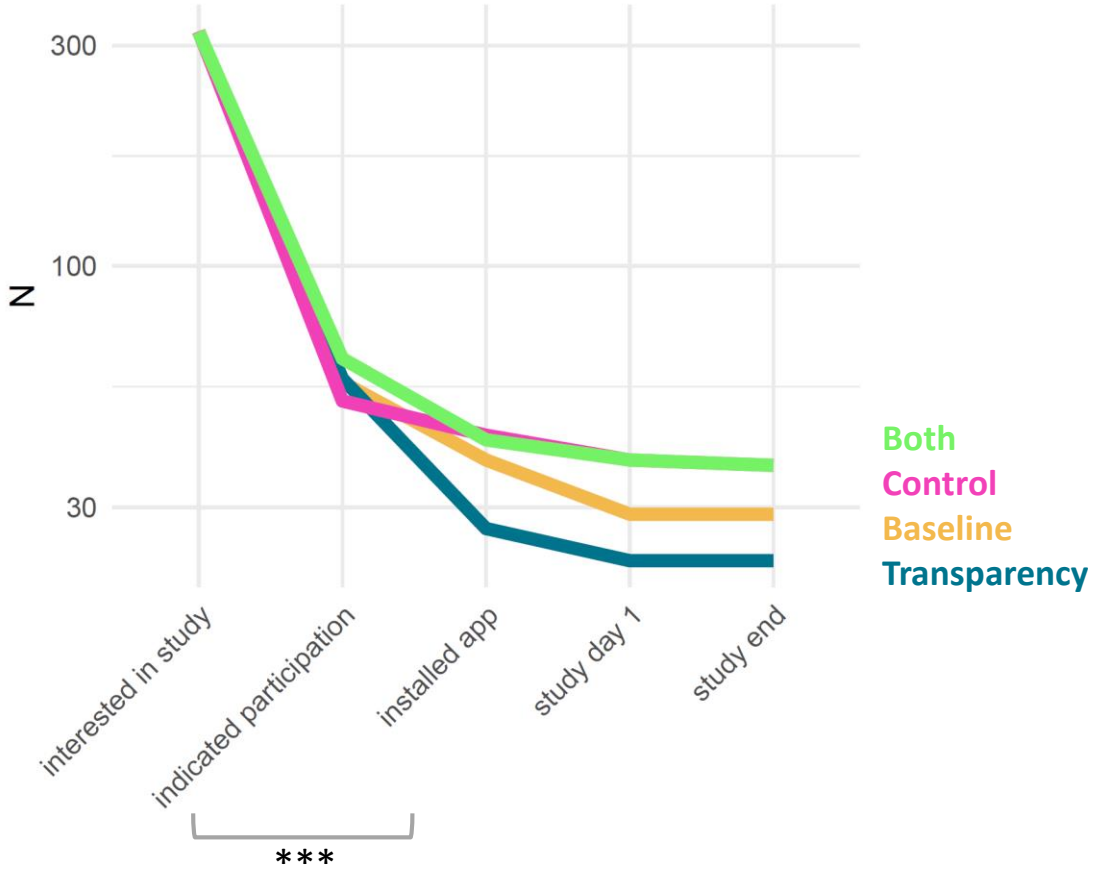


included in condition(s):

- Transparency
  - Timeline feed of recorded raw data
  - Detail view per data item
  - Filtering features
- Control
  - Pause logging temporarily
  - Delete single data items
  - Delete groups of data

