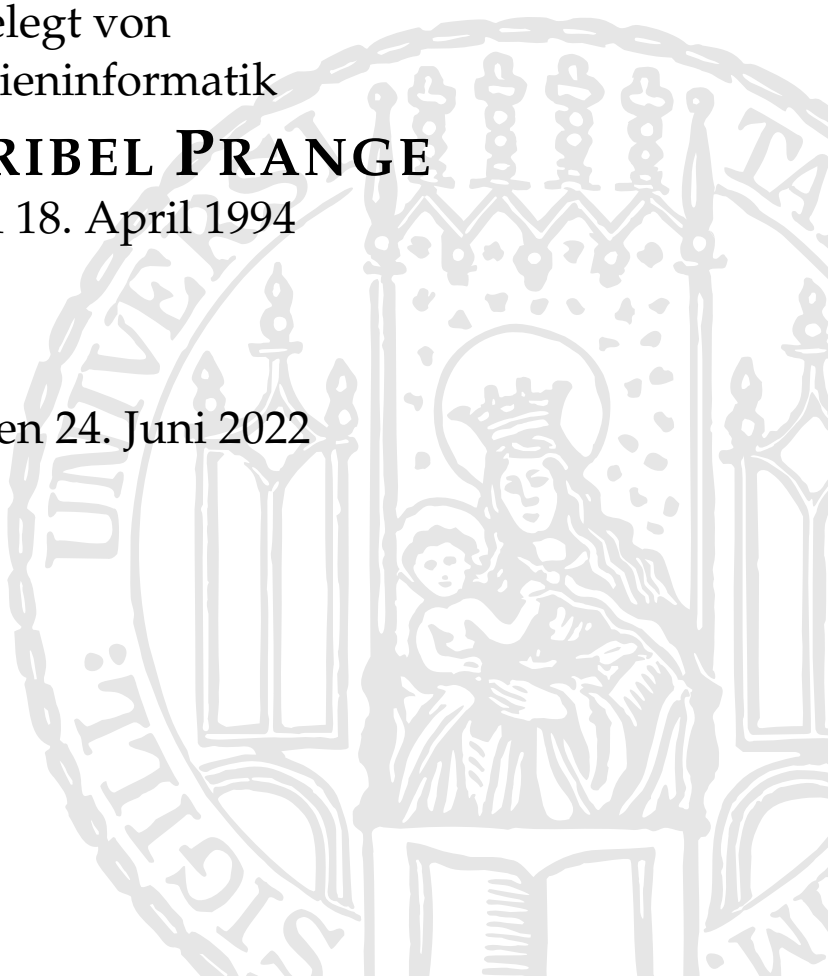
Usable Privacy and Security in Smart Homes

Dissertation

an der Fakultät für Mathematik, Informatik und Statistik
der Ludwig-Maximilians-Universität München

vorgelegt von
M.Sc. Medieninformatik
Sarah Maribel Prange
geboren am 18. April 1994

München, den 24. Juni 2022



Erstgutachter: Prof. Dr. Florian Alt
Zweitgutachter: Prof. Dr. Martina Angela Sasse

Tag der Abgabe: 24. Juni 2022

Tag der mündlichen Prüfung: 2. Dezember 2022

ABSTRACT

Ubiquitous computing devices increasingly dominate our everyday lives, including our most private places: our homes. Homes that are equipped with interconnected, context-aware computing devices, are considered *"smart" homes*. To provide their functionality and features, these devices are typically equipped with sensors and, thus, are capable of collecting, storing, and processing sensitive user data, such as presence in the home. At the same time, these devices are prone to novel threats, making our homes vulnerable by opening them for attackers from outside, but also from within the home. For instance, remote attackers who digitally gain access to presence data can plan for physical burglary. Attackers who are physically present with access to devices could access associated (sensitive) user data and exploit it for further cyberattacks. As such, users' privacy and security are at risk in their homes. Even worse, many users are unaware of this and/or have limited means to take action. This raises the need to think about usable mechanisms that can support users in protecting their smart home setups. The design of such mechanisms, however, is challenging due to the variety and heterogeneity of devices available on the consumer market and the complex interplay of user roles within this context.

This thesis contributes to usable privacy and security research in the context of smart homes by a) understanding users' privacy perceptions and requirements for usable mechanisms and b) investigating concepts and prototypes for privacy and security mechanisms. Hereby, the focus is on two specific target groups, that are *inhabitants* and *guests* of smart homes. In particular, this thesis targets their *awareness* of potential privacy and security risks, enables them to take *control* over their personal privacy and security, and illustrates considerations for usable *authentication* mechanisms. This thesis provides valuable insights to help researchers and practitioners in designing and evaluating privacy and security mechanisms for future smart devices and homes, particularly targeting awareness, control, and authentication, as well as various roles.

ZUSAMMENFASSUNG

Computer und andere „intelligente“, vernetzte Geräte sind allgegenwärtig und machen auch vor unserem privatesten Zufluchtsort keinen Halt: unserem Zuhause. Ein „intelligentes Heim“ verspricht viele Vorteile und nützliche Funktionen. Um diese zu erfüllen, sind die Geräte mit diversen Sensoren ausgestattet – sie können also in unserem Zuhause sensitive Daten sammeln, speichern und verarbeiten (bspw. Anwesenheit). Gleichzeitig sind die Geräte anfällig für (neuartige) Cyberangriffe, gefährden somit unser Zuhause und öffnen es für potenzielle – interne sowie externe – Angreifer. Beispielsweise könnten Angreifer, die digital Zugriff auf sensitive Daten wie Präsenz erhalten, einen physischen Überfall in Abwesenheit der Hausbewohner planen. Angreifer, die physischen Zugriff auf ein Gerät erhalten, könnten auf assoziierte Daten und Accounts zugreifen und diese für weitere Cyberangriffe ausnutzen. Damit werden die Privatsphäre und Sicherheit der Nutzenden in deren eigenem Zuhause gefährdet. Erschwerend kommt hinzu, dass viele Nutzenden sich dessen nicht bewusst sind und/oder nur limitierte Möglichkeiten haben, effiziente Gegenmaßnahmen zu ergreifen. Dies macht es unabdingbar, über benutzbare Mechanismen nachzudenken, die Nutzende beim Schutz ihres intelligenten Zuhauses unterstützen. Die Umsetzung solcher Mechanismen ist allerdings eine große Herausforderung. Das liegt unter anderem an der großen Vielfalt erhältlicher Geräte von verschiedensten Herstellern, was das Finden einer einheitlichen Lösung erschwert. Darüber hinaus interagieren im Heimkontext meist mehrere Nutzende in verschieden Rollen (bspw. Bewohner und Gäste), was die Gestaltung von Mechanismen zusätzlich erschwert.

Diese Doktorarbeit trägt dazu bei, benutzbare Privatsphäre- und Sicherheitsmechanismen im Kontext des „intelligenten Zuhauses“ zu entwickeln. Insbesondere werden a) die Wahrnehmung von Privatsphäre sowie Anforderungen an potenzielle Mechanismen untersucht, sowie b) Konzepte und Prototypen für Privatsphäre- und Sicherheitsmechanismen vorgestellt. Der Fokus liegt hierbei auf zwei Zielgruppen, den *Bewohnern* sowie den *Gästen* eines intelligenten Zuhauses. Insbesondere werden in dieser Arbeit deren *Bewusstsein* für potenzielle Privatsphäre- und Sicherheits-Risiken adressiert, ihnen *Kontrolle* über ihre persönliche Privatsphäre und Sicherheit ermöglicht, sowie Möglichkeiten für benutzbare *Authentifizierungsmechanismen* für beide Zielgruppen aufgezeigt. Die Ergebnisse dieser Doktorarbeit legen den Grundstein für zukünftige Entwicklung und Evaluierung von benutzbaren Privatsphäre- und Sicherheitsmechanismen im intelligenten Zuhause.

ACKNOWLEDGMENTS

Completing this thesis has been a tough and challenging, joint journey. This section is an attempt to express my gratitude for all the shared experiences with and support by amazing people - including those that I do not manage to mention explicitly:

Thank you, **Florian Alt**, for sparking my research interests early on with a great project in Museum Mensch und Natur [166], and taking me all the way with you until I joined your present research group at CODE. Thanks for your endless ideas and continuous support. Thank you also for our unforgettable road trips through the US, the summer BBQs, and for Venetian Sprizz and espresso.

My admiration and gratitude go to **Angela Sasse** for introducing the human factor in security research. I am tremendously proud and thankful that you reviewed my thesis. Many thanks also to **Albrecht Schmidt** for inviting me to countless inspirational and fun events, and to **Christian Böhm** for complementing my committee.

For most of the time during this thesis, I had the pleasure to work in Florian's growing research group on Usable Privacy and Security. Thank you, **Lukas**, for being a team from day one, for always sharing an office, leg space, pizza, and perspectives from above and below. Thanks for the shared journey across institutions, and the sword. Thank you, **Yasmeen**, for laughing and crying together (late) in the office (sometimes both at the same time), and for the painting and Krapfen sessions. Thank you, **Sarah (D. R.)**, for sharing Spanish traditions, and for building all the amazing things, including the Androids and *PriKeys*. Thank you, **Michael (F.)**, for the statistics, the wine, and the birthday cake you brought for me when we did barely know each other. Thank you, **Heike**, for all the paperwork and so much beyond, including apple cakes and the best Erdbeermarmelade. Thank you, **Yomna** for your inspiration on *PriView* and the German Tupperparty with Egyptian food. Thank you, **Mariam**, for taking me to my first conference in Stuttgart and for all inspiration ever since. Thank you, **Florian (M.)**, for the Sprizz and career talk in Frascati. Thanks also to **Michael (B.)**, **Ken**, **Rivu**, **Pascal**, **Felix**, **Verena**, and **Oliver**, for all the inspiration and discussions in the lab, kitchen, and on car and train rides. Thanks all for the amazing doctoral hat! 🎓

Thank you also to all current and former members of the Media Informatics group(s) at LMU. Thanks for your open doors and for taking me on your group trips to Bernried, Vienna, and Venice. Thank you, **Thomas (W.)**, for drawing monsters together; **Carl**, for hosting great parties and dinners; **Sarah (V.)**, for organizing our Canada trip and other events; **Malin** for sharing a room in Venice; **Sarah (A.)**, for our "Die drei ???" nights in Cairo; **Ceenu**, for completing smart home stories together; **Jingyi**, for sharing a room in Vienna; **Fiona**, for sharing the round-shaped bed in Pisa; **Sylvia**, for organizing the IDC (that got canceled) together; **Changkun** for the sushi delivery; **Sven**, for always helping with PCS and TAPS; **Linda**, for Italian summer nights at INTERACT; **Christina** for the insights on career choice;

Matthias, for sharing Irish pub food in Ulm; **Rike** for dancing to ABBA.
Thank you, **Franziska (S.)**, for taking care of all my certificates, **Christa** and **Anja** for all paperwork, and **Rainer** for running my hybrid defense.

Thank you, **Heinrich Hußmann**, for introducing the media informatics program, for making the Venice trips happen, and for exploring my vision of usable smart home authentication [168] in Stockholm together.

Other mentors I would like to thank are: Thank you, **Emanuel**, for pointing me to smart homes as a research context. Thank you, **Daniel (B.)**, for introducing me to after-CHI-traveling and Jupyter notebooks, and for all other valuable input on research and writing. Thank you, **Mohamed**, for your advice on literature and the drinks we had in Glasgow. Thank you, **Karola**, for collaborating across timezones, drawing mental models together, and taking the night train to my defense. Thank you, **Alex**, for understanding Android privacy permissions together, and **Fabian** for looking through users' eyes together.

I will also never forget the amazing time I had during my research internship at Lancaster University (UK): Thank you, **Nigel Davies** and **Team D23** (Ludwig, Peter, Mike, Mateusz, Victoria, and Asma) for your warm welcome and all the activities during my stay, including great music and food.

Thanks to all the students who contributed to the research forming this thesis, especially to **Ahmed**, **Robin**, and **Christian** for your contributions to *PriView*. Thanks also to Andreas, Stephan, Niklas, Cristina, Markus, Vanessa, Bastian, Timo, Daniel, Elias, Jan, and all other students I enjoyed working with throughout the last years.

Moreover, this thesis would not have been possible without support from outside academia. Thank you, **Daniel (R.)**, for your advice on writing and life. Thank you, **Melina**, for the yoga sessions. Thank you, **Tabea**, for reading parts of this thesis although it is so different from yours. Thank you, **Julia (S.)**, for the sunny weekend in Koblenz shortly before submitting this thesis. Thanks to the other girls with whom I dance through life as long as I can remember: **Laura**, **Jenny**, and **Judith**. Thank you, **Franziska (B.-K.)**, for endless aperitifs and great food by the lake. Thank you, **Christian**, for celebrating all (my) magic moments. Thank you, **Julia (V.)** and all others who celebrated the night after my defense with me, it was great fun!

To my family, **Sonja**, **Sophia**, and **Stefan**, for your support throughout the years. Thank you, Stefan, for laying the earliest foundations for this and submitting your very own thesis on the day I was born. Thank you, **Karin** and **Achim**, for closely following my career, supporting every step, and attending my defense.

Finally, I cannot thank you, **Max**, enough for accompanying me through all ups and downs of this work (even when f(o)unding your own company became equally challenging), and for making sure that there is pasta after paper deadlines.

Thank you all!

Publications & Declaration of Co-Authorship

This thesis is based on research that I conducted between December 2017 and December 2021 at LMU Munich, University of Applied Sciences Munich, and the Research Institute CODE at the University of the Bundeswehr Munich. However, writing this thesis was and would not have been possible in isolation and was enabled through several collaborations. While contents of **Parts I** and **V** were exclusively written for this thesis, **Parts II**, **III** and **IV** are based on co-authored publications at international, peer-reviewed conferences. Moreover, many projects were supported through practical works by students during their bachelor or master theses, which I supervised. These collaborations are listed in detail below.

Part II – Targeting Awareness is based on the following publications:

> Karola Marky and **Sarah Prange**, Max Mühlhäuser, and Florian Alt. 2021. Roles Matter! Understanding Differences in the Privacy Mental Models of Smart Home Visitors and Residents. In *20th International Conference on Mobile and Ubiquitous Multimedia (MUM 2021), December 5–8, 2021, Leuven, Belgium.* ACM, New York, NY, USA, 15 pages. **Honorable Mention Award.** https://doi.org/10.1145/3490632.3490664

This paper was a close collaboration with Karola Marky. She came up with the initial study idea. Two bachelor students, Stephan Kniep (LMU Munich) and Andreas Schütz (TU Darmstadt), conducted the interviews under our close supervision. The analysis of qualitative data and writing of the initial paper draft was equally distributed among Karola and myself. We collaboratively refined the paper. I presented the paper at the MUM Conference 2021 (fully virtual, video presentation). This paper received an *honorable mention award* at the conference.

> **Sarah Prange**, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. 2021. *PriView* – Exploring Visualisations to Support Users' Privacy Awareness. In *CHI Conference on Human Factors in Computing Systems (CHI'21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3411764.3445067

Together with my supervisor, Florian Alt, I came up with the initial idea for *PriView*. I refined the concept in several iterations with continuous feedback by him and other team members. Ahmed Shams, exchange student from the German University in Cairo, implemented the mobile application as part of his bachelor

thesis. I set off implementing the VR application. The project was further supported by two student assistants at CODE: Robin Piening finalized the implementation, and Christian Gessner created the 3D scenes. I came up with the initial study design which was iteratively refined and shaped with the help of Florian Alt and Yomna Abdelrahman. I conducted the study with Ahmed's help. I led the analysis and writing of the paper. The qualitative analysis was supported by Yomna. I led the writing of the initial and final version of the paper and presented it at the CHI Conference 2021 (fully virtual, video presentation).

Part III – Empowering Control is based on the following publications:

> **Sarah Prange**, Niklas Thiem, Michael Fröhlich, and Florian Alt. 2022. "Secure settings are quick and easy!" – Motivating End-Users to Choose Secure Smart Home Configurations. 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/10.1145/3531073.3531089

The concept and idea for "PMT-inspired nudges" in the context of smart homes was brought up by Niklas Thiem in the context of his master thesis (LMU Munich). Together with a fellow PhD student, Michael Fröhlich, we reshaped the concept in several iterations. Niklas implemented the web application that was used for a larger user study. He came up with the initial study design, which was refined by Michael and myself. I led the recruitment and data collection phase. Niklas and Michael helped with the statistic analysis. I led the writing of the paper and presented it at AVI 2022 (in-person).

> Sarah Delgado Rodriguez, **Sarah Prange**, Christina Vergara Ossenberg, Markus Henkel, Florian Alt, and Karola Marky. 2022. *PriKey* – Investigating Tangible Privacy Control for Smart Home Inhabitants and Visitors. In *Nordic Conference on Human-Computer Interaction (NordiCHI '22)*, October 10–12, 2022, Aarhus, Denmark. https://doi.org/10.1145/3546155.3546640

The concept and idea for *PriKey* was brought up by Sarah Delgado Rodriguez in the context of her master thesis and was continuously refined together with Karola Marky and myself. Sarah came up with the initial study design, which she iterated with our help. She also conducted the interview study. The qualitative analysis of the interviews was conducted by Sarah and myself. Sarah led the writing of the paper under continuous feedback by Karola and myself. Note that the paper submission includes a second study not presented in this thesis, which was conducted by the co-authors Christina Vergara Ossenberg and Markus Henkel (students at TU

Darmstadt). I rewrote the chapter compared to the published version, particularly setting a focus specific to this thesis (privacy control for visitors).

Part IV – Usable Authentication is based on the following publications:

> **Sarah Prange**, Ceenu George, and Florian Alt. 2021. Design Considerations for Usable Authentication in Smart Homes. In *Mensch und Computer '21, September 05–08, Ingolstadt, Germany.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3473856.3473878

This paper is based on a project conducted by Vanessa Sarakiotis and Bastian Wagner during their master studies at LMU Munich, under close supervision of Ceenu George and myself. The students created the interview guide under our continuous feedback. They conducted the interviews. The focus group was initiated and led by Ceenu. The both of us conducted the thematic analysis of all results. I led the writing of the initial version of this paper, and all iterations that were made until publication. I presented the paper at the Mensch und Computer Conference 2021 (fully virtual, video presentation).

> **Sarah Prange**, Sarah Delgado Rodriguez, Timo Döding, and Florian Alt. 2022. "Where did you first meet the owner?" – Exploring Usable Authentication for Smart Home Visitors. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '22 Extended Abstracts), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3491101.3519777

This paper presents a design space that evolved based on a literature review and discussions with Timo Döding (bachelor thesis, LMU Munich) and Sarah Delgado Rodriguez (fellow PhD student at CODE). Timo implemented a conceptual Wizard-of-Oz prototype and conducted the exploratory user study, including analysis of quantitative and qualitative data, under our close supervision. I led the writing of this paper and presented the (physical) poster at the CHI conference 2022.

I would like to thank all co-authors and students for their engagement in these projects and publications. To acknowledge this, I will use the scientific plural in the remainder of this thesis.

TABLE OF CONTENTS

LIST OF FIGURES

List of Tables

1

Introduction & Background

PART I – INTRODUCTION & BACKGROUND

In this part of the thesis, we introduce the topic and structure, relevant context and terms, and related work on current privacy and security mechanisms for smart homes. This forms the basis for the mechanisms and studies presented in this thesis.

- **Chapter 1** introduces and motivates the topic of this thesis, sets out the overarching research questions, and illustrates the applied research approach. It also provides an overview of the overall thesis structure.
- **Chapter 2** lays the foundations for this thesis: smart devices and their various benefits and features, users and their various roles and permissions in the context of smart homes, and privacy and security related issues.
- **Chapter 3** illustrates related work around existing mitigation strategies that increase awareness, enable privacy and security control, and authentication mechanisms. It also highlights the limitations of prior works, motivating the remainder of this thesis.

1
Introduction

"There is nothing more important than a good, safe, secure home."
– Rosalynn Carter

Smart home devices are on the rise with an ever-increasing number of sensors and features, providing great benefits to users. At the same time, such devices entail privacy and security risks. More precisely, these devices open users' private and secure place – their homes – to attackers and threats. This thesis aims at reclaiming the home as a private and secure "castle" by investigating *usable privacy and security mechanisms for smart homes*.

This chapter introduces the topic (Section 1.1), and sets out overarching research questions (Section 1.2). Section 1.3 illustrates the research approach and methods applied in this thesis. Lastly, Section 1.4 provides an overview of the thesis structure.

1.1 Motivation: Technology Enters our Homes

Our homes are traditionally a place we consider to be safe, secure, and privacy-preserving. We have full control over whom we let into this place, and we generally trust the place and the entities we let in. "Home" oftentimes is also perceived as a more abstract concept, referring to a feeling of joy, security and satisfaction [54]. As such, trust, privacy, and security are taken for granted within the home.

However, with smart home devices being on the rise with a continuous market growth worldwide since 2016 [197] and 801 million device units globally shipped in 2020 [199], the notion of whom we let into our homes shifts towards not only people, but also devices and, more precisely, sensors that can collect sensitive data about us. Examples include, but are not limited to: smart vacuum cleaning robots that collect floor maps of our homes to navigate; smart thermostats or electricity meters that monitor consumption and, hence, can assess our presence or absence; and smart voice assistants that may listen to our conversations.

With these devices, data collection is entering users' most private place – as in contrast to, e.g., surveillance cameras in public spaces which likewise collect data. This puts privacy and security in users' allegedly protected "castle" at risk. From a privacy perspective, it is especially critical that 1) users are oftentimes unaware of data being collected about them and, 2) data collection does not only affect primary users, but anybody in range of a sensor. Think about co-inhabitants who might be unaware of their room-mates setting up a smart speaker in the shared space; landlords installing smart meters without tenants knowing; maintenance workers or cleaners who are unaware of devices being installed in their sites of operation; or travelers being unaware of devices in a temporary rental apartment. Moreover, devices with low security standards can serve as an entry point for attackers, with severe consequences: they might not only get hold of digital, but also physical assets. For instance, attackers getting hold of presence data are able to identify the ideal moment for a physical burglary. Attackers with physical access to devices, such as smart fridges or voice assistants, are able to place orders on users' accounts. Related accounts or data might in turn be exploited further by attackers.

These scenarios highlight a need to draw attention to privacy and security in smart homes. At the same time, research for many years has emphasized the importance of focusing on users when designing for security [6, 76, 178, 236], finding that *usability* is crucial for privacy and security mechanisms for them to be applied and, ultimately, be effective. As such, users do not only need to be made aware but also be enabled and motivated to take action upon privacy and security [181, 182].

The design of privacy and security mechanisms for smart homes, however, is particularly challenging for many reasons. First, the nature of user roles and associated access permissions within homes is complex, including, e.g. inhabitants, co-inhabitants (also: children), and guests. Second, the number of devices and

functionalities, including data collection capabilities, in smart home ecosystems is rapidly growing, while advances in privacy and security for such devices are still scarce [135]. Also, conventional mechanisms do hardly scale to large smart home ecosystems. For instance, the number of passwords that users would need to remember if authenticating for each device and service separately would clearly exceed their memory [182]. Making informed privacy choices for every data collection source in users' vicinity separately can be likewise exhausting [44]. Both, privacy and security actions, can create a huge overhead if taken for each and every device or service separately, breaking with users' interaction flow. In addition, many devices do not even provide suitable modalities for conventional privacy and security mechanisms but employ workarounds. Think about a smart TV's remote control, with which we might have to enter a password to log into our preferred streaming platform. Particularly when the password is supposed to be secure, which typically means it is long and contains special characters, this is a frustrating experience. Other devices employ companion applications on smartphones to employ conventional authentication mechanisms, such as PINs or passwords, and configuration interfaces for privacy and security.

This thesis creates a better understanding of how usable privacy and security mechanisms can be designed for smart devices and homes, enabling mechanisms to be better integrated with users' daily lives within their own, as well as within visited smart homes. The results of this thesis can support researchers and practitioners with the design, implementation, and evaluation of three essential means to reclaim users' homes as their protected "castle": increasing users' awareness of privacy and security implications in smart environments; enabling device owners as well as guests to take control over privacy and security; and authentication for inhabitants and guests of smart homes.

1.2 Thesis Contributions & Research Questions

To address the illustrated challenges and ultimately protect smart homes from threats, this thesis argues for three necessary steps. First, users need to be made *aware* of potential privacy and security risks. Second, they need to be enabled to take *control* and execute privacy and security settings. Third, providing *authentication* methods that are secure as well as usable is indispensable. This thesis contributes to the following overarching research questions in the context of *smart homes*:

RQ_{AW}: How can users' privacy and security **awareness** be increased?

RQ_{CO}: How can users be empowered to execute privacy and security **control**?

RQ_{AU}: How can **authentication** be designed to be usable as well as secure?

1.3 Research Approach & Methods

Various roles need to be considered when designing privacy and security mechanisms for smart homes [93, 226, 228]. This thesis tackles two major roles (i.e., *inhabitants* and *guests*, cf. Section 2.2 for details) and investigates their awareness, and means for them to take control and authenticate within smart homes. To address the research questions outlined in Section 1.2, this thesis applies various research methods and data analysis approaches, which we explain in the following.

1.3.1 Roles

This thesis mainly focuses on two major protagonists (see Section 2.2 for details and Section 11.2.1 for a discussion around further stakeholders such as landlords):

Inhabitants (Residents, Primary Users) as those who own and *primarily* use the smart home devices. This includes the *purchase* as well as the *configuration* of devices.

Guests (Visitors, Incidentals, Passengers) who potentially are not knowledgeable of the environment and respective devices. They might stay for longer or shorter time periods in which they are *implicitly affected* by data collection, but would potentially also want to *actively co-use* devices.

All of these terms may be used interchangeably per role throughout this thesis.

1.3.2 Research Contributions & Methods

This thesis particularly contributes a number of *artifacts*, complemented by *empirical insights* [122, 221] to answer the research questions illustrated previously (Section 1.2). Data collection and analysis are described in detail in the following.

Methods

Data was collected using the following methods:

(Semi-Structured) Interview Most studies in this thesis include *semi-structured interviews*. Interviews allow investigating aspects deeply rather than broadly [122]. Following a certain structure in the interviews while keeping some degree of freedom (semi-structured) allows reacting to participants' responses [157]. We mostly combined the interviews with a concrete task such as participants using our prototypes ("contextual inquiry" [122]) or conducting a drawing exercise to illustrate

their mental models (Chapter 4). To encourage elaboration and detailed comments, we focused on open-ended questions rather than questions that can be answered with "yes" or "no" [122]. The interviews in Chapter 8 followed the story completion method [42]. Details on interview procedures and questions are in the chapters.

Expert Focus Group Focus groups can serve as a means to gather insights from multiple individuals, hence shedding light on multiple perspectives and encourage discussions, in one session [122]. In this thesis, *experts* were recruited for a focus group on authentication in smart homes (Chapter 8).

Online Survey Surveys allow inquiring a large number of participants without the researcher being present, hence allowing for broad rather than deep insights [122]. In this thesis, we combined a survey with a concrete task, that is a (simulated) configuration of a typical smart home setup (Chapter 6).

Questionnaires & Scales

All studies presented in this thesis were complemented with questionnaires including custom items as well as standard scales. Custom items included *Likert items* (statements for which the degree of agreement is measured, typically on three, five or seven points [67]) on, e.g., perceived privacy and security aspects of a prototype, and *multiple choice* questions (e.g., choosing a favorite design among several suggestions). Details on these questions can be found in the respective study descriptions.

Standard scales were used to measure one or several of the following constructs:

Usability (SUS) The usability of the prototypes was measured using the *system usability scale* (SUS). The SUS comprises 10 statements which are rated on 5-point Likert scales (where 5 refers to "strongly agree"). To calculate the SUS score, negative statements need to be inverted before adding all values. The sum is multiplied with 2.5. The overall SUS score ranges from 0 to 100, where a value greater than 68 is "above average" [29]. A mean SUS score above 71.4 is rated as *good*, and above 85.5 as *excellent* [18].

Workload (Raw-TLX) Participants' (perceived) mental workload during tasks was measured using the NASA-TLX questionnaire [91] in the "raw" version [90]. The Raw-TLX comprises 6 items: mental, physical, and temporal demand; performance; effort; frustration. Items are on a 100-points scale with steps of 5 points (1 to 20). The overall score can range from 5 to 100, with lower perceived workload the lower the score. A majority of common tasks results in a score between 26.08 and 68.00 [83].

Affinity for Technology (ATI) Participants' affinity for technology was measured using the ATI scale [71]. The scale comprises 9 statements which are rated on a 6-point scale, where "completely agree" refers to a value of 6. Three negative items need to be reversed (such that "completely agree" refers to a value of 1) before calculating the mean score. A higher mean score refers to higher affinity for technology. A representative German sample was assessed with a mean ATI of 3.61 [218].

General Privacy Concerns (IUIPC) To assess participants' general privacy concerns, we used the Internet Users' Information Privacy Concerns (IUIPC) questionnaire [134]. The IUIPC comprises 10 items which are rated on a 7-point scale, where 7 refers to higher concerns. The items are summarized into three main aspects, for which we report the mean value: users' wish to exert *Control* over their personal data; users' *Awareness* about privacy practices; and users' perceived ratio between data *Collection* and personal benefits.

Trust in Technology (HCTS) The perceived trustworthiness of a system can be measured using the human-computer trust scale (HCTS) [85]. The HCTS comprises a total of 12 items along the following subscales: *perceived risks*, *benevolence*, *competence* and *trust* [84, 85]. Every item is assessed on a scale from 1 to 5, resulting in an overall score ranging from 12 (low trust) to 60 (high trust). The subscales can be used to analyze more fine-grained aspects separately.

Data Analysis

Qualitative Data All interviews were audio-recorded and transcribed. The transcripts served as input for the analysis. We mainly followed the thematic analysis approach suggested by Braun and Clarke [26, 27]. While details can be found in the single chapters, the general approach was as follows. We first familiarized ourselves with the respective data set and applied open coding on a subset of the data to establish an initial list of codes (code book). By means of this code book, we analyzed the rest of the data, and extended the code book where necessary. Lastly, we summarized the codes to *themes*.

Multiple researchers were involved in the analysis to ensure high-quality coding [122]. However, we mainly refrain from reporting measures such as inter-rater-reliability due to the explorative nature of the studies. Instead, disagreements during the analysis process were solved through discussion [141]. We sometimes report the themes along with counts to analyze their relative importance [122].

Quantitative Data Standard questionnaires were evaluated as described in Section 1.3.2. For custom items, we use descriptive statistics [67]. In particular, we report the median, standard deviation and distribution of responses (mainly in the

form of bar charts) across the respective sample. For the larger online survey (Chapter 6), we applied statistical tests to compare the pre- and post-assessment in the different study groups. Details can be found in the chapter.

1.3.3 Ethical Considerations

In Germany, there is no need to acquire formal approval by an institutional review board (IRB) for the kind of studies presented in this thesis. Nevertheless, we carefully followed all guidelines provided by the ethics committees at all involved institutions. In particular, we made sure to preserve participants' privacy and gather informed consent prior to all studies following our national data protection regulations (cf. EU General Data Protection Regulation, GDPR). We stored all study data anonymously on university servers. We only used participants' personal data for handling the consent and reimbursement, did not connect this information to the rest of the study data and deleted it afterwards. As such, study data cannot be linked to participants' identities.

Note that the drawing exercise (Chapter 4) and story completion interviews (Chapter 8) were conducted prior to the outbreak of the COVID-19 pandemic (summer 2019). For the *PriView* study (Chapter 5, August 2020), we took great care to comply with all COVID-19 related rules in Bavaria, Germany. In particular, we kept the minimum distance to participants at all times, employed strict hand-washing practices, and made sure to disinfect the whole setup after every session as well as to air the lab. Other studies were conducted online, i.e. without any personal contact to participants (web simulation and online survey, Chapter 6 and online interviews with prototypes, Chapter 7 and Chapter 9).

1.4 Thesis Structure

This thesis comprises a total of 11 chapters that can be organized in five major parts as follows (refer to Figure 1.1 for an overview):

Part I continues with illustrating background and related work for this thesis. In Chapter 2, we set out with defining the smart home context (Section 2.1); highlight the complexity of users' various roles (Section 2.2); and illustrate privacy and security challenges in smart homes (Section 2.3). In Chapter 3, we illustrate related work on current mitigation strategies that aim at increasing awareness, enabling control, and authentication mechanisms. We highlight the limitations of these mechanisms.

To make smart homes usable, secure, and privacy protecting, it is essential to counteract threats while focusing on both, *inhabitants* and *guests*. For this, a number of steps is required, which we discuss in detail in the subsequent parts:

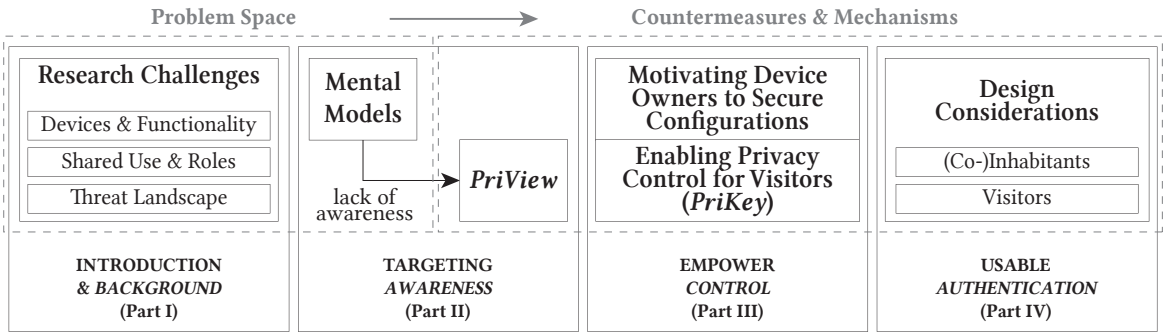


Figure 1.1: Thesis Structure: This thesis comprises a *"problem space"* (research challenges in smart homes and misconceptions in users' mental models) as well as suggestions for *countermeasures* and *mechanisms*. In particular, we target users' *awareness* (Part II), empower them to execute *control* over personal security and privacy (Part III), and investigate usable *authentication* (Part IV) for smart home contexts.

First, users need to be *aware* ($\mathbf{RQ_{AW}}$) of potential threats and privacy intrusions in smart home contexts. In **Part II**, we present our investigation of privacy mental models of smart home *inhabitants* and *guests* (Chapter 4). We identified several misconceptions, including a *lack of awareness*, especially among guests. To address this, we present our concept for privacy visualizations, *PriView*, (Chapter 5) as a means to increase users' awareness. *PriView* provides users with visualizations of potential privacy intrusions. While such a mechanism can support users in various scenarios, it can particularly help *guests* in (unfamiliar) smart homes. Awareness is a prerequisite to taking any further action to counteract threats.

Building upon users' awareness, it is also crucial to provide means for them to actively take action. Hence, in **Part III**, we investigate mechanisms to empower users to execute *control* ($\mathbf{RQ_{CO}}$) over privacy and security settings in smart homes. We looked into how device owners (most likely *inhabitants* themselves) can be nudged to employ secure smart home configurations (Chapter 6). Furthermore, with *PriKey* (Chapter 7), we enable usable privacy control, particularly targeting *guests*.

In **Part IV**, we look into usable *authentication* ($\mathbf{RQ_{AU}}$) for smart home contexts as this is an essential means to protect smart home systems and associated data in daily use. In particular, we shed light on challenges, opportunities, and design considerations (Chapter 8) for authentication within the home, considering *(co-)inhabitants*. We also explore the design of usable authentication for *guests* (Chapter 9).

Part V complements the thesis with a discussion around broader implications of the results of this thesis (Chapter 10), and concludes with a summary and future research directions (Chapter 11).

2
Fundamentals

This thesis lies at the intersection of research in IT security and human-computer-interaction (HCI), which is an emerging field of research referred to as "usable security" [76]. In particular, the design of security and privacy systems is ineffective if they are too complex for users to apply [6, 178, 182]. However, with advances in technology, the human perspective is often overlooked when it comes to privacy and security. At the same time, it is not sufficient to "blame users" as the "weakest link" [182]. Instead, research for many years calls for user-centered approaches when designing privacy and security systems [6,76,178,236]. Moreover, unlike other topics in HCI, security and privacy mechanisms are usually not targeting users' primary goal [182], and research in the field requires considering not only end-users but also potential adversaries [76].

This chapter sets out the fundamentals and motivation for this thesis: we introduce the general smart home context (Section 2.1), as well as users and their roles within this space (Section 2.2). Lastly, we illustrate the large problem space around privacy and security issues within smart homes (Section 2.3), motivating this thesis.

2.1 Setting the Scene: Smart Devices & Homes

A home is traditionally a place that conveys physical security ("a refuge from the outside world"), where users have full control over activities, with whom to share the place, and an environment that they can modify to reflect their own ideas and values [54]. More recently, our homes are increasingly equipped with devices that go beyond conventional household items such as, e.g., smart fridges, smart washing machines, vacuum cleaning robots, and smart TVs. Also novel devices, such as smart voice assistants, find their way into our homes. Popular examples include, but are not limited to, Amazon's smart voice assistant Alexa[1], Philips' Hue lightning system[2], and Google Nest devices such as cameras or thermostats[3]. The number of devices available on the consumer market is steadily rising [195].

Smart Homes
A **smart home** is equipped with devices and/or sensors that have **computing power**, are **context-aware**, and **interconnected** [17, 81, 101, 164, 174, 185, 192]. This enables remote control and automation and can serve entertainment, security, or optimization purposes to increase living comfort [8–10, 17, 22, 74, 137, 165, 180, 185].

Smart Devices The literature characterizes smart devices as *"context-aware electronic device[s] capable of performing autonomous computing and connecting to other devices wire or wirelessly for data exchange"* [192]. Thus, the home is extended with network abilities, usually including additional items such as a central smart home hub [174, 185]. Smart devices cannot only collect data about any person in their vicinity but also about the environment they are in. With devices being connected to each other, the Internet, the device manufacturer, or the provider of an associated service, the collected data is potentially shared even outside the home [135, 174].

Smart Homes Smart homes are equipped with various smart home appliances, an internal network, software-based controls, and home automation features [17, 101]. The Oxford Dictionary describes a smart home as: *"equipped with lighting, heating, and electronic devices that can be controlled remotely by smartphone or compute"* [164].

More recent research identified a smart home as *"one in which a communications network links sensors, appliances, controls and other devices to allow for remote monitoring*

[1] `https://www.amazon.com/-/de/alexa-smart-home/b?ie=UTF8&node=21442899011&ref=pe_alxhub_aucc_en_us_IC_HP_1_HUB_SMA`, last accessed April 25, 2022

[2] `https://www.philips-hue.com/en-us`, last accessed April 25, 2022

[3] `https://store.google.com/us/?hl=en-US&regionRedirect=true`, last accessed April 25, 2022

and control by occupants and others, in order to provide frequent and regular services to occupants and to the electricity system" [81]. Other definitions include the home as an assisted living facility that is *"equipped with technology that allows monitoring of its inhabitants and/or encourages independence and the maintenance of good health"* [36]. Smart homes are a popular application case of the *"Internet of Things" (IoT)*, referring to everyday objects increasingly being equipped with computing power [9, 15].

Early sample setups of smart homes for research include the *Aware Home* that was built to, among others, create an understanding of users' everyday home life and interaction within the home [111]. More recently, research employs living labs equipped with smart home technology to conduct long-term studies on user experience and appropriation [99].

Applications & Benefits Generally, smart devices primarily aim at creating a convenient living environment for users [180] by serving various purposes such as increased comfort, safety and security, and entertainment [9, 10, 17, 22, 74]. Further purposes are the optimization (of, e.g., energy consumption), (remote) control and automation, and (wireless) communication [8, 137, 165, 185]. Devices can also serve home and health care purposes by, e.g., monitoring health data to support aging in place [9, 17, 137, 185].

Smart Devices & Homes within this Thesis Rather than focusing on specific devices, we, in this thesis, focus on the context and use case of the devices: the home. While smartphones or wearable devices such as smartwatches would also fall under the category of sensor-equipped, connected devices that are potentially used within the home, these are usually exclusively used by one person as opposed to other home appliances. At the same time, smartphones or wearables oftentimes serve as a proxy or remote control and are used in conjunction with other, "classical" home devices, but are not standalone smart home devices.

2.2 Understanding Users: Roles & Permissions

Unlike personal devices and items such as smartphones or wearables, a smart home and its devices are naturally shared among multiple users [77, 229]. This not only includes those who purchase and set up the devices, but also *bystanders*. These are other individuals who do not own the devices, are more or less passive, but are still affected by the devices [43, 77, 78, 115, 226].

Inhabitants (Residents, Primary Users)
We consider **inhabitants** as those who **own** and, as such, primarily purchase, setup, configure and use devices within a smart home [77,78,115].

In a diary study with 20 households, Garg and Moreno identified a clear distinction between those who are the *device owners* and other sharees or *co-users*, indicating various levels of agency while sharing devices [77]. Koshy et al. illustrate "pilot users" as those who primarily purchase, set up, and configure devices, while "passenger users" are minimally involved in these steps, meaning the latter group might not be aware of privacy implications [115]. These smart home drivers and their co-inhabitants may face conflicts as well as cooperation in different phases, ranging from device selection to daily use [78]. Moreover, the relation between primary device owners and co-users cannot only cover individuals from within the household such as parents, partners, children, or room-mates [78], but also include individuals from outside the home. This includes *guests*, who do not live within the smart home, but might be temporarily present [7,43,93,135,138,226]. Visiting scenarios vary in terms of the relationship between owner and guests, as well as the circumstances of the visit [43]. While visiting a friend's or family member's home is a common scenario [43,62,226], it is also possible to meet smart devices outside a home environment (e.g., in stores) [43]. Lastly, it remains to be considered that relationships might also change over time as, e.g., room-mates move out or children grow up [78].

Guests (Visitors, Incidentals, Passengers)
We consider **guests** as individuals who are **temporarily present** within a smart home. They are not involved in purchasing or configuring devices, but still **implicitly affected** [7,43,77,78,93,115,135,138,226].

Permissions Device owners might want to make certain features accessible to others [93,229], but keep exclusive access to sensitive features [43,115], e.g. changing configurations [103]. All household members should have the ability to restrict (certain) access from individuals such as guests [115]. Moreover, guests should not have remote access to devices, but only while they are physically present within the home [93,135,229]. At the same time, owners should not have remote access to devices when their home is in somebody's hands (e.g., subtenants or tourists) [135].

Roles within this Thesis Prior research highlighted the need to consider multiple users in the smart home context, especially when it comes to privacy and security

mechanisms [43, 93, 115, 226, 228]. As such, we, in this thesis, particularly focus on *inhabitants* and *guests*.

2.3 Privacy & Security in Smart Homes

While providing great benefits and features (cf. Section 2.1), smart home devices also raise privacy and security concerns. In the following, we will shed light on privacy and security perceptions among inhabitants and guests (Section 2.3.1) and the large smart home threat landscape (Section 2.3.2). Both call for effective countermeasures, which we will discuss in Section 2.3.3.

2.3.1 Privacy & Security Perceptions

In general, *privacy* refers to users' ability to decide and control if and how they wish their personal data to be collected and processed by third parties [49]. Hence, privacy preferences, as well as concerns, are highly individual [43, 62, 203]. However, as computing systems become ubiquitous and tend to be invisible, users can hardly keep track of where their data is captured, and with whom it is shared [217].

Privacy
With **privacy**, we refer to users' ability to take **control** over their own personal data, and decide about its **collection** and **sharing** [49]. It is, thus, highly **subjective**.

In the context of smart homes, devices access, collect, process and store particularly sensitive data about *any* user in their vicinity, even without direct interaction [43, 62, 135, 191], as well as about the environment they are in. Examples include, but are not limited to, presence or activities of individuals. This raises major privacy and security concerns in users [3, 30, 203, 225]. In particular, they fear the physical security of their homes as well as the possibility for attackers to remotely access their devices [228, 234]. These concerns are highly subjective and impacted by a myriad of factors. This includes the type and utility of the device [43, 226], the situation and relationship to the device owner [43, 63, 124, 139, 225, 226], as well as the duration of the stay [226]. Many studies showed that users are particularly concerned about cameras and microphones (e.g., in voice assistants) [3, 35, 43, 113, 125, 153], and about data collection in private settings [62], e.g., smart devices being placed (hidden) in unknown private environments such as rental apartments [43, 136]. Prior work also showed that users wish to be informed about [43, 138, 191] and consent to data collection, independent of the context [14].

Considering the multiple roles (see Section 2.2), primary users may install devices without consulting others [78]. As such, co-inhabitants or other incidentals may be unaware of devices being in place, nor of privacy and security implications and associated risks [43, 115], especially if introduced by configuration mistakes [43]. Huang et al. showed that in households with shared smart speakers, users were concerned about false positive voice matches, as well as unwanted access to private information. Another concern was unintended use by guests [97].

Prior work also showed that both, incidental users and device owners, have privacy concerns resulting from each other: device owners do not want incidentals to access sensitive data/features via their devices, and incidentals generally feel uncomfortable with devices they are not aware of [43]. Another special case is the privacy of guests in cases the smart home owner is not present (e.g., in an Airbnb), where remote access for device owners should be selectively disabled [135]. Many users also repurpose smart devices (e.g., using security cameras for parenting or entertainment), leading to more intrusiveness along with a loss of control over personal data, also among minors [35].

Nevertheless, convenience is still a major factor for which users are willing to sacrifice their privacy, and still adopt smart home technology [62, 231], opening a need to rethink how concerns can be addressed and privacy and security be preserved in the context of smart homes.

2.3.2 Smart Home Threat Landscape

To provide their diverse and rich functionality, smart devices collect, access, and process sensitive data within the home [62, 191], and might store it in the provider's cloud [135]. Already with simple sensors, a lot of information can be revealed about smart home inhabitants' activities and routines [120]. Smart home data can be exploited for legal purposes, insurance decisions, unwanted targeted advertising, or crime [46], opening an urgent need to protect this data from strangers. At the same time, smart devices are prone to threats, opening an attack surface to users' homes [130,232]. Smart homes, however, should be protected against such attacks to be *secure*. Information security commonly follows three major goals according to the CIA triade: *Confidentiality*, *Integrity*, and *Availability*. However, heterogeneous and large-scale IoT networks make security more complex as compared to conventional systems [230]. Thus, Yin et al. add controllability and authentication as essential security properties in this context [227].