RQ1

Conversion and Dropout Rate



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

RQ2

Awareness and Knowledge of Data Logging

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 *

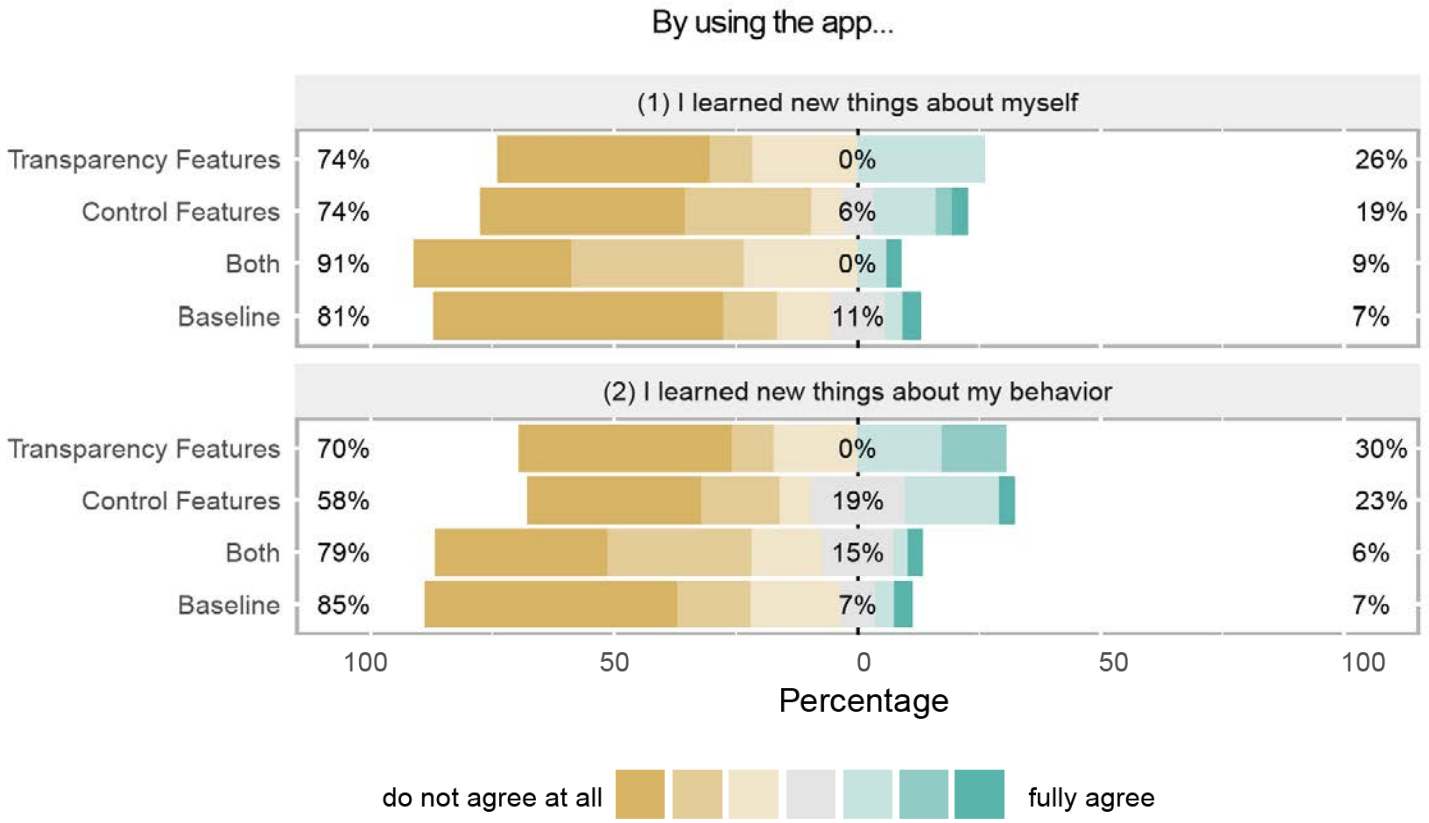
Awareness – What data is logged?

- Slightly higher knowledge about what is logged for *Transparency* users
- Slight improvements during the study period

Shapiro-Wilk test rejected normality; non-parametric Aligned Rank Transformation (ART) ANOVA tests applied to test for difference