Smart Home Security
We consider a **secure** smart home setup to be **resistant against threats**. More precisely, confidentiality, availability, controllability, and authentication are essential properties of information security in the IoT [227].

With smart home devices being "little computers", conventional attacks using malware may transfer to the smart home [185]. However, smart home devices also open new attack vectors. Attacks may originate from outside or inside the home [93]. For instance, attackers could get access to sensitive data via eavesdropping or accessing cameras, potentially manipulate sensor data, and ultimately take control over a smart home [191] or manipulate devices or automation routines [189]. They could then, for instance, lock doors and, hence, lock legitimate users physically out of their homes [185], or make the smart home unusable [11]. Attackers could also (remotely) spy on the smart home inhabitants and/or remotely gain access to presence data, identify them as being absent, and plan for physical burglary [11, 185]. Someone from within the home (i.e., with physical access to devices) could access personal data or credentials that are stored on (unsecured) devices. This data could be exploited for further attacks [46].

With the interconnection of the physical and digital world in the context of smart homes, attack vectors are blending. Thus, the smart home threat landscape is often referred to as *cyber-physical* [11, 95], i.e., attackers cannot only get hold of digital, but also physical assets. This opens the need to think about effective measures to reclaim the home as users' private and secure "castle".

2.3.3 Mitigation & Countermeasures

The large threat landscape (Section 2.3.2) calls for appropriate *countermeasures*. Effective means to protect a smart home include, but are not limited to, securing the network, changing default security and privacy *configurations*, and employing mechanisms for *authentication* and access control [11, 13, 28, 43, 93, 95, 191, 232].

Authentication
With **authentication**, we refer to the process of **verifying the identity** of individuals requesting access [178] to, in the context of this thesis, a smart device or service [35]. It is typically built on one of three factors: knowledge, token, or biometric features [158].

Furthermore, encryption of data traffic, as well as physically securing devices, can hinder attackers [191]. More drastically, users could also choose to not install devices at all or at least carefully chose where to (not) install devices (e.g., placing security cameras outside the home, but not inside) [43], withholding them from the benefits devices would provide. Moreover, many users are unaware of potential threats and consequences [11, 232], and, hence, *increasing users' awareness* and potentially provide appropriate training could help mitigate threats [181, 191].

However, as device providers and consumers alike tend to focus on functionality and features [232], current privacy and security mechanisms are only limitedly effective. For instance, many devices transfer traditional desktop metaphors [93], and/or mechanisms are poorly integrated and thus rarely used [121]. Also, devices oftentimes come with insecure default configurations [232], and the setup of sharing features and access control (e.g., within a family) is tedious [35, 135]. Even worse, security and privacy are often not considered when designing smart devices, along with a lack of standards [34]. In particular, security solutions are often low-priority, and thus based on established, technical solutions rather than innovative solutions being designed in an earlier development stage [33]. Hence, users' experience of such mechanisms is limited, calling for multidisciplinary research around usable mechanisms for privacy and security [33, 34]. The multitude of devices and functionalities, along with the complex role and sharing system, additionally challenges the design of appropriate privacy and security mechanism for smart homes [93]. Moreover, many state-of-the-art smart home systems do not even provide sufficient security and privacy mechanisms [135]. The result is a lack of usability and user experience [33–35] and users unable to protect themselves [57] in the sensitive smart home context.

While this holds true for device owners and (co-)inhabitants of smart homes, it becomes even more apparent when looking at other individuals such as guests. They do not live within the smart home, do not own the devices, and, hence, usually do not have access to privacy and security interfaces. As a result of this power imbalance, they are unable to directly act upon their privacy and security needs [78, 93]. Incidental users in prior work described how they would react to smart devices being installed. For instance, they would preemptively unplug or cover devices, or otherwise change their behavior completely depending on the situation (e.g., avoiding areas with devices installed) [43]. Other options for bystanders are filtering or blocking the input to smart devices by, e.g, playing loud music to cover private conversations from microphones or physically covering cameras [7], switching devices off or asking the owner to do so, deleting collected data, or adapting their behavior (e.g., not visiting next time) [139].

To mitigate power imbalances within a household, the system could require collaboration between users to unlock access to a feature [35]. Privacy preferences could also be negotiated through conversations among multiple residents [78], as well as

among device owners and incidentals [43]. However, they might be unaware of each other's concerns [43], or social relations make this difficult [225].

To summarize, current mitigation strategies are non-ideal given the ever-increasing number of devices and features and the complex interplay of roles within the smart home. This calls for research on usable privacy and security mechanisms that target *inhabitants* and *guests* alike.

Countermeasures within this Thesis With the *privacy mechanisms* presented in this thesis, we primarily *give users control to protect their personal data* in the smart home context. With the *security mechanisms* in this thesis, we primarily help users to *protect their smart home systems from illegitimate access*, i.e. minimizing the attack surface as far as possible. Note that some mechanisms are also blending, e.g., increasing awareness of privacy and security implications helps users to act upon both.

2.4 Summary: Research Challenges in Smart Homes

While a smart home looses the boundaries between the home and the outside world, traditional values such as security within the home can and should be preserved [81], which motivates this thesis. At the same time, smart homes are a challenging context due to the plethora of individual devices as well as the complex interplay of roles in shared use scenarios, while opening an unprecedented attack surface to users' homes.

Smart Home Devices & Functionality The ever-increasing number of smart devices from varying providers and with varying functionality makes it nearly impossible to implement "standard solutions" for privacy and security. At the same time, the heterogeneity of devices makes it hard for lay users to adequately assess privacy and security implications.

Shared Use & Roles Smart devices are typically not exclusively used by one person but are part of multi-user scenarios. Also, the role system in the context of smart homes is complex. This may include, but is not limited to, primary users, co-inhabitants (including children), and guests.

Privacy & Security Data collection by sensors built-in smart home devices affects all users in their vicinity, regardless of their relation to the device. Moreover, smart devices are prone to novel attacks and threats, coming from inside or outside the home. Particularly worrisome is that physical access to a victim's home might enable attackers to gain access to digital assets – and vice versa.

Smart homes are a challenging context.
The key challenges highlighted in this chapter are:

- **Smart Home Devices & Functionality:** The current consumer market provides a plethora of devices with diverse functionality. The increasing number and heterogeneity of devices make it difficult for users to understand and act upon privacy and security implications.
- **Shared Use & Roles:** In the smart home context, devices are naturally shared among device owners, co-inhabitants, and potential guests.
- **Privacy & Security:** Smart devices collect, process, and store sensitive data about any user in their vicinity, while being prone to novel attacks and threats.

In this thesis, we aim at creating mechanisms that support users of **various roles** in **protecting their privacy** and their **smart home setups** from attacks and threats, while considering **various devices and functionalities**.

3

Learning from Current Mitigation Strategies

Several strategies can help users protecting their smart home from threats (see Section 2.3.3). In particular, users wish to be aware of data being collected about them [62,99,148,203], and to take control over their own data [7,35,139,203]. Rather than designing complete new devices with new security and privacy standards, we, in this thesis, focus on privacy and security mechanisms that can (also) be employed *in addition* to existing devices. Existing privacy and security mechanisms, however, suffer from complexity [93], limited usability [33, 34, 189], and/or poor integration [121]. Moreover, device providers and end-users alike lean towards focusing on features and convenience rather than privacy and security [232]. It is, thus, essential to not only provide users with privacy and security mechanisms but also enable and motivate them to take action [181, 182]. We illustrate current mitigation strategies and their limitations in the following. In particular, we describe approaches from related work to increase users' awareness (Section 3.1), to enable privacy and security control (Section 3.2), and to implement usable authentication in the home (Section 3.3).

3.1 Increasing Privacy & Security Awareness

Smart home devices and built-in sensors are capable of collecting data about the environment they are in, including *any* individual in their vicinity, even without direct interaction [43]. This not only puts privacy and security at risk within the home but users are oftentimes unaware of this [11, 43, 115, 232]. At the same time, prior research found that users indeed wish to be aware of their data being collected and transferred to device providers [62,99,148,203] and that making users aware is a prerequisite for them be able to act according to their privacy and security needs [43, 138, 139]. Hence, research calls to design mechanisms for privacy awareness [203, 224] that consider all affected individuals [43, 226]. Current mechanisms provide general privacy and security information *prior to devices being used* or information on devices that are already *installed* and *in use*.

3.1.1 General Privacy & Security Information

General privacy- and security-relevant information must be provided by law prior to data collection but is rarely attractive. Research has thus made several attempts to make this information more easily accessible, including appealing designs or icons, and privacy labels for apps or devices. These mechanisms specifically target those who are involved in the device purchase and/or installation.

Privacy Notices & Visualizations

Privacy notices, as are legally required, are currently the main channel of communicating data practices to end-users. However, while existing, their appearance is often neglected. To be effective, the timing, channel, and modality of privacy notices need to be considered [183]. Still, privacy policies tend to be heavy on text and are, as a consequence, rarely read thoroughly by users [215]. Research thus suggested privacy notices to be concise and salient [58] and came up with various attempts to make privacy policies more accessible and appealing. Harkous et al. suggested *PriBot*, a chatbot that can deliver privacy information and answer questions on privacy through conversations [89]. In follow-up research, Harkous et al. introduced a framework for automated analysis and presentation of privacy policies [88]. Kitkowska et al. suggested enhancing privacy policies through visual designs, which can successfully target users' curiosity to foster their understanding of privacy policies [112]. Another approach to visualizing privacy and security risks is the use of icons [59]. Mozilla's "Privacy not included guide" assesses smart devices on a scale from "not creepy" to "super creepy" visualized through emojis. This assessment is a based on crowd-sourced data[1].

[1] `https://foundation.mozilla.org/en/privacynotincluded/`, last accessed September 1, 2020

Privacy & Security Labels

Another approach that particularly targets users' purchase or installation decisions is the "nutrition label" for privacy. Initially suggested by Kelley et al., the privacy label presents information on an organization's data collection and sharing practices. Inspired by nutrition labels, the visual presentation of the privacy label is easier and more comprehensible as compared to natural language privacy policies [108]. Emami-Naeini et al. found that privacy and security information is not available to consumers prior to device purchases, yet has the potential to raise serious concerns later on. A label that comprises privacy and security information does not only make this information more accessible to users but can also inform purchase decisions [64]. In follow-up work, Emami-Naeini et al. evaluated the design of such labels in more detail with consumers and experts. Experts suggested that critical information should be displayed prominently (e.g., on the product's packaging), while less critical information can be moved to a secondary layer such as, e.g., an accompanying website and linked through, e.g., a QR code. While some of the details included in the secondary layer are harder to understand for consumers without prior knowledge, they appreciated the availability and split of information [61].

Such "nutrition labels" for security and privacy recently even became mandatory for smart devices in several countries (e.g., UK[2], Singapore[3]), and were introduced for apps by Apple[4].

3.1.2 Privacy & Security Information on Installed Devices

For devices that are already installed and in use, privacy and security information is usually unavailable or at least decoupled from the device and operation site. While devices being active in public spaces need to be communicated to passers-by given through new data protection regulations (e.g., physical signs for CCTV being active), such regulations do not exist for devices in private spaces. Some approaches tried to tackle this and increase awareness by providing information on devices, their location, or state.

[2] https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/consultation-on-the-governments-regulatory-proposals-regarding-consumer-internet-of-things-iot-security#designing-a-security-label, last accessed September 1, 2020

[3] https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme/about-cls, last accessed June 17, 2022

[4] https://mashable.com/article/apple-privacy-nutrition-labels-ios14/?europe=true, last accessed September 1, 2020

Indicators at Devices

For many smart devices, the current *state* is information that is particularly relevant to users and is thus provided by many devices through *indicators*. For instance, small LEDs help users identify whether a webcam is currently on (i.e., recording data). Amazon's Alexa comes with a light ring that changes its color if the smart assistant is currently recording users' voice [41, 121]. However, users might overlook these indicators [40, 163] or – particularly if not the device owner – not realize the meaning of this indication. Especially bystanders expressed uncertainty about device states in prior work, impacting their perceived privacy [7]. Research thus came up with alternative device indicators. For cameras being active, Koelle et al. suggested using tangible mechanisms rather than simple status lights, e.g., in the form of a flower [114]. *EyeCam* is an anthropomorphic webcam that simulates a human eye in terms of gaze (recording) direction [204]. Indicators integrated into a keyboard can increase privacy and security awareness while browsing online, e.g., in the form of color illuminations [52] or thermal warnings [152].

Device Locators

Other means also help users to not only learn about devices, data, and their state but also *locate* devices in their vicinity. This requires two steps: *detecting* sensors (i.e., data collection) being present in the environment, and means to *present* this information to users.

Detecting Sensors As for the detection of sensors (as parts of smart devices), various approaches exist. For instance, the presence of devices within a Wi-Fi or Bluetooth network can be determined by scanning for MAC addresses. Cameras are usually particularly concerning [35, 43, 113, 125, 153], especially when installed in places considered private, such as rental apartments [43, 136]. As such, the web provides several suggestions to find hidden cameras in rental apartments, including searching manually for plugged in items[5], but also apps for network scans (e.g., Fing[6]), or radio frequency detectors[7]. Recent research suggested using smartphones to emit laser signals and locate unique reflections from cameras via the phone's time-of-flight sensor [179]. Another opportunity is thermal imaging. Thermal cameras cannot only be used to detect surfaces [38] and, as such, potentially detect devices in the environment. The thermal image can also be used to determine a device's state, i.e. whether it is currently recording or not [2].

[5] `https://www.abc15.com/decodedc/technology/apps-help-track-hidden-cameras-in-airbnb-and-hotel-rentals`, last accessed August 23, 2020

[6] `https://play.google.com/store/apps/details?id=com.overlook.android.fing&hl=de`, last accessed July 03, 2020

[7] `https://www.cnbc.com/2019/06/28/how-to-find-cameras-in-your-airbnb-or-hotel-room.html`, last accessed August 23, 2020

Visualizing Device Positions Related work also looked into how to communicate devices' position to users. To this end, Song et al. suggested using visual or auditory cues that are attached to installed devices. This increased users' search efficiency compared to searching with no device locators [194]. Funk et al. visualized the indoor location of smart objects and supported users navigating there by means of smart glasses [73]. Cobb et al. suggested that such device locators should particularly target incidental users who are otherwise unaware. This could be done in the form of physical signs or sounds, and by highlighting the areas that are covered by the device's data collection [43].

Additional Awareness Mechanisms

Research also suggested some additional means to increase privacy and security awareness that are independent of the actual device(s). In their recent research, Thakkar et al. suggested four different privacy awareness mechanisms to particularly target device users as well as potential bystanders: a data dashboard on a physical device, a mobile application, ambient light, and a smart speaker emitting voice messages on privacy. They found that both, users and bystanders, preferred detailed information via a dashboard or app. However, while users' preferences were strongly focused on usability, bystanders considered social norms (e.g., avoiding awkwardness). Thus, privacy awareness mechanisms need to be designed in such a way that they are accessible and socially acceptable for both, primary users and bystanders [205].

Specific information to be transferred to users includes the data flow within smart environments. Castelli et al. visualized this and provided a visualization creation tool in a smart home living lab, and showed the usability of their system [32]. Mayer et al. visualized interactions between devices in a smart environment in a "magic lens", an augmented camera view on a tablet [140]. Kurze et al. used a technology probe to enable smart home inhabitants to familiarize with and reflect on their data, helping them to understand the implications of simple sensors [120]. Such systems can help to not only understand the data flow and interconnection of devices but also to increase awareness of privacy and security implications.

3.2 Enabling Privacy & Security Control

With an increasing number of devices and services collecting and processing user data, legal regulations require to not only inform users, but also provide mechanisms to take control and opt-out. The most common approach for this is "notice and choice" [47, 66, 186, 193]. However, control interfaces are oftentimes non-accessible [43,93], overly simplified [66] or too complex [7,77,93]. Research thus calls for more accessible and meaningful control [66, 231] and particularly bystanders

wish to have active means to limit data collection [139]. Yao et al. found that privacy control mechanisms for smart homes should ensure transparency, security, safety, and user experience. They should further allow for a certain degree of intelligence (e.g., context-awareness), and use suitable modalities [225]. However, for current smart home devices, control interfaces are oftentimes poorly integrated and, thus, rarely used [121].

In a longitudinal study with six households, Chalhoub et al. identified several usability issues in privacy and security controls of state-of-the-art smart home mechanisms. In particular, it was difficult for participants to consent or revoke data collection, and to define different levels of access for other household members [35]. As a result, users share complete accounts rather than delegating permissions, and employ workarounds such as, e.g., physically covering camera lenses [7, 35]. Both is non-ideal from a privacy and security, nor usability perspective. Existing privacy and security mechanisms are usually too complex for less tech-savvy or less experienced users and suffer from usability as the number of devices increases [44, 187].

Research thus suggested several approaches to enable privacy and security control with *additional mechanisms*, including such that particularly target *guests*.

3.2.1 Additional Mechanisms for Privacy & Security Control

To counteract privacy and security intrusions in smart environments, prior work also suggested *additional* mechanisms to give users control. These mechanisms are mostly independent of the actual devices. An example is Seymour et al.'s *Aretha*, a privacy assistant that provides knowledge in form of visualizations of the smart home network and data traffic, and enables smart home inhabitants to take control over data disclosure. Using *Aretha*, participants were not only interested in data receivers, but also in what information was shared outside their homes and why. This increased their awareness and, as a consequence, ability to take privacy and security measures on their home network using the assistant [187]. Fernandez et al. suggested *PARA*, an interface based on augmented reality that enables *in-situ* privacy control. *PARA* allows applying filters to nearby data collection. Using the interface, participants were not only more aware of privacy risks, but also applied more privacy filters as compared to current privacy management interfaces [20]. Similarly, the IoT assistant application[8] allows exploring nearby devices and data they collect, with the opportunity to opt-out.

Personalized Privacy Assistance (PPA) Another approach is to automatically predict and recommend privacy settings based on the scenario [94]. With these recommendations, personalized privacy assistants (PPA) support users to make and

[8] `https://play.google.com/store/apps/details?id=io.iotprivacy.iotassistant&hl=de&gl=US`, last accessed May 26, 2022

communicate their decision on respective settings [44]. Several use cases for this concept exist, e.g. Android applications, where the amount of data and the number of decisions is increasing [132], similar to environments with increasing numbers of (IoT) devices. In this context, PPAs can support users in keeping control over the many devices that collect and share their personal data. This can be realized, for instance, through a mobile application (cf. [50] for an overview). Colnago et al. confirmed that PPAs can help users in IoT contexts, where many privacy decisions are to be made due to the plethora of data collection sources. They suggested three possible ways to realize PPAs: sending users *notifications* about nearby devices, additionally providing *recommendations* whether to accept data collection, or *automatically* communicating settings to nearby devices. They found that most participants preferred to receive awareness, but stay in control rather than having a completely autonomous PPA. However, some were afraid of being overwhelmed by notifications as the number of decisions increases [44].

3.2.2 Privacy & Security Control for Guests

Moreover, not only device owners should have the ability to control, but also other individuals who are affected by potential data collection wish to actively consent and/or take control [62, 139, 224, 225, 229, 231]. However, incidental users usually only have limited means to take action due to what they are able and/or feel comfortable doing [43]. Control interfaces are oftentimes unavailable for co-inhabitants or guests as they require access to an associated application [93]. Current coping strategies of bystanders to take control over privacy and security are non-ideal workarounds such as, e.g., unplugging or turning off devices [43, 139], or interrupting the data collection [7, 43, 139]. Also, resignation and helplessness were mentioned in prior work [139].

As a consequence, research calls to actively empower (also) incidental users to limit or anonymize data collection and sharing in (foreign) smart environments [43, 62, 138, 139, 226]. In this regard, Cobb et al. suggested fostering communication between both, device owners and incidental users, and providing means for device owners to easily reduce data collection to accommodate others [43]. Zeng et al. suggested developing and communicating best practices for end-users to accommodate guests, e.g., muting devices when not in use [228]. Other studies found that bystanders wish to explicitly take control themselves [138, 139, 226]. Making controls explicitly available would be more comfortable for passenger users rather than using device owner's apps [115]. Yao et al. highlighted that this includes a wish for agency within a foreign property, potentially leading to conflicts with the device owner. However, they also identified that bystanders would focus on their personal data rather than on others' devices [226]. Emami-Naeini et al. suggested adapting personalized privacy assistance (PPA) in this context, rather than conventional notice and choice approaches, as these do not accommodate the number of devices,

nor different types of users [62]. Moreover, access control should be simplified to support device owners setting restrictions for visitors, e.g. based on proximity to devices or time [229].

Another option is to provide guest modes on devices that would consider the presence and privacy needs of bystanders [139,226]. For instance, devices could provide full functionality by default, but turn off data collection in case other individuals are detected within the environment. A voice assistant could stop recording when recognizing additional voices, and prevent access to account information for unrecognized voices [121,226].

3.3 Designing Authentication for Smart Homes

Conventional authentication mechanisms such as passwords were designed when users were confronted with way less computers and accounts. However, nowadays, authentication is required for a plethora of devices and services that did not need authentication before [76], including those within the smart home. Examples include devices that have access to sensitive data or critical services such as, e.g., a router or smart home hub, a fridge capable of placing grocery orders, or streaming services on a smart TV.

However, current smart home devices oftentimes do not provide sufficient affordances for authentication, but instead, conventional mechanisms are applied, e.g. using passwords or PINs via a smartphone [93]. While this might somewhat match users' expectations [93], it breaks users' experience with the actual device. A popular example is passwords that are required for many devices and associated services. As a consequence, users are forced to enter passwords via modalities that were never designed for this, such as, e.g., a smart TV's remote control. Moreover, the known phenomenon of *password fatigue* is getting worse as the number of smart home devices and services requiring passwords increases, leading users to non-ideal workarounds such as physically noting passwords down [35].

Research already highlighted the need to seamlessly integrate smart home authentication with devices [100], to ensure usability. Moreover, a home and its devices are naturally shared among various users with various roles and relationships (cf. Section 2.2), which needs to be considered when designing authentication [93,200]. For authentication for sensitive tasks on smart speakers within the home, Ponticello et al. highlight that authentication should adapt to *context*, be *transparent* and *trustworthy* in terms of whom users authenticate against, and the authentication procedure should be *effortless* (e.g., using continuous mechanisms) [162]. More generally, authentication mechanisms need to be accessible, memorable, and secure [48].

Research proposed some concrete solutions for authentication in smart homes.

3.3.1 Smart Home Authentication Mechanisms

Voice, as common input channel for smart home assistants, could be used for authentication. However, voice is currently used for personalization features rather than authentication [93] or to speak out loud low-security PINs [162]. Moreover, voice authentication could easily be eavesdropped or replayed by bystanders [93,162]. Further suggestions for explicit mechanisms include virtual touch sensing to identify users by how they "pet" IoT devices [129]. Shah et al. provide an overview of novel authentication mechanisms for ubiquitous devices not specific to smart homes, including knowledge-based mechanisms (e.g., security questions, cf. Section 9.1.1) or mechanisms based on physical or digital tokens [188]. Knowledge-based mechanisms would require either sharing the main password with all (trusted) individuals who should have access, which is not ideal, or setting up separate accounts. The latter, however, is tedious and complex on current smart home systems [35,93,135]. As for token-based mechanisms, the question remains as to who should provide the token (and to whom).

Another opportunity is continuous or implicit authentication within the home. For instance, cameras within the home could track and identify individuals, which, however, introduces (new) privacy risks [93]. Further sensors that could be used to track users' behavior for authentication include, e.g., infrared sensors to capture movement patterns, or force sensors to capture users' posture [117]. Also, Wi-Fi signals could be used to capture users' daily life activities as input for authentication [190]. Another opportunity could be to employ gait recognition at a smart home's door to authenticate legitimate users before entering [143]. While continuous authentication provides great benefits, including easily revoking access if someone is not welcome anymore [93], it requires individuals to share biometric data with the home.

3.3.2 Smart Home Authentication for Guests

As for guests, device owners might want to make some features accessible to them [93,229], but still require authentication to prevent illegitimate access as well as preventing legitimate guests from accessing sensitive features [43, 115] or changing configurations [103]. However, authentication interfaces are usually not available to co-users or guests [93]. This calls for suitable access control, authentication mechanisms, or guest modes [93, 229]. Yet, current consumer smart home systems only scarcely allow to even define different user roles, and manually configuring guest permissions is burdensome for device owners [135].

3.4 Summary & Limitations of Current Mechanisms

As sensing technologies are fluently integrated in our environment [216], including our homes, novel threats towards privacy and security arise (Section 2.3.2), that call for effective mitigation strategies (Section 2.3.3). Research has thus suggested several approaches to increase awareness (Section 3.1), enable control (Section 3.2), and employ usable authentication (Section 3.3) in the smart home context. We now summarize the limitations of these approaches. In the following parts of this thesis, we will suggest means to overcome these limitations.

Lack of Privacy & Security Awareness (Part II) Smart devices capture data about *inhabitants* and *guests* alike, raising privacy and security concerns. While perceptions towards privacy and security (cf. Section 2.3.1) of both target groups have been investigated separately, we investigate and compare mental models of smart home ecosystems among both groups in more depth (Chapter 4). We found that awareness of privacy and security limitations was limited among both, guests and inhabitants. Yet, awareness is a prerequisite to take action. However, current mechanisms to increase awareness (Section 3.1) mainly target device purchase and setup. At the same time, those who are not the device owners should be particularly informed that data is collected about them, especially as they are affected even without direct interaction [43,115]. Yet, they are usually not in hand of the device's packaging, nor involved in the setup procedure. In addition, static labels do not cover the current *state* of a device, nor the exact area of data being collected. Thus, in this thesis, we suggest *PriView* (Chapter 5) as a mechanism that increases awareness of potential privacy intrusions. *PriView* does not only help *inhabitants* as well as *guests* to *locate* devices, but to also identify their *state* and *area being covered by sensors*, as suggested by Cobb et al. [43]. To detect devices, including their state, we use thermal imaging as illustrated in Section 3.1.2.

Lack of Privacy & Security Control (Part III) Current privacy and security controls in smart home devices lack usability and are, thus, oftentimes used only as a reaction to negative experiences rather than proactively [35]. However, secure and privacy protecting device configurations are crucial to be protected against cyber-physical attacks (see Sections 2.3.2 and 2.3.3). It is, thus, essential to *motivate* end-users to actively take action. We target this by designing nudges based on the Protection Motivation Theory (PMT), which we included in a simulated smart home setup procedure (Chapter 6). Moreover, current control interfaces are usually not accessible to those who are not the device owners, which motivated us to build *PriKey* (Chapter 7). *PriKey* enables privacy control specifically for guests.

Lack of Usable Authentication Mechanisms (Part IV) Current smart home systems apply conventional authentication mechanisms (such as, e.g., passwords),

leading to poor usability and user experience [33–35, 93]. Yet, authentication is necessary to protect access to sensitive data or features within the smart home context. Guests, while being recognized as potential attackers [135, 162], are only sparsely addressed in current smart home systems [135]. In particular, it is unclear if and how legitimate guests should authenticate to access permitted features.

This raises a need to rethink how usable authentication can be designed for *inhabitants* (Chapter 8) as well as *guests* (Chapter 9) of smart homes.

Privacy and security mechanisms for smart homes are not sufficient.
This chapter highlights the **limitations** of current privacy and security mechanisms in smart homes, in particular:

- **Privacy & Security Awareness:** Mechanisms that aim at increasing users' awareness usually target device owners, who are involved in the device purchase and setup, rather than incidentals or passers-by who are likewise affected by a device's data collection.
- **Privacy & Security Control:** Privacy and security control interfaces are usually hidden, unnecessarily complex, and unavailable to those who are not the device owner.
- **Authentication Mechanisms:** Authentication within the smart home is currently poorly integrated and, thus, of limited usability. Moreover, it usually considers only one role (i.e., a main account).

In this thesis, we aim at overcoming these limitations by **targeting awareness** of inhabitants and guests alike (**Part II**), enabling both groups to exert **control** over privacy and security (**Part III**), and exploring the design of **usable authentication** considering both roles (**Part IV**).

II

Targeting Awareness

Part II – Targeting Awareness

First and foremost, users need to be *aware* of potential threats to be able to actively take countermeasures and act according to their privacy needs [43, 138, 191]. For instance, those who visit a smart home for the first time, are likely unaware of devices being in place, let alone implications on privacy and security. As such, they would be implicitly and unknowingly affected by devices, putting their privacy at risk.

We target users' awareness in this part of the thesis. As smart devices do not only affect single users but any person in range, we investigate the mental models of both, *inhabitants* and *guests*, to ultimately gain a better understanding of current awareness and potential misconceptions. In addition, we present a mechanism to help users locate and understand devices in their vicinity, to increase awareness.

- **Chapter 4** presents an in-depth investigation of mental models of smart home ecosystems, its data collection and storage among *inhabitants* and *guests* of smart homes.
- **Chapter 5** presents *PriView*, a concept for privacy visualizations to support users' awareness. We illustrate potential application scenarios, including *visits of familiar and unfamiliar smart homes*. We implemented two prototypes, namely a handheld, mobile application, and a handsfree application in a head-mounted display. We also present results of our exploratory study with both prototypes in various application scenarios.

4

Privacy Mental Models of Smart Home Visitors and Residents

This chapter is based on the following publication:
Karola Marky and **Sarah Prange**, Max Mühlhäuser, and Florian Alt. 2021. Roles Matter! Understanding Differences in the Privacy Mental Models of Smart Home Visitors and Residents. In *20th International Conference on Mobile and Ubiquitous Multimedia (MUM 2021)*. **Honorable Mention Award.**
https://doi.org/10.1145/3490632.3490664

The previous chapters highlight how the rise of smart devices in private households puts users' privacy at risk. In particular, smart home devices collect, store, and process data, independent of *who* is present and might be affected. While device owners and *residents* might be aware of devices in their homes and have the power over respective settings, *visitors* of smart homes are typically unaware of smart home devices collecting and using data about them or have little to no means to influence which data is collected about them and when [115, 138, 139, 161, 226].

Prior work showed that visitors wish to limit data sharing in foreign smart homes [62, 138, 139] and recommended to design devices that provide visitor modes [115, 139, 228, 229], to investigate options for making smart devices discoverable [194], or to provide means for visitors to exert control over the data that is collected about them [138, 226].

What remains mostly unexplored though, is whether and to what degree visitors *understand* how smart devices affect their privacy. This knowledge is yet crucial to design appropriate solutions. To close this gap, we specifically focus on the perspectives of smart home *residents* and *visitors* as well as the interplay of both roles.

In this chapter, we contribute an in-depth investigation of the privacy mental models of two roles in smart home ecosystems, namely primary users (*residents*) and bystanders (*visitors*). We invited 30 participants (15 per role) to participate in a drawing exercise. The participants were asked to illustrate their mental models of data creation, flow, and storage in smart home ecosystems. The drawing exercise was complemented by semi-structured interviews. Participants in the resident perspective were asked about their own experiences with smart home devices, while those in the visitor perspective were asked about experiences while visiting smart homes.

We found that residents generally have a more detailed understanding of data collected about them in smart home ecosystems with fewer misconceptions than visitors. Furthermore, misconceptions in the visitors' privacy mental models prevent them from acting in a way that matches their privacy needs and are independent of their technical understanding of the data flow in the smart home ecosystem. For instance, visitors often believed that active interaction or registration with a smart device (e.g., a smart doorbell) is necessary for it to collect and process sensitive data about them. Thus, future privacy and security interfaces for the smart home context need to respect both, smart home inhabitants and visitors, as well as the heterogeneity of smart home ecosystems and increasing number of devices. These findings raise the need for means to a) overall increase privacy awareness (cf. Chapter 5) and b) enable control over privacy and security settings (cf. Part III).

In this chapter, we

1. contribute an in-depth investigation of privacy **mental models** of smart home **residents** and **visitors**,
2. shed light on **differences** and **misconceptions** in these mental models based on our results.

4.1 Research Approach

Smart devices affect all users in their vicinity, including not only primary users (*residents*) but also *visitors*. Prior work investigated privacy perceptions of both roles separately and identified several *misconceptions* and a *lack of awareness* [43, 138, 139, 226]. Moreover, *multi-user* scenarios, in which all users are residents of the smart home, have been subject to prior work [78,225]. However, visiting a smart home differs from such multi-user scenarios as smart home devices can capture data without explicit interaction [43]. At the same time, mental models help users to assess technology and whether it violates their privacy. Misconceptions within these models can prevent users from acting according to their privacy needs.

4.1.1 Mental Models

Mental models are internal representations humans derive from the real world [104]. Based on mental models, humans adapt their behavior. The level of sophistication of mental models differs between individuals [24,104,107]. When using technologies, users can have two types of mental models: 1) functional and 2) structural models [156]. Users with *functional* models know how to use a technology, but not how the technology works in detail. Users with *structural* models have a detailed understanding of how a technology works. This also implies that mental models must be sound enough for users to interact with a technology [119]. Once a mental model has been constructed, it is rarely modified [208]. Misconceptions in mental models might lead users to behaviors that do not match their actual needs.

4.1.2 Research Questions

In this chapter, we answer the following research questions:

$RQ_{AW}1.a$: What are common **privacy perceptions** of **residents** and **visitors** regarding smart home ecosystems?

$RQ_{AW}1.b$: What are **misconceptions** of **residents** and **visitors** regarding privacy in the smart home data ecosystem?

$RQ_{AW}1.c$: What are **differences** in privacy perceptions of **residents** and **visitors** regarding smart home ecosystems?

In particular, we report on our empirical study, in which we investigate both, residents' and visitors' privacy mental models, by means of a drawing exercise and

semi-structured interviews (Section 4.2). This allows us to compare them in detail and investigate the origin of misconceptions (cf. results, Section 4.3). We discuss our results and implications in Section 4.4.

4.2 Methodology

To investigate the mental models of *visitors* in smart home ecosystems, we conducted two studies – one with visitors and one with *residents* – as basis for a comparison. The study for each targeted role was split into two parts: 1) a drawing exercise in which we asked participants to sketch their mental models and 2) a semi-structured interview to obtain a deeper understanding. Drawing exercises are effective to capture the mental models of users considering specific systems or technologies [107, 228, 233]. We further opted for semi-structured interviews since they offer a certain structure while at the same time providing enough freedom to investigate participants' perceptions in depth [157]. To inform the interview guide, we conducted one exploratory interview per targeted role. Further pilot tests helped improve question clarity. Results from the pilots are not reported.

4.2.1 Procedure

The procedure was identical for both targeted roles. However, we adapted the questions and the scenario to match the respective role. All sessions were audio-recorded, while the sketching surface was also video-recorded during the drawing process. A session lasted approximately one hour in total. We deliberately did not mention "privacy" in the study invitation, nor the consent form or interview questions to avoid priming. The detailed procedure was as follows (cf. Figure 4.1):

1.) **Consent and Demographics.** We commenced by providing participants a consent form which we asked them to sign. Next, participants provided demographics, including their living situation, employment status, affinity for technology following the ATI scale [71], and experiences with the usage of smart devices. We included the 10-item IUIPC [134] to assess participants' privacy perception prior to the study (see Section 1.3.2 for details on scales).

2.) **Drawing Exercise.** We introduced participants to the scenario to nudge them to think based on their role. Residents were asked to consider devices that they use at their home while visitors were asked to consider visiting the smart home of another person. Then, participants conducted the drawing exercise. We provided a piece of paper in DIN A3 size and pens in different colors.

Participants in prior studies including a drawing exercise (cf. [233]) faced two challenges. First, it was difficult for them to add details to their sketches resulting in very simple sketches. Second, the participants struggled in commencing with sketching. To mitigate these issues, we provided a wide range of printed cut-outs of smart home devices that the participants could choose for their sketches. We furthermore wanted to ensure that participants indeed consider a smart home ecosystem as a whole. In particular, we asked them to choose devices of five categories of smart home devices that are already available on the market (at least one each). Those categories were: 1) entertainment and communication, 2) energy management, 3) security and safety, 4) health and 5) home automation (cf. Appendix A.1 for the full list of devices). We specifically asked participants to sketch their understanding of how the devices are connected to each other, including their understanding of the data flow with a focus on data that contains personal information about them. During the drawing exercise, we encouraged participants to think aloud and comment on what they were drawing. Previous studies demonstrated the effectiveness of this combination [228].

3.) **Semi-Structured Interview.** We proceeded with role-specific, semi-structured interviews. We used the sketch from the previous part as the basis for the discussion. Participants were instructed to highlight devices and entities that collect or receive data about them and explain their understanding of it. We also asked them to label entities in their sketches to clarify them.

4.) **End and Reimbursement.** After the interview, we gave participants the opportunity to ask questions or to provide additional feedback. Finally, we reimbursed them with an online shopping voucher valued at 10 €.

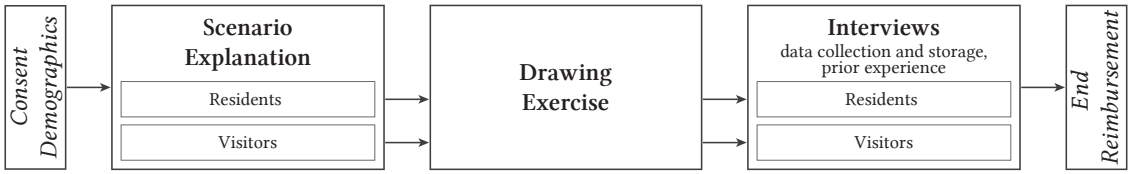


Figure 4.1: Study Procedure: We investigated the mental models of two roles within smart home ecosystems, that is *residents* and *visitors*. Participants were introduced to the respective scenario (role) and conducted a drawing exercise. We complemented the sessions with role-specific, semi-structured interviews on data collection and storage, and prior experience with smart homes.

4.2.2 Participants and Recruitment

We recruited 30 participants (15 residents, 15 visitors) via mailing lists, flyers, poster advertisements, and social networks. We aimed at recruiting participants with different experiences regarding smart home devices in order to capture a wide range of possible mental models. Considering the resident role, we invited participants that either already own smart home devices or are interested in buying devices soon. We did not apply restrictions to the visitor role.

Demographics

Participants' age ranged from 18 to 64 ($M = 30.33$, $SD = 12.12$), $N = 7$ identified as female, most of them were students ($N = 18$), and living with their family ($N = 10$). By means of the ATI scale [71], we assessed participants' affinity for technology on a scale from 1 to 6, where higher values indicate a higher affinity for technology. Residents' ATI ranged from 2 to 5.78 ($M = 4.06$, $SD = 1.04$), visitors' ATI was similar and ranged from 2.78 to 5.56 ($M = 4.33$, $SD = 0.66$). Table 4.1 provides an overview of our sample. Refer to Appendix A.2 for details per participant.

		Residents	Visitors	Sum
Age	Mean	35.73	24.93	30.33
	SD	15.29	2.84	12.12
Gender	male	12	11	23
	female	3	4	7
	prefer not to say	0	0	0
	other	0	0	0
Work	student	7	11	18
	self-employed	3	0	3
	employed full time	0	3	3
	other	5	1	3
ATI Scale	Min	2.00	2.78	2.00
	Max	5.78	5.56	5.78
	Mean	4.06	4.33	4.19
	SD	1.04	0.66	0.86

Table 4.1: Participants' demographics, employment status, and ATI scale, for residents, visitors and both.

Prior Experiences with Smart Devices

Within the demographics questionnaire, we asked participants to list their own smart home devices, if applicable. Furthermore, we asked them about prior experiences and how often they interacted with smart devices (at home and in general) in the semi-structured interview. Overall, ten participants (residents: 6, visitors: 4) reported owning smart devices[1]. Of them, three participants in the resident role

[1] In case only the smartphone was mentioned (questionnaire and/or interview), we did not count it as it is not a standalone smart home device, but is usually used together with other devices.

and one in the visitor role had multiple smart home devices that are connected to each other. Participants reported on *further* experiences with smart home devices, including visits of smart homes (residents: 2, visitors: 11), or having shared a device (e.g., in their flat share, visitors: 2).

Privacy Perceptions

To assess participants' privacy perception, we applied the 10-item IUIPC questionnaire [134] (cf. Section 1.3.2). Higher values in the IUIPC scales indicate that participants are more sensitive regarding privacy concerns. Overall, they rated their wish to exert *Control* with $M = 6.07$ (residents: 6.15, visitors: 6.00), their *Awareness* about privacy practices with $M = 6.1$ (residents: 6.2, visitors: 6.00), and the perceived ratio between *Collection* and benefits with $M = 5.38$ (residents: 5.42, visitors: 5.33, refer to Appendix A.3 for detailed values).

4.2.3 Data Analysis

First, we transcribed the audio recordings and digitized the sketches. Then, we analyzed the sketches and interview transcripts in two sessions using thematic analysis [27]. The analysis consisted of open, axial and selective coding.

In the first session, we analyzed the *level of sophistication* of the mental models expressed in the *sketches*. For this, we followed an open-coding approach in which two authors were coders. In an initial discussion, they developed a code dictionary. The dictionary consisted of four codes for the expressed level of sophistication by reviewing all sketches and by agreeing on a final code dictionary. Then, they independently coded all sketches. Results were discussed and final code allocations for each drawing were agreed upon. Throughout the analysis, we also considered the audio recordings to complement the information expressed in the sketches in cases where parts of the drawing were unclear. To determine the inter-rater reliability, we calculated Cohen's κ, which is 0.824 (almost perfect agreement).

In the second session, we analyzed the *interview transcripts* to develop the mental models of *data collection and storage*. Two researchers individually coded two representative interviews for each view, using thematic analysis with open coding. We then established a coding tree in a review meeting and applied it to the remaining interview transcripts. The coding tree consists of 103 codes. We related those codes to each other by using axial coding which resulted in six final categories of codes. Through selective coding, we removed codes without sufficient data to be considered as robust, such as codes which were used only once over all participants. The full coding tree is available in Appendix A.4.

Finally, based on the codes from the transcript analysis and the level of sophistication, we developed participants' mental models of the smart home ecosystem, including their perception of entities that capture and store personal data.

4.2.4 Limitations

Due to the qualitative nature of our study, quantitative conclusions cannot be made. We provided our participants with printed pictures from smart home devices to support them during the drawing exercise, which might have had an impact on their drawings. However, in order not to limit them in their expression, we provided products that are already available on the market from a wide range of product categories. To create a list of available devices, we systematically searched best-seller lists of online stores resulting in a list of 89 smart home devices. We grouped similar devices and provided a generic depiction as print out to the participants. Not to limit them in their drawing, we also told them that they could add devices if they are not present as print-out.

Our sample consists of participants with a mean age of 30.33 years. While the usage of smart homes is dominant within this age group in Germany [196], our sample might not be representative. Furthermore, 18 of 30 participants were students and many were living with their family (10) or partner (9). Hence, our results may only apply to users with a similar background.

4.3 Results

In this section, we illustrate the findings of our study. First, we provide a descriptive overview of the *content and topology* of the participants' sketches showing the devices and additional entities they incorporated. Then, we present the mental models on the *smart home ecosystem*, *data collection*, and *data storage*. We cite residents as P_R (N_R for descriptive counts) and visitors as P_V (N_V).

4.3.1 Content and Topology

In this section, we summarize the content of participants' sketches. We provide details on the *devices* chosen by the participants, *additional entities* they added to their sketches, and the *topology of the sketches*. This serves as a descriptive overview about what the participants drew.

Device Choice

To ensure that participants consider an ecosystem of *different devices*, we asked them to choose one device from each of the following five categories: 1) entertainment and communication, 2) energy management, 3) security and safety, 4) health and 5) home automation. Participants were free to add further entities and devices. Appendix A.1 provides an overview of available and chosen devices.

In general, participants in the visitor scenario tended to choose devices with which they would interact directly (e.g., the smart doorbell ($N_V = 4$)), while residents rather chose devices that are likely to be used in their home even without a constant direct interaction (e.g., smart heating ($N_R = 4$)). Considering specific devices, both groups mostly added a smartphone for communication ($N_R = 8$, $N_V = 7$), smart lights for energy management ($N_R = 8$, $N_V = 7$), and smartwatches for health ($N_R = 8$, $N_V = 12$) to their sketch. As for security and safety, participants mostly chose a smart smoke detector ($N_R = 5$, $N_V = 5$). For automation, a smart vacuum cleaner was most popular for residents ($N_R = 6$) and smart jalousies or fridges ($N_V = 4$ each) for visitors.

Additional Entities

Participants were not limited to the five chosen devices. All of them added *additional entities* in their sketches (cf. Table 4.2 for an overview). First, they added physical *objects* and devices (e.g., routers) or set the scene with concrete rooms of their smart home scenario. Second, *abstract entities*, such as service providers, the Internet, or apps were mentioned in some sketches. Third, participants added themselves as *a user*. Finally, some added *potential threats* (such as hackers) to the ecosystem.

		N_R	N_V	Sum
Objects & Setting	Router	6	3	9
	Homes / Houses / Rooms	2	2	4
	Additional Smart Devices	6	11	17
Abstract Entities	Apps & Services	5	0	5
	Companies & Providers	9	2	11
	Cloud	3	2	5
	Internet	5	5	10
People	User	5	1	6
	Guest	0	3	3
Threats	Hackers	2	0	2
	digital footprint	1	0	0

Table 4.2: Overview of additional entities: participants added various entities to their sketches (N_R: counts for residents, N_V: visitors).