RQ3

Behavior Change and Self-Reflection

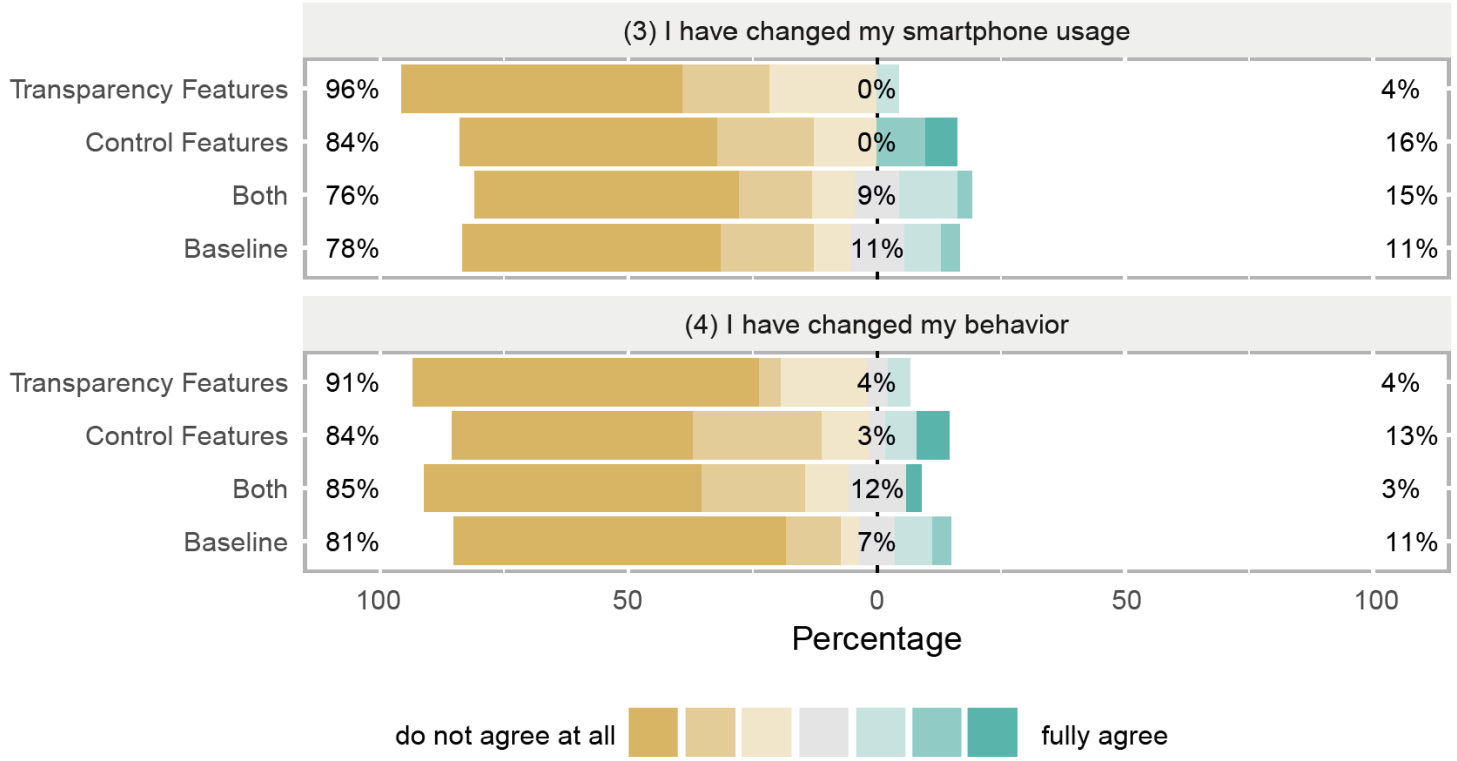


The data shows moderate evidence that there is no effect of Transparency or Control on self-reflection.

$BF_{0+} = 0.89$ (item 1)
$BF_{0+} = 1.96$ (item 2)
Bayes Factor analysis, classification according to Jeffreys [33]

RQ3

Behavior Change and Self-Reflection



The data shows strong evidence that there is no effect of Transparency or Control on behavior change.

BF_{0+} = 0.85 (both items)
Bayes Factor analysis, classification according to Jeffreys [33]