Topology of Sketches

All participants except for one resident arranged their sketch around a *central node* which is connected with the majority of devices to control them and/or process and store the data. The central node was either a local server/network or router within the smart home ($N_V = 5$, $N_R = 4$), an external server that is reachable over the Internet ($N_V = 2$, $N_R = 0$), an additional IoT/smart device, such as a smartphone/tablet ($N_V = 5$, $N_R = 8$), the users themselves ($N_R = 2$), a generic/unspecified device ($N_V = 2$, $N_R = 2$) or a smart home app ($N_R = 1$). Note that 2 residents specified both, a router and a smartphone, as central device. Residents stated, e.g.:

> *"(...) they're connected somehow. But I don't know how it gets there."* (P_R8)
>
> *"There is that central component, but I don't know how this is called."* (P_R13)

Comments given by the participants in the visitor target group are:

> *"A Wi-Fi router or maybe the particular company has its own kind of wireless connector that wirelessly controls all the devices."* (P_V12)
>
> *"Well, there is the smartphone from which everything can be controlled."* (P_V5)

Furthermore, participants had different understandings of how the entities of the smart home ecosystem can be *connected* to each other. Devices were either connected via a local Wi-Fi network, Bluetooth, or the Internet.

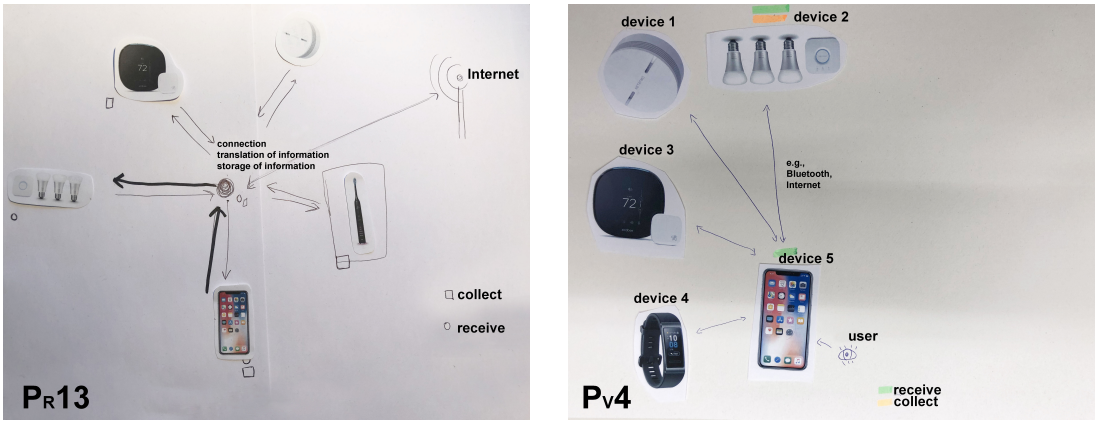
4.3.2 Level of Detail

Based on the interviews and sketches, we found four types of mental models regarding the smart home ecosystem, differing in their *level of sophistication*. For the individual assignment of each participant to a mental model, refer to Appendix A.2. Previous work on mental models of smart home users used two levels of sophistication (e.g., [203]). We provide a more nuanced view to demonstrate differences between the investigated target groups of visitors and residents.

1.) Schematic Simplification. Some participants illustrated smart home technologies without a detailed understanding, referring to a functional mental model [156]. Accordingly, they only sketched connections between the devices within the five categories provided by the examiner. These connections were not further specified. The role of external entities, such as the Internet or external service providers, were not explained or not mentioned at all.

For instance, P_R13 in the resident group only connected the five devices with a point in the middle that represents a network between them (see Fig. 4.2a). Similarly, P_V4

in the visitor group used the smartphone as a central node and sketched simplified connections to the smart home devices, depicting additional entities outside the home (see Fig. 4.2b). Five visitors and three residents demonstrated this level.



(a) Schematic Simplification (Resident) (b) Schematic Simplification (Visitor)

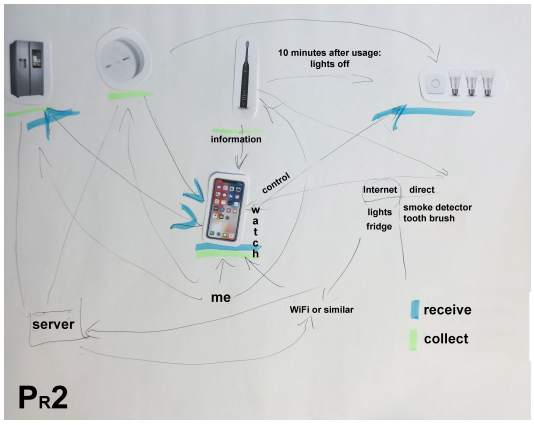
Figure 4.2: Participants' sketches showing examples of *schematic simplification* mental models. We replaced participants' notes with digital labels to enhance readability.

2.) Basic Understanding. This type of model is characterized by extending the previous type with external entities, such as the Internet or a cloud as well as a clear connection to them. The basic understanding also forms a functional model [156] since details are very limited.

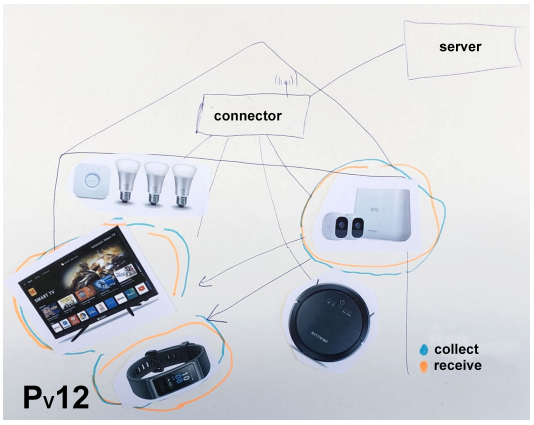
For instance, P_R2 sketched a basic server as an additional entity and an Internet connection (Fig. 4.3a). P_V12 drew an external server and a connector within the smart home and different connections between entities (Fig. 4.3b). Seven visitors demonstrated a basic understanding, and three participants in the resident group.

3.) Advanced Understanding. Participants demonstrating an advanced understanding frequently sketched a central component (e.g., a smartphone or server) controlling all other devices. They made a distinction between a local network and the Internet and added other components (e.g., a central server) that go beyond the five categories we provided. This forms a basic structural model since details about the connections and topology are included [156].

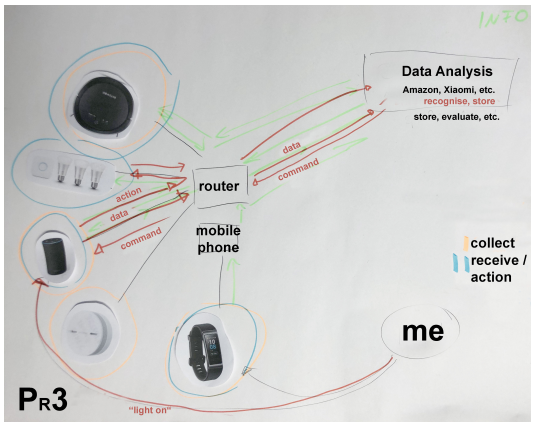
P_R3 depicted different types of connections. They made a distinction between data within the smart home and data that leaves it but did not differentiate entities outside the smart home (Fig. 4.3c). P_V15 drew a similar sketch but included a window and a treadmill within the smart home. Again the entities outside the home were simplified (see Fig. 4.3d). Six visitors showed an advanced understanding, and five participants in the resident group did.



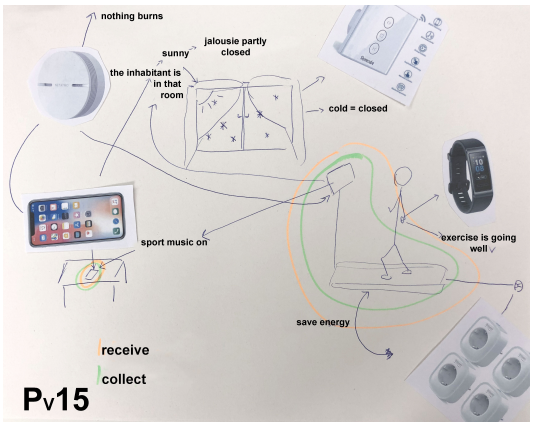
(a) Basic Understanding (Resident)



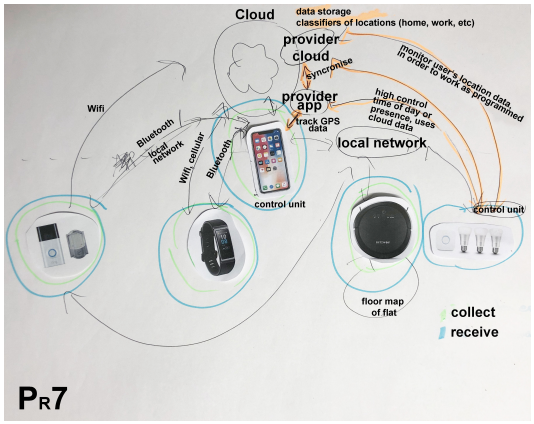
(b) Basic Understanding (Visitor)



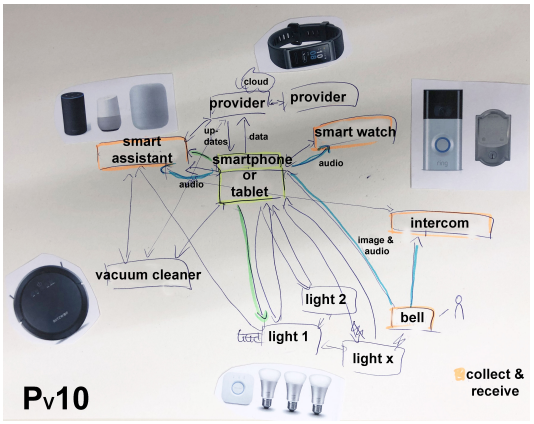
(c) Advanced Understanding (Resident)



(d) Advanced Understanding (Visitor)



(e) High-level Depiction (Resident)



(f) High-level Depiction (Visitor)

Figure 4.3: Participants' sketches showing examples of *basic*, *advanced*, and *high-level understanding* mental models. We replaced participants' notes with digital labels to enhance readability.

4.) High-level Understanding. The high-level understanding is a sophisticated structural model [156]. The participants made clear distinctions between different network types within and outside the smart home. They added additional entities, such as the Internet, clouds, and even attack surfaces. They also sketched a clear data flow between the devices.

For instance, P_R7 demonstrated a detailed understanding of entities outside the smart home by including entities such as a cloud, different providers, and data types (see Fig. 4.3e). P_V10 added different providers, a cloud, and the Internet and sketched the connections between the different devices, the possibility to receive updates and how to interact with them as a visitor (see Fig. 4.3f). One participant in the visitor group showed a high-level understanding and four residents did.

4.3.3 Data Collection

We asked participants to mark devices that *collect* data about them (e.g., new data created by sensors) and to explain how the data collection works according to their understanding. We also asked them to mark devices that *receive* data (e.g., existing data within the ecosystem captured by other devices' sensors) about them and to explain how.

1.) No interaction, no data collection. This cluster of mental models describes cases in which no data is collected automatically but only as users directly interact with a smart home device. Six participants in the visitor target group believed that devices do not collect data about them unless they directly interact with the device's interface. Surveillance cameras and motion sensors form an exception. For these, participants understood they only need to be in the vicinity of the devices.

> *"I also do not know who registers that I am out of the house and what registers that I am out of the house and what registers that the lights are still on, no idea."* (P_R13, schematic simplification)

> *"It depends a lot on the usage. For example, if I would charge my phone and go to the power outlet. But in principle the power outlet could collect data from me [...] I don't wear the smartwatch, thus I do not think so [that it collects data about me]."* (P_V14, basic understanding)

This model was prominent among participants with a functional mental model of the smart home ecosystem, i.e. a schematic simplification or a basic understanding.

2.) No registration, no personal data. Another aspect mentioned by visitors is that even if they interact with a device that captures data, the data is not personal unless they register as users with the specific device. This was mentioned by four participants in the visitor target group, e.g.:

> *"With the refrigerator, the question is what kind of functionality it has. In principle, if I take a beer out now, it collects data somewhere that at least one beer is missing. It probably can't assign it to me, but it is missing."* (P_V14, basic understanding)

> *"When I sit on the sofa as a guest and switch through the TV, I also generate data. Also not individually, so they can't draw conclusions about me, nevertheless, it generates data (...)"* (P_V2, advanced understanding)

Again, this type of model was mostly expressed by participants with a functional mental model, i.e. a schematic simplification or a basic understanding.

3.) Known devices form exceptions. Visitors believed that smartphones collect data about smart home visitors. All participants who explained this aspect connected it to their experiences with smartphones:

> *"With a smartphone, I could imagine the front camera running or anything else being recorded. The moment it is collected, I always assume that it will be stored."* (P_V11, schematic simplification)

4.) All devices collect data, except wearables. Participants expressed that in general all devices in the vicinity of a person can collect data about them. Wearables, however, form an exception as participants expected that they have to be worn to collect data. Two participants in the visitor target group expressed that all smart home devices collect data about them. They considered the resident's smartwatch as an exception because the visitor is not wearing it, e.g.:

> *"All except for the owner's smartphone and smartwatch."* (P_V9, basic understanding)

> *"Generally all [devices] that I've described I would say, except for the smartwatch."* (P_V6, basic understanding)

5.) Local actions without an Internet connection. When considering the data flow, participants in both groups believed that a connection to the Internet is only required if controlling or accessing data from a device at a remote location but not to trigger a local action.

> *"I think it is also a simple connection because only mechanically something [the jalousie] goes up and down. Compared to other devices, there is no connection to the Internet in the sense that it is now looking or something special."* (P_R5, advanced understanding)

> *"What I actually think about are light bulbs, but I don't need light bulbs that I have to switch off from outside the house, I just need a light bulb where I don't have to get up from the bed."* (P_R12, high-level understanding)

6.) Configuration by a third party can violate privacy. Two participants in the visitor group reported negative experiences based on smart devices that were configured by a third party in their own apartment, e.g.:

> *"My landlord installed a device showing how warm it is in the room and how humid the air was, and said it would be for my own control when I have to ventilate and turn on the heating. [...] Later, I found out that this [device] sent data via Wi-Fi to my landlord's laptop. He actually came up and knocked if it was too warm or too humid or something and told me to air the room. Unpleasant experience."* (P_V4, schematic simplification)

4.3.4 Data Storage

Finally, we assessed mental models on where data collected in smart home environments is *stored*.

1.) Data is stored locally. Participants that described this mental model believed that data about them is only stored within the smart home (network). It could be stored on the smart device itself ($N_V = 6$, $N_R = 1$), or on a dedicated storage device ($N_V = 4$, $N_R = 4$), e.g.:

> *"I think the [vacuum] robot has its own processing power, it does not need a cloud."* (P_R7, high-level)

> *"The best thing would be to have your own server, where your data [...] is stored, without the data leaking out, without anyone being able to infer consumer behavior from it [...]. Only if you then agree correspondingly, the data may also be used."* (P_R15, schematic depiction)

2.) Data is stored remotely. Remote storage refers to a cloud server accessible via the internet ($N_V = 2$, $N_R = 3$). Note, that only the smart home user was perceived to have access to it, e.g.:

"On the devices themselves only for a short time, because I assume that not much data can be stored there and that there is no storage capacity, i.e. the data is always deleted. Everything is stored in the cloud." (P_V2, advanced understanding)

3.) Data is stored remotely by the provider. In this model, the data is stored in the cloud of the device provider ($N_V = 8$, $N_R = 7$), e.g.:

"On a server. Someone is the provider of all of that." (P_V5, advanced understanding)

"[...] I'm scared because I don't know exactly what's going to happen with the data." (P_R14, adv. understanding)

4.) No knowledge of data storing. Finally, one participant from the visitor group expressed to have no idea where the data is stored:

"I don't know. I really don't know. I could imagine that there might be local memory for one thing, but probably it will be more like cloud-based external memory. I don't know." (P_V14, basic understanding)

4.4 Discussion

We now discuss the results of our study, in particular the difficulty to derive a sound mental model due to the *heterogeneity of smart home ecosystems*, as well as the *differences* and *misconceptions* in the mental models of visitors compared to residents.

4.4.1 $RQ_{AW}1.a$: Privacy Perceptions Towards Heterogeneous Smart Home Ecosystems

The first common theme throughout our results is a difficulty with the heterogeneity of smart homes. While a generic smart home ecosystem can be explained by a simplified depiction, there are a plethora of possibilities to configure specific environments. This results from the large variety of devices on the market. For instance, smart TVs range from simple models with a Wi-Fi connection to more sophisticated models with additional sensors, such as microphones or even cameras. Thus, there is no standard way of abstracting the data collected and stored by an arbitrary smart home device.

Heterogeneity is also reflected by the various connection types and device configurations participants sketched. This indicates that it is difficult to judge whether a device collects data without prior knowledge making it particularly difficult to derive a sound mental model of a specific smart home, especially for visitors. Participants in both roles correctly depicted the data flow of specific devices that they had prior knowledge of, for example, Amazon Echos. Furthermore, the data captured by smartphones was depicted accurately. This might result from most smartphones sharing a common set of sensors and being well-known to participants. As a result, a mental model being correct for one smart home might be wrong for another. However, known devices were depicted accurately.

Prior work has also shown that once established, existing mental models are difficult to change [208]. Hence, residents or visitors with pre-existing mental models of privacy-respecting smart home ecosystems might not easily adjust their mental model to a new, less privacy-respecting smart home ecosystem. While residents can adjust their mental models over time as they interact with or add new devices, visitors might face difficulties in adjusting their mental models as the environment is less well-known to them and might change without their knowledge. Thus, they might rely even more on their – potentially wrong – mental models.

This answers **RQ_{AW}1.a**: *What are common privacy perceptions of residents and visitors regarding smart home ecosystems?*

4.4.2 RQ_{AW}1.b: Misconceptions of Visitors and Residents

Within our study, we identified several misconceptions in the mental models in both roles, but mainly in visitors' mental models.

Visitors often illustrated the data collection in such a way that only devices they actively interact with are able to collect data about them (e.g., the doorbell), while other devices (i.e., those they did not interact with actively) were mostly considered to not collect information about visitors. While this holds true for some devices, it is not representative. Sensors in the environment might indeed collect data about visitors without them interacting actively. However, cameras and motion sensors formed an exception. Similar to smartphones, those devices are more common nowadays and, thus, participants demonstrated better knowledge about them.

Furthermore, visitors underestimated how personal and sensitive collected data about them can be. Visitors frequently thought that registration on the device is necessary such that collected data can be linked to their identity (e.g., login into an account). While this again can be true, the interconnectivity of smart home devices might result in data getting linked to a specific person without previously being registered to an account. This might lead visitors to act in a way that does not match their privacy needs.

Our research confirms this misconception as it has also been demonstrated by related work [139]. While main factors impacting privacy perceptions identified by related work are data sensitivity, familiarity with the environment, and trust in the device owner (cf. [62, 138]), we add users' *role* within the smart home ecosystem to this list. Based on our results, we assume that the origin of the misconceptions is not necessarily rooted in technology affinity or understanding, but connected to the users' role within the smart home. In particular, visitors with rather high ATI scores and sophisticated sketches of the smart home ecosystem still showed misconceptions regarding data collected about them. Moreover, participants of both target groups expressed that a connection to the Internet is required for remote control rather than for data collection and processing.

It is particularly alarming that even visitors with advanced mental models about the data flow did not consider data to be linkable to them. That means previous knowledge of a specific smart home device is not enough to judge the consequences of data collection. Lastly, (faults in) users' mental models may persist and can highly impact their privacy perceptions potentially preventing them from acting in a way that matches their privacy needs. This addresses $\mathbf{RQ_{AW}1.b}$: *What are misconceptions of residents and visitors regarding privacy in the smart home ecosystems?*

4.4.3 $RQ_{AW}1.c$: Differences in Privacy Perceptions

Our study also provides insights on how the mental models can differ depending on the users' role (resident or visitor). A first main difference is given by different distributions of the mental models considering the level of sophistication. While we did not perform a quantitative analysis, the residents' mental models tended to be more sophisticated. This can result from the active usage of a technology, enhancing the understanding of it.

The second main difference we found in the mental models is based on the perception of devices that collect and store data about residents and visitors. As illustrated before, bystanders underestimated the sensitivity of collected data because they thought the data cannot be linked to their identity. This difference seems to be based on the different perspectives of the investigated roles rather than on their understanding or affinity of technology. While visitors and residents demonstrated a similar level of sophistication in their mental models with detailed knowledge about data collection and storage, visitors in our study missed the connection between collected data and their identity.

The final main difference is given by the fact that visitors were more likely to demonstrate misconceptions in their mental models than residents. This could prevent them from acting according to their privacy needs.

To summarize, the differences in mental models are primarily based on the user's role, i.e. resident or visitor. Hence, considering privacy, the user's role is more im-

portant than their technology knowledge, answering $\mathbf{RQ_{AW}1.c}$: *What are differences in the privacy perceptions of residents and visitors regarding smart home ecosystems?*

4.5 Summary & Conclusion

In this chapter, we presented the findings from a qualitative study investigating the privacy mental models of *residents* and *visitors* in smart home environments. We interviewed 30 participants (15 in each target group) by means of a drawing exercise and semi-structured interviews. The mental models of our participants had four different levels of sophistication. Those with rather functional mental models miss enough soundness to act following their privacy needs. As further results, we revealed essential differences in the perceptions of visitors and residents regarding the collection and storage of sensitive data. Even though participants in both roles had a similar understanding of the data flow in smart home ecosystems, visitors voiced several misconceptions connected to sensitive data that is captured about them. These misconceptions prevent them from protecting their privacy matching their personal needs. Hence, roles matter more than technology knowledge. Improving the privacy mental models, in particular for visitors who might have limited abilities to act within the environment, constitutes a fundamental challenge due to the heterogeneity of smart home environments and the increasing number of devices. Hence, it is essential to a) provide mechanisms that *increase awareness*, especially for visitors in (foreign) smart homes, and b) provide them with means to *configure and communicate their privacy preferences* without interfering with the device owner. These findings pave the way for the following chapters of this thesis, which will make suggestions on how such mechanisms could be realized: *PriView* to increase awareness (Chapter 5), and *PriKey* to enable control (Chapter 7).

Misconceptions in mental models limit privacy & security awareness.

The key contributions in this chapter are:

- **Method:** Using two scenarios (resident or visitor of a smart home) and a drawing exercise with semi-structured interviews, we investigated users' mental models of smart home ecosystems.
- **Empirical Insights:** We found that even users' with a rather high level of sophistication in their mental models missed enough soundness to correctly assess their data being collected and stored, with implications on privacy and security. This was particularly prominent among visitors.

The results of this chapter call for mechanisms that raise users' awareness. Not only should users be made aware of the functionality of a certain technology, to enjoy interacting with it, but more importantly also of privacy and security implications to ultimately be able to protect themselves.

5

PriView– Exploring Visualizations to Support Users' Privacy Awareness

This chapter is based on the following publication:
Sarah Prange, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. *PriView* – Exploring Visualisations to Support Users' Privacy Awareness. In *CHI Conference on Human Factors in Computing Systems (CHI '21)*.
https://doi.org/10.1145/3411764.3445067

The previous chapter highlighted a need for means to increase awareness of data being collected by sensors in our daily life surroundings. Such sensors can be found in personal devices as well as in our environment. While in many cases the data collected by those sensors serve a meaningful purpose, such as assisting users or ensuring public safety, their presence might be problematic from a privacy point of view. In particular those who are not the owner of devices are typically unaware of sensors and, hence, data collection being present, which is problematic from a privacy point of view as they cannot avoid being exposed to them.

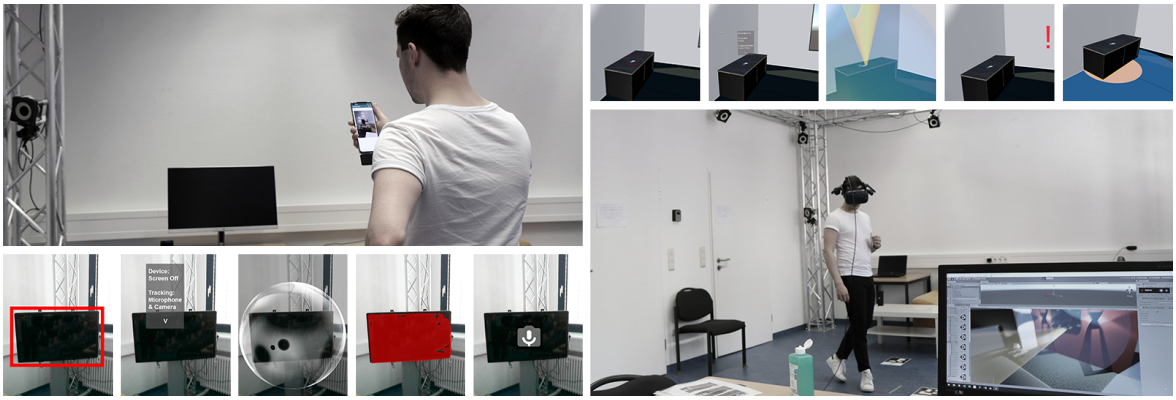


Figure 5.1: *PriView* is a concept to visualize potential privacy intrusion (i.e., video or audio recordings) in the users' vicinity. We compared two output devices, namely a mobile application (left) and a head-mounted display (right) and implemented five visualizations for each. We found that detailed text labels were preferred in both versions. However, more subtle indications were considered adequate in some scenarios.

Think about guests in smart homes who might be unaware of the loudspeakers serving as voice assistants or hidden cameras that might be placed in rental apartments[1,2]. Other scenarios beyond the home include public transport stations where users generally do not know where surveillance cameras are placed and whether additional measures, such as face recognition, are employed[3]; or business settings where smartphones carried by employees might observe their environment or record conversations. In such cases, people might want to know about devices to deliberately decide to avoid a particular area or not to disclose certain information.

In this chapter, we present *PriView* as a concept to support users in such situations. The idea is to visualize the position of sensors in the environment; provide users information about the sensor (e.g., which data is collected and with whom it is shared); and in particular, highlight areas of potential privacy intrusion (such as video or audio recording). An example output device for such visualizations is Augmented Reality (AR) glasses. AR is likely to find its way into users' everyday life in the near future (cf. Apple's new generation of AR glasses[4]).

[1] `https://www.theatlantic.com/technology/archive/2019/03/what-happens-when-you-find-cameras-your-airbnb/585007/`, last accessed August 9, 2020

[2] `https://www.forbes.com/sites/suzannerowankelleher/2020/01/27/why-you-should-start-screening-for-hidden-spy-cameras-when-you-travel/#ffe069b5afd8`, last accessed September 1, 2020

[3] `https://www.theguardian.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras`, last accessed August 9, 2020

[4] refer to, e.g. `https://www.techradar.com/news/apple-glasses`, last accessed June 26, 2020

We first explore the design space and possible application scenarios of *PriView*. Secondly, we built two prototypes, namely a) a mobile application capable of detecting smart devices in the environment using a thermal camera; and b) mockups of possible application scenarios, private as well as public, where *PriView* might be useful (e.g., a public train station or a rental apartment), using Virtual Reality (VR). For both applications, we implemented various ways of visualizing the privacy relevant information (e.g., frames around the device or text labels with detailed information). Thirdly, we report on a user study (N=24) in which we investigated both versions of *PriView*. In particular, we let users try out our prototypes using the think aloud method and conducted semi-structured interviews.

Our results show that participants appreciated the ease of using a headset to explore their environments, but could also imagine using *PriView* in a mobile application on-demand. For unfamiliar private places in which device owners and the purpose of data collection might be unclear, participants generally wished for more detailed visualizations, while appreciating simple warning indications to get a first overview in a new scene.

With ***PriView***, we contribute

1. potential application scenarios and design opportunities for **privacy visualizations** in both, private and public spaces;
2. **two prototypes** (a mobile and a VR application), exploring both, detection and visualization of smart devices in the user's vicinity and various sample use cases (VR only);
3. a discussion of our results, formulation of **design challenges**, and directions for future research.

5.1 Research Approach

Users might be unaware of (hidden) smart devices collecting their personal data [39] and generally wish for information in that regard, in particular in spaces they perceive as private [194]. We implemented *PriView* to help users not only physically *locate* but also *understand* sources of potential tracking by providing them with AR visualizations in a mobile application or a head-mounted display (HMD). Moreover, with *PriView*, users can identify sensors that are *static* in arbitrary environments, but also *dynamic* devices (e.g., smartphones in bystanders' pockets). In addition, *PriView* highlights *areas being covered* by potential recording (i.e., potential privacy intrusion) and provides *additional information* (e.g., data practices). This will help users to take

action, if necessary. Additionally, as opposed to existing measures, *PriView* is independent of device providers in the first place as we suggest detecting devices in users' vicinity using sensing technology such as a thermal camera. With our work, we contribute to answering the following research questions:

RQ_{AW}2.a: Can ***PriView*** support users in protecting their privacy?

RQ_{AW}2.b: Which **amount of information** do users prefer (in which context) and why?

RQ_{AW}2.c: Which **type of visualization** is most preferred by users for which setting?

RQ_{AW}2.d: How would users like to **interact** with such visualizations?

In the following, we describe potential application scenarios for our concept, based on factors that impact users' privacy concerns (Section 5.2). Next, we describe our concrete implementations for *PriView* (Section 5.3). We then report on our user study with two prototypes using two output devices, namely a mobile application and an HMD (Section 5.4). We illustrate our results and discuss challenges of privacy visualizations for varying smart environments (Section 5.5). We conclude with potential future implementations of *PriView* (Section 5.6).

5.2 Application Scenarios for *PriView*

To choose a sample of application scenarios for *PriView*, we built upon factors impacting users' privacy concerns.

5.2.1 Factors Impacting Privacy Concerns

Smart devices are increasingly present in users' daily surroundings, including their own homes, but also other places such as unfamiliar private households, hotel rooms or public spaces. While such devices provide a rich variety of features (cf. Section 2.1), they have the potential to invade users' privacy by collecting and processing their data. Users' acceptance of such devices is influenced by a myriad of factors, including perceived privacy risks [116] and perceived benefits [169]. Tabassum et al. investigated user perceptions and concerns towards smart homes and respective data policies and highlighted the need for increased awareness [203].

Moreover, concerns are no longer bound to a device, but rather to the whole scenario. In particular, related work identified a myriad of factors that influence users' privacy perception as well as ultimately their concerns [40,63,123–126,225,226] and decisions as to when and where data collection is acceptable. Among these are the (perceived) information sensitivity, receiver, and usage [5] as well as who is collecting what data, where, for which reason, and at which frequency (i.e., once vs continuously) [125]. We now discuss a number of these factors in detail.

Social Aspects & Trust

Social aspects and relationships have been identified as a crucial factor for users when it comes to making their own decisions on their opinion of data collection [63,124,225,226]. For example, users are more willing to accept data collection if friends do so as well [63]. Furthermore, it is very important to users who is collecting their data (i.e., the identity of the "information inquirer") [124]. In particular, users are more willing to share their data if they know and/or trust the owner of a device [138]. Finally, users also tend to make a difference as to whether or not they trust the environment. For instance, in unfamiliar smart home settings, such as rental apartments, users are concerned about hidden devices and even tend to search for them manually [194].

Environment

Also, users' relation to the environment plays an important role when assessing potential privacy concerns. For instance, data monitoring in private spaces such as users' own or others' homes is completely unacceptable, while they are more comfortable with data collection in semi-public (e.g., restaurants) or public spaces [62,125]. Furthermore, users' privacy concerns are influenced by how often and for how long data is monitored [125]. This is often coupled to the frequency at which they visit a certain place. Note that while an environment is unfamiliar – hence likely untrusted – upon users' first visit, this fact is likely to change over time as users visit a place more often. Finally, in semi-public and public places, data collection might be dynamic as passers-by might carry further tracking technologies.

Context, Devices & Purpose

Furthermore, the context – including the purpose, type, and frequency of data collection [40,125,126], data processing policies and storage – as well as the concrete devices and their capabilities are important factors. For example, cameras and microphones have been shown to be particularly privacy invasive sensors to users as they are capturing sensitive data [113]. Photo and video-based monitoring is generally considered unacceptable, regardless of the purpose [125]. Users are also uncomfortable with continuously recording audio and are – while still feeling uncomfortable – more willing to accept occasional recordings, especially for work environments requiring confidentiality [113].

Many sample devices exist that include these sensors. Examples are personal devices (such as smartphones) as well as ubiquitous devices in public spaces (such as CCTV cameras). While personal sensing is gaining popularity and acceptance (for example, monitoring personal data for long-term goals, such as losing weight [19]), ubiquitous sensing in varying environments is less personal, but at the same time less controllable for users, which makes informed privacy decision challenging.

Summary

Users' perception of privacy and concerns highly depend on the context [62, 154], what is being recorded in a particular context, and the perceived value of the recordings [113]. Furthermore, users are concerned about their privacy and wish to be *aware* of devices recording their data and the affected space [43,139,194,226], as well as respective data processing [203]. Hence, we built *PriView* for various scenarios.

5.2.2 Sample Scenarios

As privacy highly depends on context [154,155,225], related work has used various scenarios when it comes to privacy in the context of the Internet of Things (IoT) (cf., e.g. [63,225,226]). However, using fictional IoT scenarios for research purposes comes with several limitations. In case participants are not familiar with the factors that build the scenario (such as, e.g., devices, place), results might be limited. IoT scenarios being used in online surveys suffer from the fact that participants conduct the survey in a decoupled place that may not at all be related to the scenario [125]. In our lab study, we used VR as a means to overcome this limitation and immerse participants in the scenario as best as possible. Based on the factors discussed in Section 5.2.1, we chose the following six sample scenarios (cf. Figure 5.2).

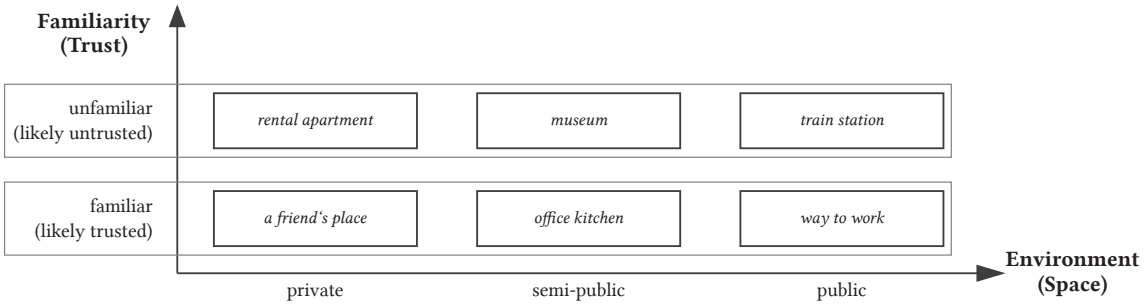


Figure 5.2: We created 6 scenarios for the evaluation of *PriView*, differing in the space (cf. "Environment", namely private, semi-public and public) and the users' familiarity with it (cf. "Familiarity"). Note that we consider familiar places to be likely trusted by users, while unfamiliar places are likely to be untrusted.

Public Environment

In public environments, users might be more hesitant to share their personal data, especially if they are unaware of data collection and policies. At the same time, if benefits are clear, users are more willing to accept their data being tracked [153,169] (e.g., CCTV in a train station for safety reasons).

Unfamiliar Users who are traveling in a foreign country might be interested in knowing which data is being collected, e.g. in a *train station*. While their main goal is finding their way, they might also want to avoid their personal data being collected in this public space (e.g., avoid being on CCTV). Such places tend to be crowded, opening the opportunity for further data collection sources being carried by other people, but also for hiding in the crowd.

Familiar Users on their daily *way to work* are highly familiar with the place. However, it is still public, and they might be unaware of potential data collection. Especially in this scenario, data collection might be inconspicuous, such as through personal devices carried by passers-by or sensors in smart cars.

Semi-Public Environment

In semi-public environments, the number of ubiquitous sensors might be more limited as compared to public spaces, as the fluctuation of personal devices is less high and/or owners of personal devices are known to the user.

Unfamiliar In a *museum*, users' primary intention is usually to visit the exhibition. At the same time, data recording in the form of surveillance cameras, interactive exhibits or other visitors' personal devices might be present.

Familiar In a shared *office kitchen*, users usually enjoy coffee/tea or lunch breaks during long workdays. However, smart kitchen appliances including audio recording capabilities might be present. While users are familiar with all people who can access this space, they might want to avoid, e.g., being eavesdropped by the device owner (i.e., their boss).

Private Environment

In private environments, users expect their privacy to be protected by default. However, in times of smart home devices being on the rise, data recording might not stop at private places' doors.

Unfamiliar In a *rental apartment*, users might appreciate the convenience of smart devices, but on the other hand be concerned about their privacy, hence, be reluctant to share personal information (e.g., browsing history) with their (unknown) host [136]. Such scenarios have been applied in prior investigations [225,226].

Familiar In contrast, at *a friend's place*, the device owner, as well as the environment, are well known to users. However, users still might not want to share, for example, their private conversations, with device providers.

5.3 Design & Implementation Samples of *PriView*

To explore the rich opportunities of *PriView*, we implemented a set of *visualizations* on two different *output devices* (i.e., a smartphone (mobile) and a head-mounted display (HMD)). Table 5.1 provides an overview on which visualization was shown on which device.

Bounding Boxes	**Text Labels**	**3D Shapes**	**Segmentation**	**Sensor Icons**	**Warning Icon**	**Floor Markers**
frames around devices	textual descriptions	3D tracking space	thermal highlighting	camera, microphone icons	static exclamation mark	2D tracking space
Mobile HMD	Mobile HMD	Mobile HMD	Mobile –	Mobile –	– HMD	– HMD

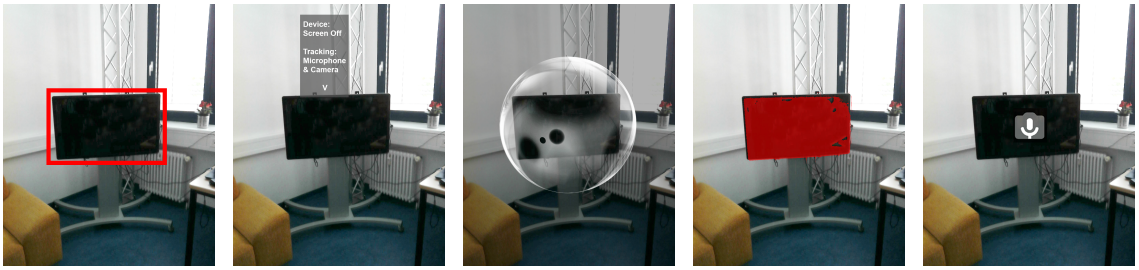
Table 5.1: Visualization samples we implemented for *PriView*, in the mobile application and VR prototype (HMD), respectively.

5.3.1 Visualizations

With many sensors being present in personal devices and our environment(s), it becomes increasingly harder for users to keep track of what information is collected about them when and where. At the same time, several factors influence their privacy concerns (cf. Section 5.2.1) that can be addressed by communicating respective information. *PriView* could provide, e.g., information on device position, type of sensor, type of data being collected, tracking space, and device status. We implemented the following sample visualizations, differing in the provided information:

Bounding Boxes To highlight devices in the users' vicinity, red frames are displayed around them (mobile cf. Fig. 5.3a, HMD cf. Fig. 5.4a). *Bounding Boxes* are mainly creating awareness of specific devices and their location.

Text Labels To hint at devices while at the same time providing additional information, we implemented *Text Labels* (mobile cf. Fig. 5.3b, HMD cf. Fig. 5.4b). Similar to the Bounding Boxes, labels show the devices' position, but also information such as the device name, provider, and data being collected. This information was selected as prior work shows that this particularly matters to users [40, 113, 125, 126].



(a) **Bounding Boxes** (b) **Text Labels** (c) **3D Shapes** (d) **Segmentation** (e) **Sensor Icons**

Figure 5.3: *PriView* in a mobile application: We implemented five types of visualization, namely a) Bounding Boxes (framing the device), b) Text Labels (indicating the device's state), c) 3D Shapes (around the device), d) Segmentation (thermal highlighting), and e) Sensor Icons (camera or microphone).

3D Shapes To visualize devices' potential tracking space, this visualization shows *3D Shapes* emerging from the devices' sensors (mobile cf. Fig. 5.3c, HMD cf. Fig. 5.4c). As users generally wish for information about the physical space being affected [139,226], this visualization informs users about and enables them to avoid such spaces.

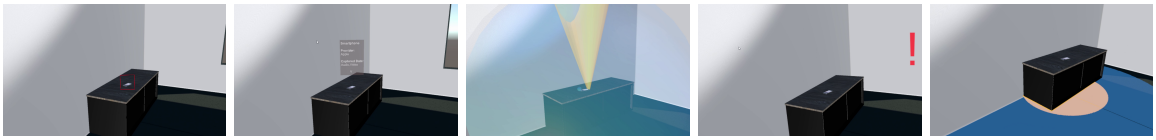
Segmentation To not only highlight a device but also indicate its (thermal) state, we use *Segmentation*. This visualization is strongly coupled to our detection modality, i.e. the thermal camera (mobile application only, cf. Fig. 5.3d).

Sensor Icons As an unobtrusive indicator per device, we implemented camera and microphone icons as these data types are especially relevant to users [113] (mobile application only, cf. Fig. 5.3e).

Warning Icon As an additional visual indicator, we added an exclamation mark in a general, static position (bound to the users' view, HMD only, cf. Fig. 5.4d). This supports users' wish to be generally aware of data being recorded [194].

Floor Markers As a more decent variant of showing devices' tracking spaces, we implemented 2D *Floor Markers* (HMD only, cf. Fig. 5.4e).

We argue that there is no "one-fits-all" solution of *PriView*. Rather the specific visualizations are intended to support particular scenarios. For instance, in some cases it might be sufficient for users to have the *Warning Icon* as a general indicator, while in other cases the visualization should be as detailed as the *Text Labels* or an indication of the specific tracking space is desired.



(a) **Bounding Boxes** (b) **Text Labels** (c) **3D Shapes** (d) **Warning Icon** (e) **Floor Markers**

Figure 5.4: *PriView* in VR: We implemented five types of visualization, namely a) Bounding Boxes (framing the device), b) Text Labels (indicating manufacturer, sensor and data being collected), c) 3D Shapes (highlighting the tracking space for audio: blue bubble, and video: yellow cone), d) a Warning Icon (general alert), and d) Floor Markers (highlighting the tracking space for audio: blue circle, and video: yellow circle).

5.3.2 Output Devices: Handheld vs. Handsfree

While *PriView*'s visualizations could be shown on any handheld output device such as a smartphone screen or as a physical image of the environment (cf. [194] for an example of device locators on contextual images), it could be used more immersively by means of, e.g., augmented reality as it provides an "ideal interface to IoT applications" [219]. We particularly investigated a handheld device (smartphone) and a handsfree device (head-mounted display).

Furthermore, while most visualizations are *device-centric* and thus should be shown within the environment, a *general* indicator such as our warning icon could be shown on any personal device. While device locators, as suggested by Song et al. [194], help find devices that are static in the environment, using *PriView* in a mobile application or an HMD allows new and/or moving devices in the users' environment to be *dynamically* highlighted. Regardless of the output modality, *PriView* can be activated and interacted with in various ways. For instance, scanning the environment with the smartphone is equivalent to an "on demand" concept, while mockups in the HMD can be "always on". Alternatives could show visualizations implicitly on change or on proximity.

5.4 Study: Exploring the Opportunities of *PriView*

To explore the rich opportunities of *PriView*, and to answer our *RQs*, we implemented two prototypes, namely device detection and visualization in a mobile application (Part I, Section 5.4.1) and visualizations in an HMD in various scenarios using virtual reality (VR) scenes (Part II, Section 5.4.2). We implemented a total of seven possible visualizations, three of which are similar in both systems and two that are unique for the respective output device (cf. Table 5.1 for an overview). We evaluated both prototypes in an exploratory lab study in combined study sessions (i.e., participants experienced both prototypes subsequently).

5.4.1 Part I: Smart Device State Detection using *PriView*

Implementation

We built an Android application capable of detecting a) locations of smart devices and b) their state (on/off) by means of a FLIR One[5] thermal camera attached to the smartphone. Our implementation utilizes the fact that different devices have different temperature profiles captured by thermal cameras. Additionally, this temperature profile changes based on the operation state of the device. Our application analyses the FLIR One's camera stream. We trained the real-time object detection framework Yolo [172] to detect the position of a subset of smart devices, namely an Amazon Echo Dot, a speaker, a laptop, a screen, and a mobile phone, with an average loss of 0.4143[6]. Furthermore, we created another model that can detect the devices' state (i.e., on vs off) with an accuracy of over 90%.

Visualizations

The mobile application can represent the respective information (i.e., device position and state) in five different visualizations (cf. Figure 5.3). Note that combinations of these might be suitable, yet we showed them separately to participants.

Apparatus

For the study, we designed a setting in our lab including the aforementioned sample of devices that our mobile application is able to detect. In particular, we placed an Amazon Echo Dot, a speaker, a laptop, a screen and a mobile phone in varying positions in our lab. Note that we also used varying specific devices (e.g., we used multiple smartphones) to reduce learning effects. We provided participants with the application running on a OnePlus 8 smartphone complemented with the FLIR One thermal camera dongle. Participants were to search for the devices without (i.e., baseline) and using all visualizations in the mobile application (i.e., five search tasks in counterbalanced order). We created a device layout for every visualization, consisting of five devices each. We made sure to have a consistently low search difficulty (i.e., all devices were visible rather than hidden) as we wanted participants to focus on the visualizations. We ensured consistent environmental conditions (e.g., lightning). After every search task, participants answered 5-point Likert items on comfort, learnability, understandability, and frequency of use (cf. Appendix B.1.1). In a final questionnaire, we acquired usability using the system usability scale (SUS) [29] and cognitive workload using the NASA-TLX (Raw TLX [90], see Section 1.3.2 for details on scales). We additionally conducted semi-structured

[5] `https://developer.flir.com/flir-one-software-development-kit/`, last accessed July 28, 2020

[6] Note that loss is a way of evaluating models by giving them a larger penalty for each mistake, i.e. the lower the loss, the better.

interviews particularly covering participants' experience with the application and potential use cases (cf. Appendix B.1.2 for full interview guide).