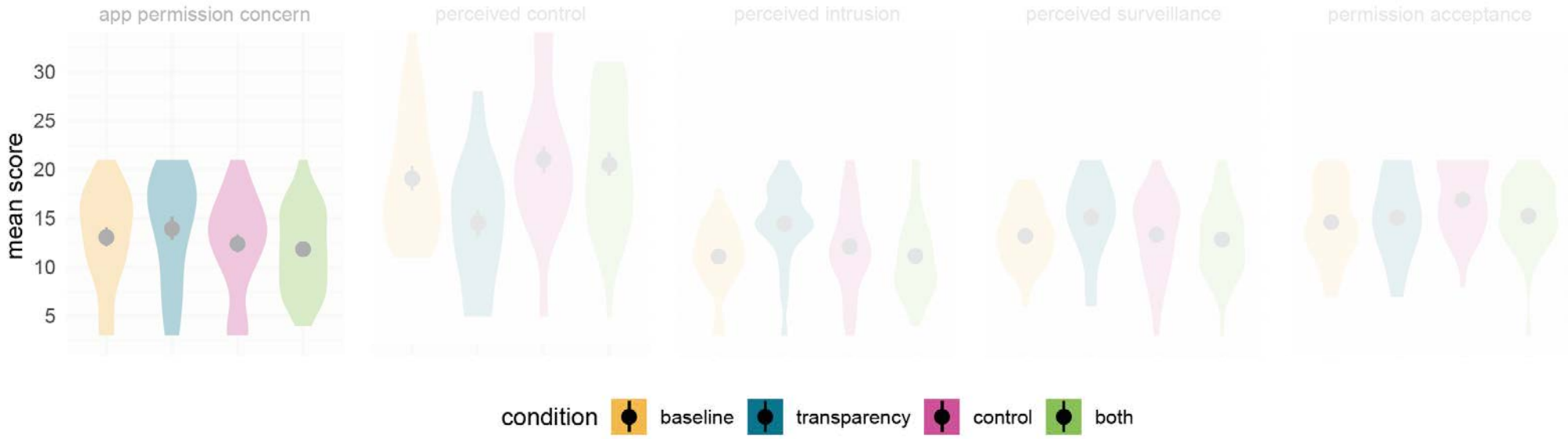
RQ4

Privacy Concerns and Trust

Perceived control is highest for Control***, and lowest for transparency

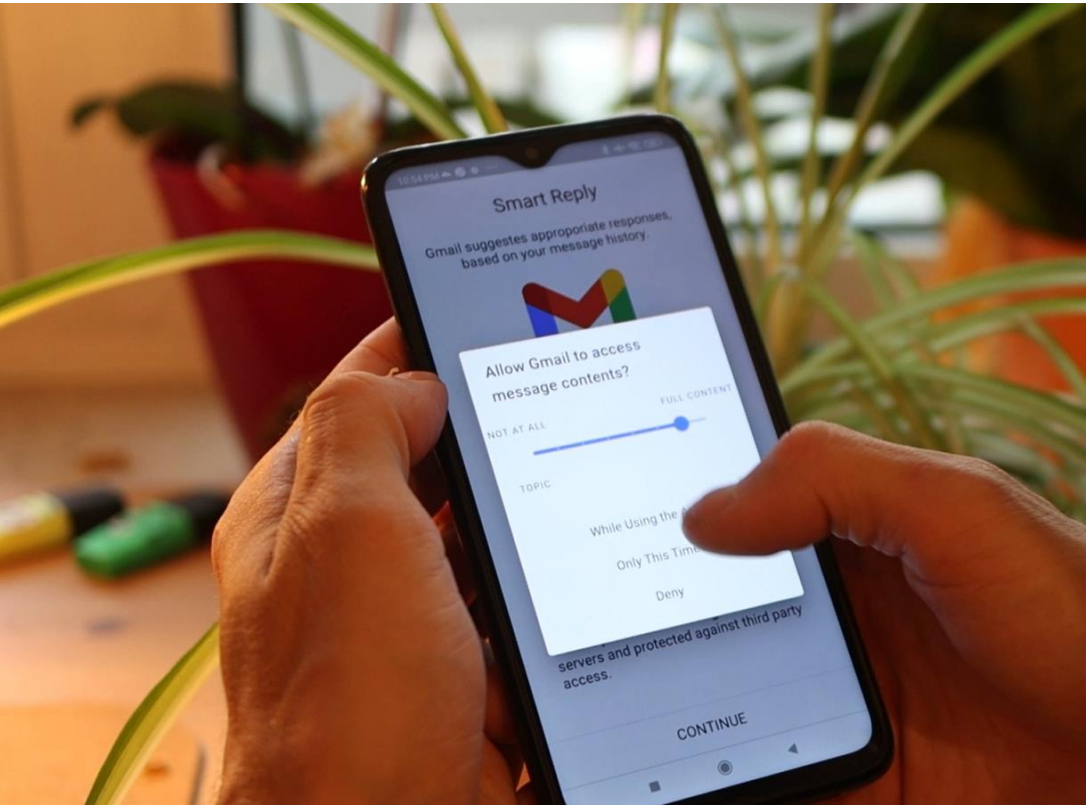
Transparency tends to show higher concern, intrusion and surveillance scores