Study Design

We conducted a within subjects study with VISUALIZATION TYPE and DEVICE POSITION as independent variables. We counterbalanced the order of VISUALIZATION TYPE according to a Latin Square [220]. For each representation, participants' conducted a search task using our mobile application, i.e. name all devices they could find in our lab. We deliberately did not reveal the total number of devices present per condition (five devices per condition). Note that in this part of the study, using *PriView* was participants' *primary task*. We varied DEVICE POSITION in our lab setting to avoid learning effects. However, we coupled DEVICE POSITION to VISUALIZATION TYPE, i.e. device position per visualization was consistent for each participant to ensure comparability.

We asked participants to think aloud while searching and particularly include the devices they found as well as the information they got from the application. In addition, participants rated use and feel per visualization on 5-point Likert scales (cf. Appendix B.1.1). We complemented this part of the session with a questionnaire (SUS and Raw TLX) and semi-structured interview (cf. Appendix B.1.2).

5.4.2 Part II: *PriView* in Various VR Scenarios

Visualizations

We implemented five sample visualizations (refer to Figure 5.4) in the HMD. We did not investigate possible combinations but showed them separately to participants.

Scenes

We implemented 6 sample scenes (cf. Figure 5.2 for an overview and Appendix B.2.1 for detailed descriptions):

Rental apartment (bedroom): an unfamiliar private place

A friend's place (living room): a familiar private place

Museum: an unfamiliar semi-public space

Office kitchen: a familiar semi-public space

Train station: an unfamiliar public space

Way to work (street): a familiar public space

In every scene, we placed various tracking sources (i.e., devices with cameras and microphones) for which we employed the visualizations (cf. Section 5.4.2). However, not all of them might have been able to actually track the user (e.g., in the train station scene, passengers on the train were recording audio using their smartphone while the user was on the track outside the train).

Implementation

We built the scenes using the Unity game engine and made them accessible to participants via an HTC VIVE Pro headset (2880 $\times$ 1600 pixels combined, 90 Hz, 110° fov), using the SteamVR plugin. The application was running on a stationary HP VR backpack computer with Windows 10. Participants were free to move within a 4 m $\times$ 4 m tracking space, covered by 2 VIVE base stations (Gen 2.0). Participants' view and actions could be monitored from the Unity "ingame" view. In every scene, every visualization could be activated and deactivated during run time by the experimenter. Some visualizations were rendered to be always on top (*Bounding Boxes*, *Text Labels* and the *Warning Icon*), others blended with the environment (*3D Shapes* and *Floor Markers*).

Apparatus

We implemented five samples of visualizations (cf. Figure 5.4) in six sample environments (cf. Figure 5.2) in VR. In every scene, we gave participants a number of details such as their relation to the environment (cf. Appendix B.2.1 for detailed scenario descriptions). We chose VR as a tool to immerse participants in the respective scenarios, together with the story details. Note that the VR application did not include a detection part, but mockups of devices and respective tracking spaces within the virtual scene. Participants tried every scene using an HTC Vive Pro headset. There was no search task for the scenes, however, we asked them to think aloud and report on their experience. After every scene, participants answered 5-point Likert items on comfort and frequency of use and ranked the five visualizations from most preferred to least preferred (referring to the current scene, respectively). After all scenes, we put 5-point Likert items per visualization on learnability and understandability (we provided screenshots of all five visualizations for recap). We measured usability of an HMD as an output device for *PriView* using the SUS [29] and workload using the Raw TLX [90] (Section 1.3.2 provides details on scales). We conducted a final semi-structured interview covering participants' experience, potential usage contexts, preferred visualization, and preferred output device (i.e., mobile application vs HMD, cf. Appendix B.2.3 for full interview guide).

Study Design

We conducted a within subjects study with SCENARIO and VISUALIZATION as independent variables. Every participant experienced every VISUALIZATION in every

SCENARIO. The order of scenarios was counterbalanced using a Latin Square [220]. Within SCENARIO, we counterbalanced the order of VISUALIZATION. Note that in most scenarios, using *PriView* would be the *secondary tasks* (e.g., at a train station, users' main task is usually to find their way). However, within the study, exploring the environment and visualizations was participants' main task. We asked participants to think aloud while exploring the environments. Each scenario was complemented by a questionnaire on comfort, use, and preferred visualization (refer to Appendix B.2.2). The session ended with a final questionnaire on the VR part (including Likert items for every visualization, SUS, and Raw TLX), the IUIPC scale [134] to acquire participants general privacy perception and a semi-structured interview, including opinions on the VR prototype, potential use cases and a comparison to the mobile application (refer to Appendix B.2.3).

5.4.3 Procedure

To ensure a smooth study procedure, we conducted a total of three pilot runs. The final procedure was as follows. Upon arrival at our institute, we asked participants to disinfect and wash their hands (the two experimenters did the same). They then signed a consent form, and we introduced them to the general concept of *PriView*. Participants then conducted the study (cf. Figure 5.5):

Study Part I. Participants first conducted the baseline task (i.e., search for devices in our lab without using the mobile application). We then send them to a PC behind a black curtain to fill in demographics, while we would rearrange the DEVICE POSITION. We then introduced them to our mobile application. Next, they conducted five search tasks using every VISUALIZATION in counterbalanced order. After every task, they filled in Likert items (on comfort, learnability, understandability and frequency of use, cf. Appendix B.1.1) on the PC behind the black curtain while we changed DEVICE POSITION. After the last search task, participants filled the SUS and Raw TLX for the mobile application, and we conducted a semi-structured interview (cf. Appendix B.1.2 for the full interview guide).

Study Part II. We introduced participants to the idea of using *PriView* in everyday life using a head-mounted display (in the form of, e.g., AR glasses), and presented our prototype. Participants then experienced every VISUALIZATION in every SCENARIO in counterbalanced order. After every SCENARIO, participants filled in Likert items on comfort, potential use and preferred visualization (cf. Appendix B.2.2). After the last SCENARIO, participants filled in a final questionnaire (including learnability and understandability of the visualizations, SUS and Raw TLX of the VR application, and the IUIPC scale, cf. Appendix B.2.2) and we interviewed them (cf. Appendix B.2.3 for the full interview guide).

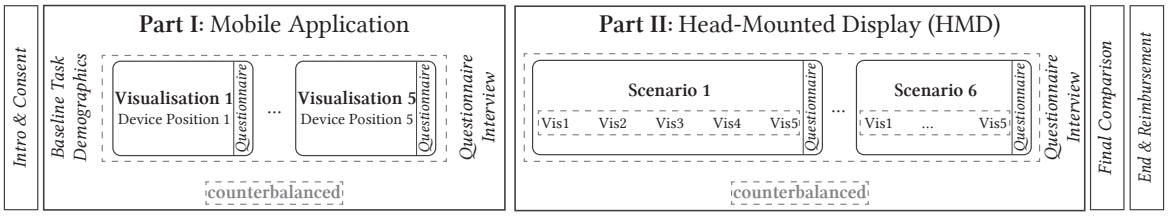


Figure 5.5: Study Procedure: We investigated two *output devices* of *PriView*, namely a mobile application (Part I) and a head-mounted display (Part II). We used a within-subjects design in which every participant encountered Part I and II in this order. In both parts, we explored various visualizations. For the mobile application, participants conducted a total of 6 search tasks: one without using the application (baseline) and, in counterbalanced order, one for every visualization. Each task was followed by a questionnaire. For the HMD, participants experienced various application scenarios in counterbalanced order. Within every scenario, we counterbalanced all five visualizations. Each scenario was followed by a questionnaire. We complemented the session with an interview and a final comparison of both output devices.

We concluded with a final question on comparing the two prototypes (i.e., handheld vs handsfree) and an opportunity for participants for further comments or questions. We recorded audio during the whole session. We conducted interviews in English or German.

5.4.4 Recruitment

We recruited 24 participants through university mailing lists and social networks. The study took place in a single, separate room at our institute. A study session took around 90 minutes in total. Participants were reimbursed with 15 €.

5.4.5 Participants

A total of 24 people participated in our study, 9 female and 15 male (we additionally provided "other" and "prefer not to say", but no participant chose that). Participants' age ranged from 20 to 56 ($M = 25.54$, $SD = 6.95$). Most of them were students (18), others employed full and part-time (3 each). Participants rated their prior experience with VR ($M = 2.33$), AR ($M = 2.21$), and smart homes ($M = 2.87$) on a 5-point scale (1=Low). We additionally asked participants to list their smart devices. They mentioned between 0 and 10 devices (mean number of devices: $M = 2.79$), mostly smartphones (22), but also smart TVs (7), smart speakers (6), and more. Using the IUIPC [134], participants rated their wish for *control* ($M = 5.75$[7], $SD = 1.19$), a high

[7] the IUIPC ranges from 1 to 7, where 7 denotes high sensitivity towards privacy, see Section 1.3.2

awareness ($M = 6.24^7$, $SD = 1.05$), and the perceived ratio between benefits and *collection* ($M = 5.44^7$, $SD = 1.39$).

5.4.6 Limitations

Our sample is biased towards young male students and might thus not be representative. Moreover, we chose a within-subject design to make participants experience our approach from both, a technical (Part I) and a conceptual (Part II) perspective. We only compare participants' preference regarding output device after they experienced both parts, hence we assume latency and recency effects to be minimal.

For our lab setting (Part I), we applied randomization to the order of visualizations and respective device positions, yet we cannot fully exclude learning effects in the search tasks. Moreover, we only explored a subset of devices and possible visualizations. Lastly, the study was conducted in a single room to avoid noise in the device detection, hence we cannot make assumptions about different settings.

For the varying scenarios in VR (Part II), we took great care to immerse participants in the different settings. However, not every scenario might have been realistic to every participant (e.g., if they never happened to find a recording device in a rental apartment). Furthermore, self-reports on privacy preferences are known to differ from users' actual behavior (cf. the "privacy paradox", see [79] for an overview).

5.4.7 Data Analysis

All think-aloud and interview recordings from both parts were transcribed for analysis (except for one corrupted audio recording). Initially, three researchers performed inductive coding for three participants independently and discussed the results with each other. The researchers agreed on a code book containing a total of 67 codes (cf. Appendix B.3). Disagreements were tracked, and inter-rater agreement was calculated at 89.82%. Then, two coders proceeded with half of the remaining transcripts each and coded them independently by means of the code book. They compared and discussed codes and resolved any disagreements. In the following, we present first qualitative insights towards our concept[8]. We enumerate participants from P1 to P24. Quotes were translated from German where necessary.

[8] Our sample comprises 24 participants. Note that only little new information is gained beyond 20 participants [149].

5.5 Results & Discussion

We summarize and discuss the results of our study in the form of *design challenges*. While some results are strongly coupled to the respective *output device*, we will also highlight overarching opinions towards our concept.

5.5.1 Overall Perception of *PriView*

Participants overall were positive towards the idea of *PriView*, e.g.:

> *"Actually, I think the idea is pretty cool. I think there is a lot of concerns about technology nowadays (...), so that's good to have something user-friendly."* (P2)

> *"It was a very good experience for me to see that some devices are on, (...) and informed me that they are tracking or recording anything of me."* (P6)

> *"It was interesting, especially the [Text Labels] so I can actually see that the device is turned on, and I see there is a microphone, and it could actually record me (...) It was also fun to see visually, (...)."* (P8)

> *"I like that they show you where there is a recording device. The application, I think, is really useful."* (P18)

In particular, it made them feel safer (e.g., *"I really felt safer, because I feel like when I walk out of here, I will think a lot about which information I'm sharing with third parties."*, P16), supported them to protect their privacy (e.g., *"I wouldn't say it protects it directly, but when you use the app, and you see that there is a camera or microphone you might behave differently, and this protects your privacy."*, P7) and enabled them to take countermeasures, if necessary:

> *"Let's take the hotel room example. There I could unplug the smart TV or something like that."* (P14)

> *"And I would turn it off or ask the host to pick it up or take it away. For the smart TV, I think I would put a post-it or so [to cover the camera]."* (P19)

PriView also supported participants in finding devices (e.g., *"(...) it did help me know a lot of devices which otherwise I would have had no chances of knowing."*, P24), which was perceived positively.

5.5.2 Output Devices

We particularly compared two output devices for using *PriView*, namely a mobile application and an HMD. Participants saw benefits in both, but mostly preferred the HMD ($N = 19$).

Handheld: Mobile Application

Overall, the mobile application received positive feedback with a rather high SUS ($M = 71.14$[9], $SD = 8.53$) and a rather low cognitive workload ((Raw) NASA-TLX $M = 14.28$[10], $SD = 4.52$). Participants particularly liked that the app was *"very innovative and comfortable"* (P24), convenient (P17, P20), and easy to use (P15, P16, P19, P20). Participants preferring the mobile application over the HMD particularly appreciated the fact that they would have it with them anyway (P17) and could put it away anytime (P11).

Furthermore, they felt rather comfortable using any of the visualizations (Median over all visualizations: $Mdn = 4$, cf. Fig. 5.6a for details per visualization) and would use the application frequently if they had access to a thermal camera (Median over all visualizations: $Mdn = 3$, cf. Fig. 5.6b for details per visualization).

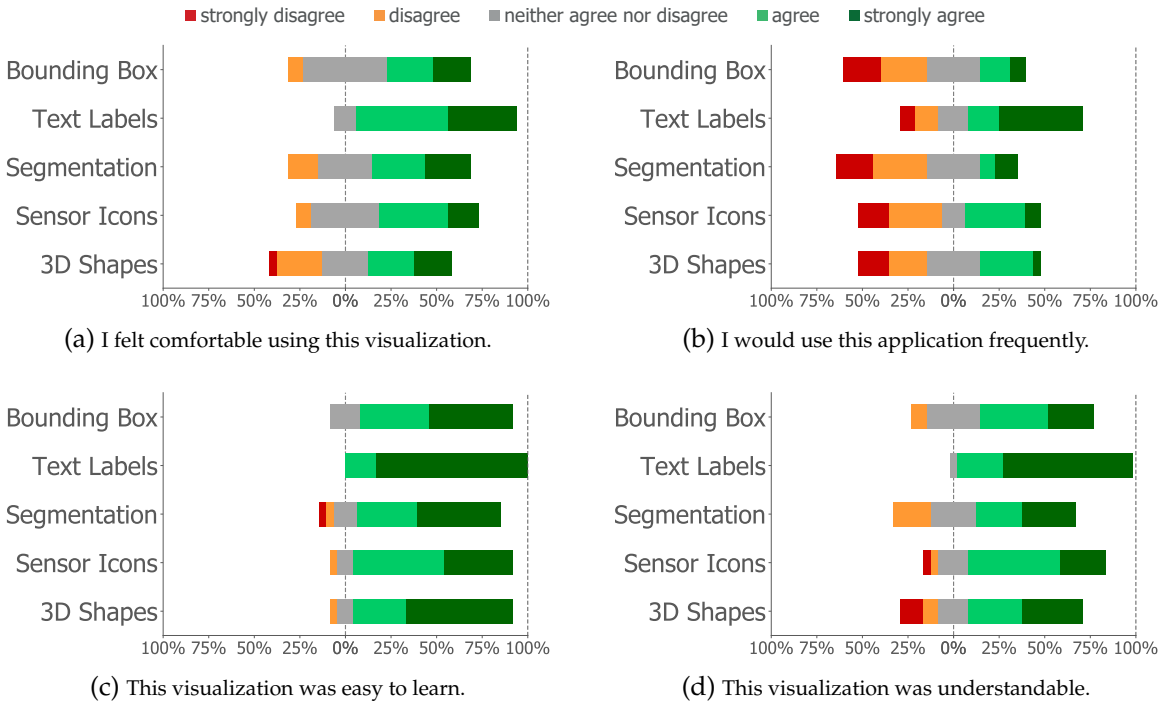
Handsfree: Head-Mounted Display (HMD)

Likewise, using *PriView* in a head-mounted display (HMD) overall received positive feedback. Participants found our prototype usable (SUS $M = 73.85$[9], $SD = 7.52$) while perceiving a rather low cognitive workload ((Raw) NASA-TLX $M = 12.85$[10], $SD = 4.66$). In particular, participants liked that it was easy to use (e.g., P4, P7, P18, P20), and that there was no need to scan the environment manually using their mobile phone (e.g., *"I guess just for convenience it's easier to take off and on a pair of glasses rather than having to scan the room with the phone."*, P2). Participants wearing glasses could well imagine having it integrated with their daily life (P6 and P10).

> **Output Devices.** For *PriView* to be applicable in daily life, it should be easily accessible and ideally be integrated with personal devices. Thus, some participants preferred the smartphone. Yet, this might change as smart glasses become more ubiquitous. In any case, scanning the environment for potential privacy intrusion should be effortless and fast.

[9] a SUS score greater than 68 is considered "above average" [29], see Section 1.3.2

[10] the NASA-TLX workload score ranges from 0 to 100 [90], see Section 1.3.2



(a) I felt comfortable using this visualization.

(b) I would use this application frequently.

(c) This visualization was easy to learn.

(d) This visualization was understandable.

Figure 5.6: Study Part I (using *PriView* in a mobile application): Likert Ratings per visualization for a) comfort, b) frequent use, c) learnability, and d) understandability.

5.5.3 Visualizations

Learnability & Understanding

Overall, our visualizations were understandable as well as easy to learn in both modalities. For the mobile application, participants strongly agreed that the *Text Labels* and *3D Shapes* were easy to learn ($Mdn = 5$). They agreed ($Mdn = 4$) for the other visualizations (cf. Fig. 5.6c). Regarding understanding, they strongly agreed for the *Text Labels* ($Mdn = 5$) and agreed for the rest ($Mdn = 4$, cf. Fig. 5.6d).

As for the second part of the study (using the HMD), we exposed participants to the same visualizations multiple times in various scenes (in counterbalanced order). Overall (i.e., at the end of the study session), participants strongly agreed that all visualizations were easy to learn ($Mdn = 5$), except for the *Floor Markers* ($Mdn = 4$, cf. Fig. 5.7a). Regarding understandability, participants strongly agreed on *Text Labels* and *Bounding Boxes* ($Mdn = 5$, cf. Fig. 5.7b). Looking into more detail at participants' comments, we found that they understood the *Text Labels* immediately:

> *"This is way easier to understand."* (P18)

> *"So this one does give me a bit more comfort in a sense. It tells me that the provider is from this place – because I expect the security camera to be from this place. "* (P9)

Also, the *Bounding Boxes* were mostly clear and easy to understand for participants:

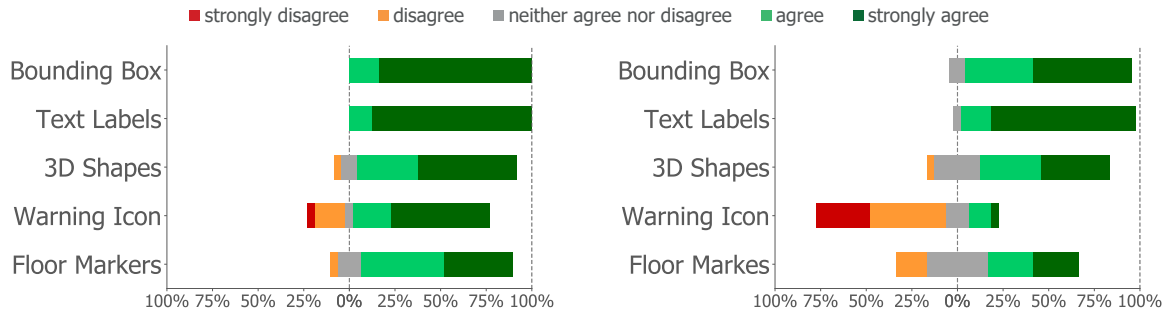
> *"Okay, so now it's again with the red squares. It's very intuitive to use. Usually, when you stand here at the station you actually move forward and maybe around so you can (...) look around and spot them. So in this case it's very practical actually."* (P8)

In contrast, the meaning of the *3D Shapes* and *Floor Markers* sometimes was not clear at first sight and/or only became clear after a while:

> for the *Floor Markers*: *"I think it could be some kind of escape route or direction sign."* (P7)
>
> for the *3D Shapes*: *"As soon as I figured out how it worked, I liked the 3D Shapes."* (P21)
>
> *"There is a cone of light emerging from the fridge. I am not a 100% sure what that is."* (P10)

For the *Warning Icon*, participants often expected more to it, while it was just a static indicator in our current mockups:

> *"I don't know what this is supposed to show me. It's just an exclamation mark."* (P6)
>
> *"There is a red exclamation mark. It stays there (...). It doesn't change, nor change its position."* (P7)



(a) This visualization was easy to learn.

(b) This visualization was understandable.

Figure 5.7: Study Part II (using *PriView* in an HMD in various scenes): Likert Ratings per visualization for a) learnability and b) understandability.

Enhance Understanding. Our results indicate that textual information is immediately easy to understand, while visualizations of tracking spaces might be misleading at first sight. However, the latter transported information that users would like to understand (e.g., where they can stand in a train station without being recorded):

> *"Now the question is where I can stand without being tracked."* (P11)

> *"Yes I like this because now I can see I am in an area where it does not record me that well."* (P19)

Future work should thus investigate in more detail how such visualizations can be made understandable.

Preferred Visualizations

In every part of the study (mobile app and HMD), we asked participants for their preferred visualization, addressing **RQ$_{AW}$2.c**. For the second part (HMD), we additionally asked participants to rank the visualizations from most preferred (rank 1) to least preferred (rank 5) for every scene, resulting in a total of 144 rankings (see Figure 5.8 for an overview of rankings and Appendix B.4 for details on the ranking per scenario).

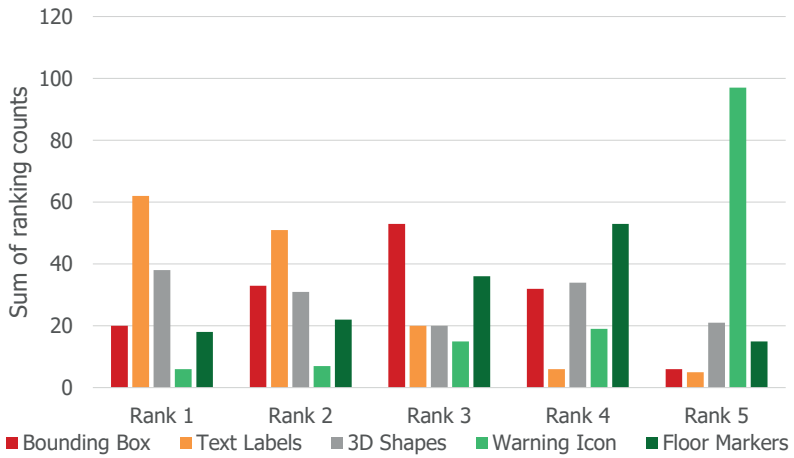


Figure 5.8: Study Part II (using *PriView* in an HMD): Overall ranking of visualizations, i.e. sum of count of rank positions over all scenes. Each of the 5 visualization was ranked in 6 scenes by 24 participants.

Participants mainly preferred the *Text Labels* (ranked first $N = 17$ for the mobile application and $N = 62$ for the HMD), mainly due to the fact that it gave them the highest level of information, i.e. most details on the devices. P19 additionally

valued the arrow within the text labels (HMD) pointing to the concrete devices. However, participants also raised concerns regarding the visibility of the text boxes (i.e., they were transparent in gray which was hard to see in, e.g., the train station scene), text boxes disappearing before having them read completely (for the mobile application, P17), and also the source of information. In addition, many participants did not want this information about their own personal devices to be revealed.