Control tends to improve permission acceptance even lower than baseline



The Effects of Transparency and Control

- Transparency should always be accompanied by control
- The feeling of being in control is important for users
- Users in fact make use of their control rarely
- Always offer control, make it available on-demand, advertise it, but do not force users to exert it



Privacy Slider: Fine-Grain Privacy Control for Smartphones

MobileHCI 24

Methodologies

❓ Survey
💬 Interviews
👨‍👧‍👦 Focus Group
🧪 Lab Experiment

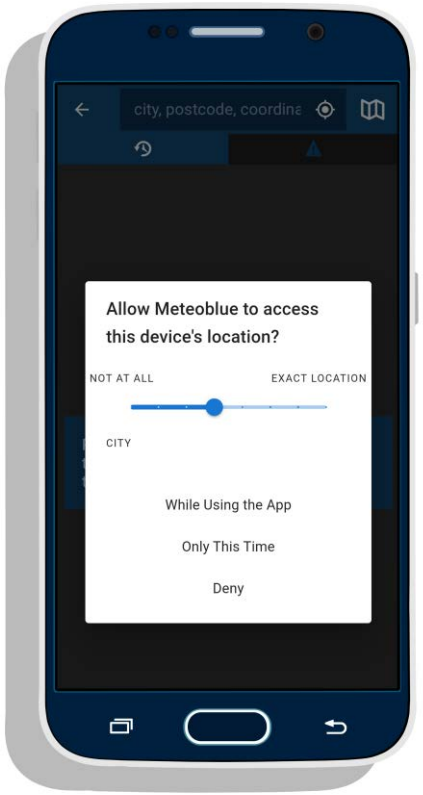
Contribution

📱 Interface Concept

Limitations of Current Permission Systems

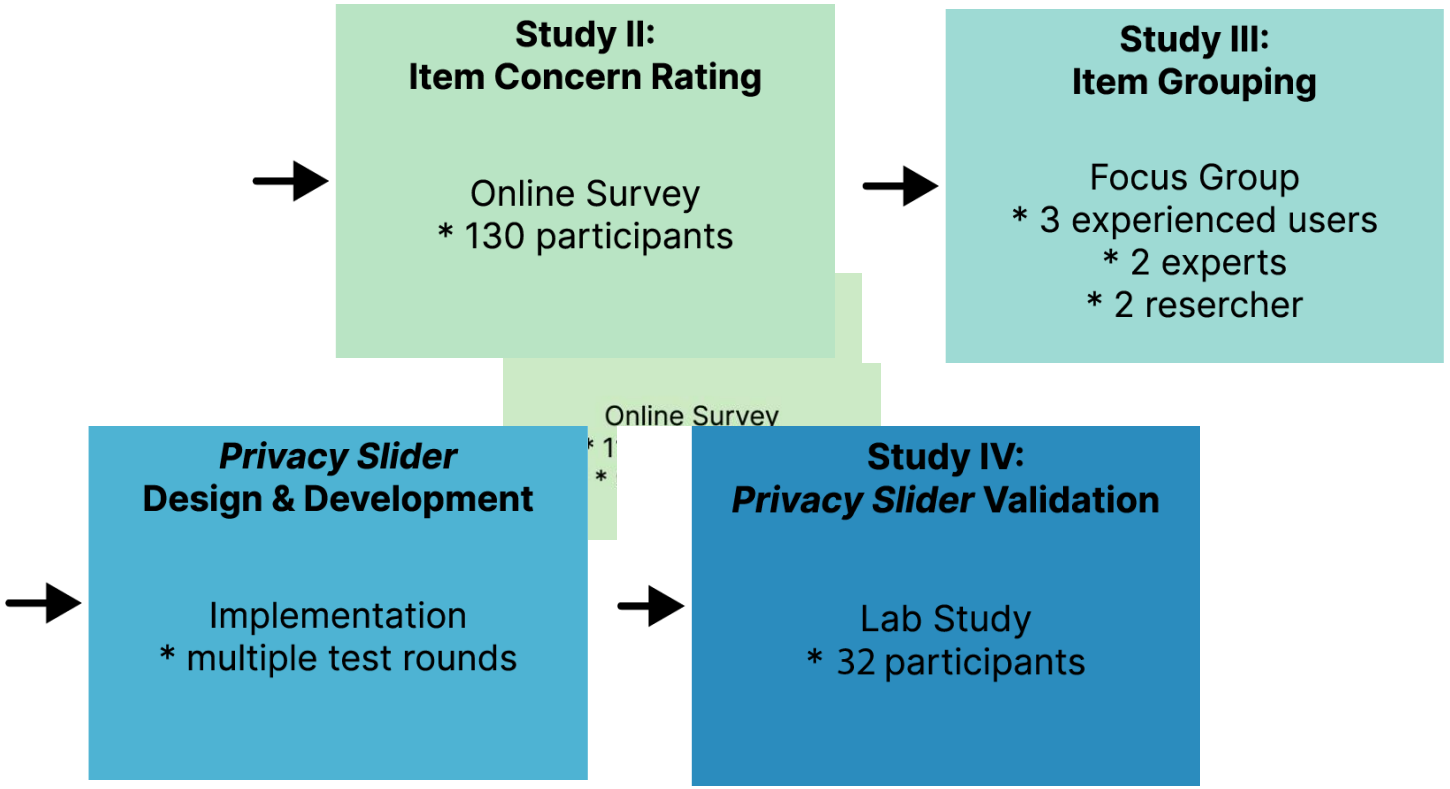
- Users are constrained by binary permission systems
- Users rarely understand the scope of permissions they agree to
- The scope of current permissions is mostly too large, violating the principle of *data minimalization*

Privacy Slider



- a continuous smartphone permission interface
- Allows for choosing a degree of detail

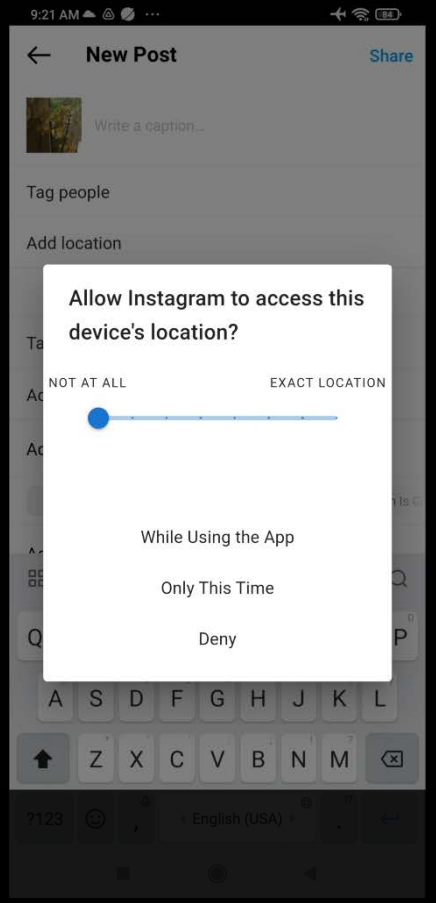
Design and Evaluation Process

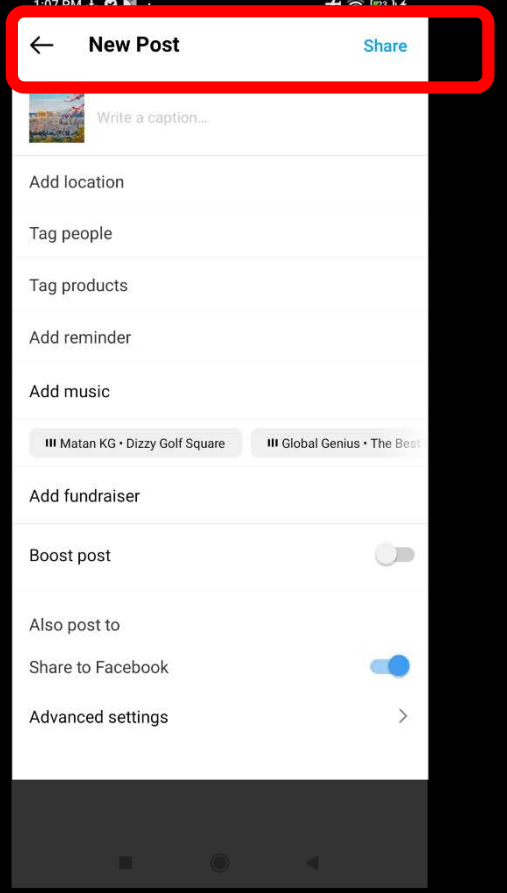


Privacy Slider: Study Implementation

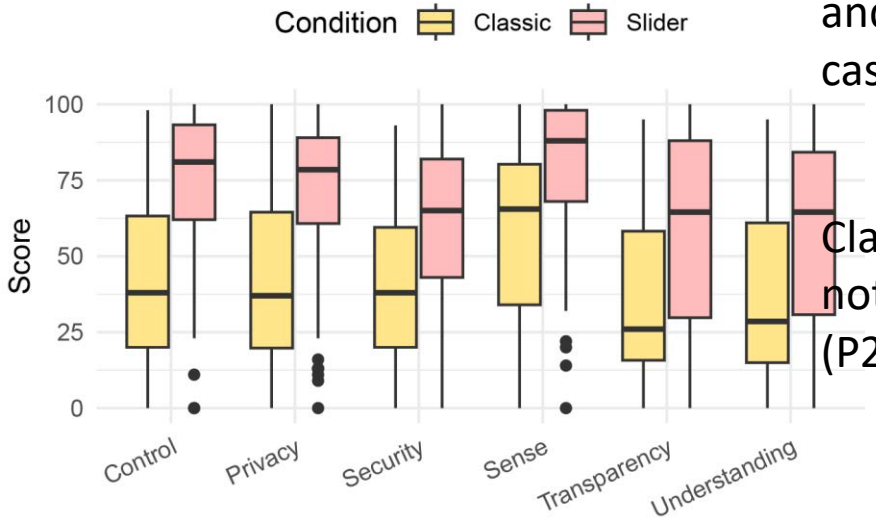
- Lab study with mockups
- 4 app usage scenarios
- 2 conditions: buttons-only vs. slider
- Within subjects

- Progressive Web App


9:21 AM
New Post
Share
Write a caption...
Tag people
Add location
Allow Instagram to access this device's location?
NOT AT ALL
EXACT LOCATION
While Using the App
Only This Time
Deny


New Post
Share
Write a caption...
Add location
Tag people
Tag products
Add reminder
Add music
Matan KG • Dizzy Golf Square
Global Genius • The Best
Add fundraiser
Boost post
Also post to
Share to Facebook
Advanced settings

Runtime Permission Slider



p<.001 in all pairwise comparisons

Slider:
a big improvement over the usual UI and would definitely prefer this in all cases – P39

Classic:
not enough options for data privacy" (P26) and being "too general".

Slider for me is only useful for continuous values like distance. – P51

Qualitative Findings

- Control interfaces should adhere more to the „natural structure“ of the data – e.g. slider for continuous data
- The interface gives both, more control and transparency on what is in there
- Critical: Warning fatigue / privacy resignation

User-Centered Privacy-Enhancing Interfaces

- On-device preprocessing minimizes data, can be transparent, and leaves user in control of their data
- Understanding data practices and the presence of control make the difference for users
- Transparency can have averse effects on users privacy perception
- Main challenge: Privacy interfaces act on the edge of user annoyance and warning fatigue

Summary

- Privacy as Barrier to App Adoption
- Technical privacy and security measures
- Abstract concepts for user-centered privacy were proposed
- Specific concerns with smartphone sensing and factors towards app adoption
- User-Centered Privacy Enhancing Technologies
- Operationalization of User-Centered Privacy

Future Work

Dealing with lacking user motivation

Ecologically valid field studies on privacy behaviors

Control beyond the own device

Future

florian.bemmann@ifi.lmu.de

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

This image is AI generated