The second most favorite (38 times on rank 1) in the HMD were the *3D Shapes*, again due to their high level of detail in terms of covering the tracking space. However, participants tended to feel visually overloaded with this visualization, especially in places crowded with sensors. They would have preferred to turn them off after having completed inspecting the scene. However, the *3D Shapes* supported participants to even localize out-of-view cameras and the direction in which they are placed, especially in the "way to work" scenario. Furthermore, P23 doubted that the "sharp edges" of the *3D Shapes* are realistic, especially for the audio bubbles. P19 mentioned that environmental noise might crucially influence the tracking space, which was not included in the visualization. Within the mobile application, the *3D Shapes* around the devices were perceived differently by participants. On one hand, participants found them visually appealing:

> *"I really liked them. The bubbles were aesthetically the one that I liked the most."* (P15)

On the other hand, the shapes were perceived as transporting no information (P18), and being *"very intrusive"* (P14), but then again potentially hard to spot for small devices (P14).

The third most favorite (20 times on rank 1 for the HMD) were the *Bounding Boxes*. Participants especially valued these for the fast localization of – especially hidden – devices. However, many participants would have liked the option to then reveal additional information upon having found the framed devices. In the mobile application, the red frames were preferred by 3 participants.

As for the *Floor Markers* (HMD only), participants' had split opinions (18 times on rank 1, 15 on rank 5). Some participants appreciated the shown information, i.e. highlighting areas with potential privacy intrusion. P19 even mentioned the floor markers to be *"suitable for daily life"*, but still raised concerns regarding accuracy.

Lastly, the *Warning Icon* (HMD only) was least preferred by participants (6 times on rank 1, 97 on rank 5). Main reasons for this were the low amount of information (e.g., *"I don't know what this is supposed to show me."*, P6) and the possibility of getting too used to it, i.e. not recognizing it anymore (e.g., *"In the city center, where there are lots of cameras, you probably don't recognize it anymore"*, P19). Participants would however see benefits in combining the warning icon with more detailed information on demand or the icon flashing up on changes they would not be aware of otherwise.

In the mobile application, the *Segmentation* was appreciated for being conspicuous and easy to recognize (e.g., *"It's easier to catch it"*, P13). While the *Sensor Icons* were not preferred by some participants for being too small or unclear (e.g., *"It's hard to really walk very close to the device in order to get the icon. It's so small."*, P22), others suggested iconography as visualizations (e.g., *"Though I would think that having this information, (...) probably easier for me to grasp if it was in some kind of iconography or symbols."*, P14).

> **How to visualize?** Overall, participants liked the visualizations that we suggested. However, they raised two main questions. Firstly, participants would have liked a hint to out-of-view devices before having to scan the environment manually. As an example, in the "way to work" scene, we placed a security camera around the corner from the participants' perspective. This means they could not see text information next to or red frames around it but could recognize the camera's tracking space using the *3D Shapes* or *Floor Markers* (e.g., *"Ah, back there is more yellow. I didn't see this so far."*, P19).
>
> Secondly, participants were questioning if particularly audio recording has such a sharp border as suggested by our visualizations. However, there are probably many factors to this, including not only the devices' specifications but also environmental noise and the volume of users' voice. Moreover, participants were interested in whether data collection would actually affect them. For instance, in the train station scene, we placed passengers on the train recording audio while users were standing outside the train. In the office kitchen scene, P7 would have liked to know whether they can still be overheard by the coffee machine while sitting at the table.

Amount of Information

Generally, participants valued cases in which they got information through *PriView* that they would not have known otherwise. As an example, in the rental apartment scene, where data collection was unexpected to most participants, they generally wished for a higher level of information. For instance, the *Warning Icon* was most of the time providing too little information for participants: participants perceived the conveyed information sometimes as redundant (e.g., in the train station, where participants already expected CCTV to be present) and in other situations as insufficient (e.g., in the rental apartment).

Few participants wished for additional information, e.g. the precise position (P23) and type of sensor (P8, P23), whether it is actually capturing them (P7, P15), as well as more fine-grained device status information, i.e. if it is currently on or recording (P13). P21 suggested to also add the owners of personal devices. P15 and P19 were especially interested in differentiating devices that belong to a public organization

from private ones. Moreover, the desired amount of information might vary over time, e.g., P12 would have preferred to see all available details on first use, but would subsequently be fine with a less detailed visualization, such as the bounding boxes. Lastly, the adequate information level also depends on the number of devices being present according to P21.

> **The right amount of information.** The main question that arises is how to balance the desired level of information with visual overload. Participants recognized that especially if scenes are crowded, visual clutter might overwhelm them (e.g., *"If I imagine, there was hundreds of people on the platform, this would be a huge blue mass."*, P23). However, detailed information about, e.g., tracking spaces was still appreciated. To reduce visual overload, P7 suggested a lower level of information for devices that do not actually capture them (e.g., the smartphone in somebody's pocket).
>
> Moreover, the information should be justified. For instance, in public scenes, we added some device providers as "unknown" in the text labels. This was irritating participants more than actually informing them (e.g., *"There is another one, provider 'unknown'. This is different from the other one. This makes me suspicious."*, P19). In such cases, it might be more meaningful to present reliable information only. To summarize, the right amount of information is highly context-dependent (cf. $\mathbf{RQ_{AW}2.b}$).

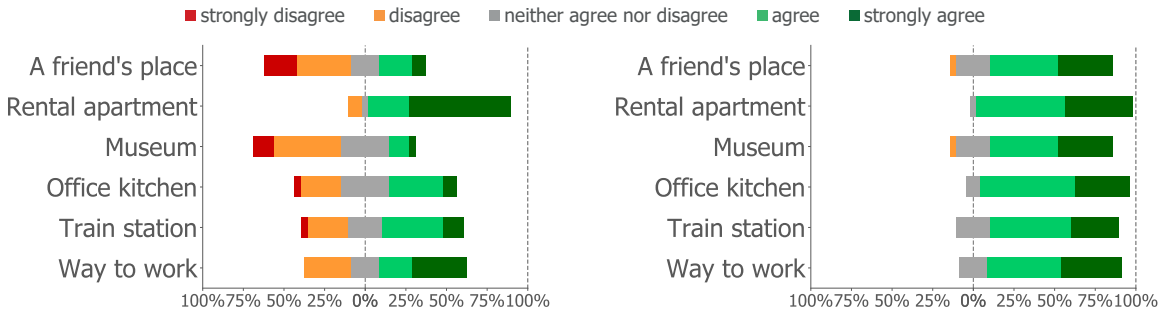
5.5.4 Usefulness and Potential Use Cases

Overall, participants saw benefits in using *PriView* in the scenarios we presented them. However, most participants would not use it in places where the information is redundant (e.g., in a train station or museum, CCTV being present was obvious to them). Other *scenarios* were more convincing to them for the following *purposes*.

Scenarios

From the scenarios we presented in VR to our participants, they strongly agreed to use it frequently in a rental apartment ($Mdn = 5$, cf. Figure 5.9a). They, however, felt comfortable using it in all scenarios ($Mdn = 4$ for all scenes, cf. Figure 5.9b).

Some participants mentioned further scenarios, including unfamiliar and/or public restrooms (P1, P19), changing rooms (P15), and doctors' waiting rooms (P19). Other participants mentioned unspecific locations such as *"outside my home"* (P6), *"places where I don't feel well"* (P4), or *"foreign private spaces"* (P11). P19 even mentioned a rental car as it is *"temporarily private"*.



(a) I would use this application frequently (per scene).

(b) I felt comfortable using this application (per scene).

Figure 5.9: Study Part II (using *PriView* in an HMD in various scenes): Likert Ratings per scene for a) frequent use and b) comfort.

Contextualize *PriView*. There is a myriad of factors that impacts users' privacy concerns (cf. Section 5.2.1) and thus their preference on where to use *PriView*. Our results indicate that places that are considered private beyond users' homes are especially relevant. At the same time, this is where they did not necessarily expect data collection to happen. *PriView* should thus adapt to such cases.

Purposes

The main purpose we imagine *PriView* being used for is supporting privacy by increasing users' awareness. Many participants agreed that this is indeed the case:

> *"In most buildings, cameras are signed, but not in every building. (...) In a law office or when you talk about certain contracts or another example is in the restroom, I don't want a camera to be in the cabin."* (P7)

> *"Maybe if there are meetings where there is some secret information. Then I might check the room first."* (P10)

Furthermore, many other interesting purposes were mentioned, from curiosity and fun to maintenance and search for lost devices. P19 mentioned to apply the concept for safety and warn about dangerous parts in the street. P4 would also check if devices are still on to improve sleep quality. P3 and P19 reversed the museum scene and argued that *PriView* could help thieves not to be recorded.

Why to use *PriView*. Regardless of the specific scenario, *PriView* should not stand in the way of users' primary task. While in some cases, this might be identical with using *PriView* (e.g., for maintenance), in other cases the visualization should stand behind (e.g., in a train station where users are mainly trying to find their way).

However, it remains questionable how to verify users and their purposes to avoid thieves and potential attackers misusing *PriView*.

5.5.5 Interaction Modalities

In our study, the mobile application was following an "on demand" approach (i.e., actively scanning the environment), while the VR mockups from a participants' perspective were "always on", controlled by the experimenter. However, participants generally wished for an opportunity to interact with *PriView* (cf. **RQ_{AW}2.d**). On one hand, many explicit approaches to activate the visualizations were mentioned, including buttons (P2, P10) or gestures (P14). On the other hand, participants also wished for an opportunity to be notified about changes by the system rather than to actively interact. e.g.:

> *"(...), if you leave an untracked area or an area where you turned it off, then (...) the exclamation mark could reappear, and you could click on it for details."*, (P23)

Others emphasized a wish for turning it off (rather than on), e.g.:

> *"Maybe in the museum, just being aware for the first 5 - 10 seconds, and then having the option to switch it off could be useful. Because a museum is not a dangerous environment. I just want to be made aware and then have the personal choice to continue. But I don't want that information to be there 24/7."*, (P22).

P23 would prefer to have control over the level of detail at any time. Moreover, many participants could imagine nested approaches, i.e., having the possibility to reveal more details on demand, e.g.:

> *"I think this [text labels] would be the third level I want to have. I want to be notified by the exclamation mark: 'hey, something is going on'. I want to see where the thing is that's tracking me, and then I would go to this one to actually see."* (P14)

Interacting with *PriView*. When using *PriView*, users should a) not miss out important information, but at the same time b) not be overwhelmed with information they do not need. This raises the question to what extent the system should keep users (not) in control what and when to show.

5.5.6 Privacy: Self vs Others

Participants agreed on the fact that *PriView* could actually help them to protect their privacy by increasing their awareness, answering $\mathbf{RQ_{AW}2.a}$. Some participants explicitly mentioned they would take countermeasures, e.g. unplug devices in a rental apartment or create noise in the office kitchen (P19). While participants were highly interested in the shown information, some explicitly mentioned that they would not want to reveal information about their own personal devices:

> *"To a certain degree, it's redundant and maybe even TMI [too much information], because like it tells me about other people's devices. At the same time, I'm still kind of wondering that – if they have the same features that I do – can they also see my phone and the brand of my phone?"* (P9)

> *"In a train station, I can imagine having this running to see if somebody is recording me. However, this is a bit paradox as I then record others as well."* (P19)

Moreover, participants reacted differently when thinking about others using *PriView* in their vicinity. While some would be comfortable, many would not like *PriView* to be used in their surroundings, especially in their own places, as it might create an atmosphere of mistrust:

> *"If it was at my home, I would not feel comfortable, because I would like my friends or guests to trust me. In a public building, I would maybe use it too, so it would be not that unusual, and it would be okay for me."* (P7)

> *"In my place, if somebody whom I invited is walking in my living room and would be using the app, just per standard protocol, I think that would be rude. I wouldn't mind if someone used it, for example, when they're going to my bathroom, because I mean, there have been cases where people have been recorded in other people's bathrooms. I think as long as the person is using it in a situation or in a moment where [they have] a reasonable expectation of privacy, I would consider it okay. If you're just generally suspecting that I'm recording you in any way, then I would think it's kind of rude because you could have just asked me."* (P19)

"At my place, I would probably feel a little bit insulted, since like for me, it would mean that he's not feeling safe at my place. (...) In public, I think it wouldn't really disturb me." (P21)

How to (not) protect privacy using *PriView*. While all participants were interested in the information provided trough *PriView*, many of them would not like to have their personal devices included and shown in the system. Thus, *PriView* needs to strike a balance which information (not) to reveal, also considering multiple users' privacy needs. Prior work, e.g., suggested considering different types of relationships between device users [78] and to provide usable access control mechanisms [229]. For *PriView*, this eventually means to refrain from including personal devices, to consider users' relationship to the place and device owner as well as potential bystanders being present, or to give users the opportunity to explicitly opt out the fact that their devices are included and shown to others.

5.6 Future Implementations of *PriView*

5.6.1 Information Sources

One prerequisite to employing *PriView* is gathering the respective information to visualize. For our mobile application, we used a training dataset of 1239 photos and computer vision techniques. However, gathering such training data would be costly in terms of time and effort. Another opportunity would require providers to reveal general device information, which might be another limiting factor (cf. [194]). While this information might reveal the device specifications (including tracking space), it might not include the current device status. The latter would then need to be detected on spot using, e.g., a thermal camera. Moreover, such information could also be crowd-sourced (cf. the *IoT Assistant*[11]). However, this again requires contribution by individuals as well as knowledge about devices.

This opens interesting directions for future research. Firstly, how can the respective information be collected to be visualized in *PriView*? Secondly, how can this information be handled in a way that preserves the privacy of device owners, recorded users and bystanders? Thirdly, how to choose the information that is relevant for users in the respective situation?

[11] `https://www.iotprivacy.io/login`, last accessed September 1, 2020

5.6.2 Adapting, Configuring, Contextualizing

In our study, using *PriView* was participants' primary task. However, in most of the settings, this is not necessarily the case (e.g., enjoying a museum exhibition). Thus, many participants wished for more subtle visualizations and/or for a possibility to turn it off to focus on their actual goal. Other wishes for personalizing *PriView* included color (P19) and information (P9, P22) choice.

To summarize, future research should investigate the following questions: how can *PriView* be adapted to users' needs automatically, e.g. based on context? Which options should be given to users to adapt *PriView* to their needs manually? And how would a configuration interface for *PriView* be integrated?

5.7 Summary & Conclusion

In this chapter, we present *PriView*, a concept with which we can visualize potential privacy intrusion in the users' vicinity (by, e.g., audio or video recordings). We explored sample application scenarios and visualizations for *PriView* and implemented two prototypes, namely a mobile application and a head-mounted display showing mockups of various scenes in VR. We found that users generally appreciated the idea of *PriView* and saw interesting use cases, including, but also beyond protecting their privacy. We further found that more detailed visualizations were preferred in most settings, while in other settings subtle indications might be more suitable. We summarize our results in design challenges and point out future opportunities for implementing *PriView*. We hope our exploration to inform further work on privacy visualizations for varying smart environments. Note that while such visualizations can target users' *awareness*, they do not actively call for users' action and provide no means of control over data collection settings. *Enabling control* will be subject to the next part (Part III) of this thesis.

***PriView* can increase awareness.**

The key contributions in this chapter are:

- **Concept:** We present *PriView*: a concept for privacy visualizations that support users not only locating specific devices but also respective areas of data collection. This can help users protect their privacy (by, e.g., avoiding such areas) within (unfamiliar) smart homes and beyond.
- **Artifacts:** We implemented two prototypes of *PriView*. The handheld, mobile application can detect a set of sample smart devices in the environment using real-time object detection running on the phone. An additional pre-trained model can detect devices' state based on the thermal image. The app displayed our sample visualizations on detected devices. The handsfree application (running on a head-mounted display) used a set of VR scenes in which we placed smart devices and our sample visualizations, to simulate using *PriView* in several scenarios within and beyond the home.
- **Method:** In an exploratory study, participants tried both prototypes: the mobile application was used to detect and learn about devices placed in our lab, and to prove technical feasibility; while the VR application was used to immerse participants in the varying scenarios to investigate where and why they would use *PriView*.
- **Empirical Insights:** Participants of our study agreed that *PriView* can support them in protecting their privacy, particularly in unfamiliar contexts. They preferred more details in private settings, while in other settings subtle indications were considered more useful.

The results of this chapter can support the design of visualizations that increase users' awareness of privacy and security implications in various contexts. Such visualizations are independent of device owners or manufacturers but can be employed by third parties.

III

Empowering Control

PART III – EMPOWERING CONTROL

As soon as users are aware of privacy and security risks, we need to enable them to actively take control over privacy and security. Configuring devices securely as well as matching individual privacy needs is thus important. However, existing interfaces are inaccessible or unusable, and/or users are unaware of available options [33–35,57,78,93]. In this regard, we investigate means to enable *device owners* to securely set up their devices and built a mechanism that particularly enables *guests* to configure devices in a (foreign) smart home according to their privacy needs.

- **Chapter 6** targets *device owners* to set up their smart home devices securely as well as privacy preserving. Drawing from the Protection Motivation Theory (PMT), we built nudges that can be included in the device setup procedure to motivate secure configurations. We present the results of a large online experiment, in which we found that high detail nudges led to significantly more secure actions as well as higher protection motivation.
- **Chapter 7** presents *PriKey*, a tangible privacy control mechanism for smart homes, enabling inhabitants as well as *guests* to communicate their privacy preferences. We present the concept, an implementation sample in the form of a tangible key, and the results of an exploratory user study.

.

6

Motivating Inhabitants to Choose Secure Smart Home Configurations

This chapter is based on the following publication:
Sarah Prange, Niklas Thiem, Michael Fröhlich, and Florian Alt. "Secure settings are quick and easy!" – Motivating End-Users to Choose Secure Smart Home Configurations. In *Proceedings of the 2022 International Conference on Advanced Visual Interfaces (AVI 2022).* https://doi.org/10.1145/3531073.3531089

The previous chapters highlighted smart home threats as a growing concern and illustrated means to increase users' awareness. This is a first important step towards protecting the smart home from attacks. Nevertheless, it is also essential to *motivate* users to actively *take action* to mitigate attacks. A promising mitigation strategy is the *secure configuration* of devices.

The setup and configuration of smart home devices are commonly done by end-users rather than by security experts. Yet, lay users might either not be aware of security and privacy issues or not consider themselves knowledgeable enough to

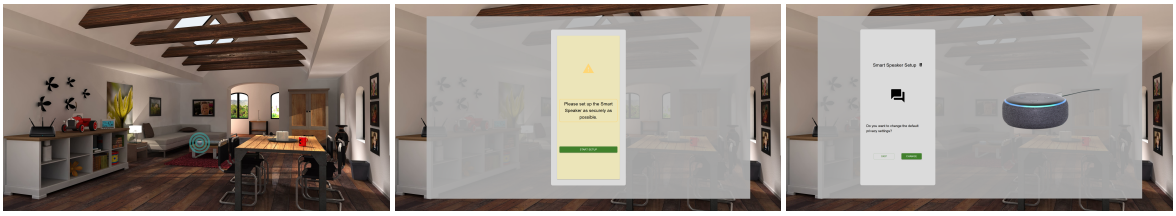


Figure 6.1: In a randomized online experiment ($N = 210$), we simulated a smart home setup procedure (left) to investigate nudges (center) with the aim of fostering secure smart home configurations. For a set of standard smart home devices (e.g., smart speaker, right), users were prompted with both, security-enhancing options and options with no security impact. We found that nudges providing a detailed description of threats and countermeasures led users to choose more secure options.

configure their devices securely and, hence, not be *motivated* to invest time in the secure setup of new devices. This is particularly worrisome, as even a single vulnerable device can substantially increase the attack surface on users' home network. With one's home generally considered to be a "secure place", helping users configure their devices securely can help reclaim parts of this notion.

To address this, it is essential to generate awareness and *motivate users to employ secure configurations* as a means for threat prevention. To this end, we use the Protection Motivation Theory (PMT) [175] as theoretical framework. According to this theory, users' protection motivation is impacted by two major factors: 1) their awareness of threats, including individual consequences (*threat appraisal*), and 2) their confidence to cope with threats and apply adequate countermeasures (*coping appraisal*). These factors can efficiently inform the design of *nudges*, that ultimately lead to more secure decisions in security and privacy contexts [201, 202, 235].

In this chapter, we investigate the question *"How can end-users' motivation to configure their smart home devices (more) securely be increased?"* Based on the PMT, we built two types of nudges for the context of smart home configurations, differing in their levels of detail (see Table 6.1): low (with basic information) and high (with detailed information on threats and countermeasures). In a randomized online experiment ($N = 210$), participants were asked to complete a simulated smart home setup procedure with three typical smart home devices — a router, a light bulb, and a smart speaker – while being exposed to either type of nudge or a control message (Figure 6.1). Users could configure each of the devices by choosing several *secure actions* (e.g., changing the router's default password or updating the light bulb's firmware). In addition to configuration choices, we collected participants' smart home protection motivation with a survey instrument in a pre-/post-experiment assessment.

We found that participants exposed to nudges chose significantly more secure actions compared to a control group with simple instructions. While high detail nudges result in the largest change of user behavior, we found that already low

detail nudges lead to improved behavior. In line with the PMT, we also found that exposure to either type of nudge increased participants' protection motivation along several dimensions. These results show that increasing users' motivation can help them to protect their home by employing secure configurations. In particular, our findings can inform the design of (detailed) nudges for the context of smart homes.

We conclude with a discussion around the design and deployment of PMT-inspired nudges in the context of smart home configurations.

In this chapter, we

1. suggest **nudges** guiding the smart home setup procedure based on the **Protection Motivation Theory (PMT)**,
2. investigated two concrete types of nudges (low/high level of detail) in a randomized online **experiment** ($N = 210$),
3. **discuss** the design and deployment of **PMT-inspired nudges** in the context of smart homes.

6.1 Research Approach

Prior research designed *nudges* to evoke users' protection motivation and, ultimately, lead to more secure and privacy-protecting decisions [109,201,202,235]. The components of the Protection Motivation Theory (PMT, 6.1.1) can efficiently inform the design of such nudges [201,202,211,212].

In this chapter, we employ such *PMT-inspired nudges* in the particularly sensitive context of smart homes, where secure behavior (i.e., device setup) is crucial to be protected against *cyber-physical* attacks [11,95]. Hence, we need to *motivate* users to actively take appropriate countermeasures [189].

6.1.1 Protection Motivation Theory (PMT)

First introduced in 1975, Rogers' Protection Motivation Theory (PMT) describes the impact of fear appeals on human behavior [175,176]. At the core of the PMT are two cognitive processes, influencing people's protection motivation: *Threat Appraisal* and *Coping Appraisal*. The higher individuals perceive these components, the higher their motivation to take action and protect themselves [175]. The threat appraisal comprises users' perceived threat severity and vulnerability, which should

outweigh the perceived maladaptive rewards (i.e., perceived benefits of not changing the own behavior) [70, 176]. For the coping appraisal, users' perceived self- and response efficacy need to outweigh the perceived response cost to increase motivation [57, 70, 176]. Figure 6.2 illustrates this relationship.

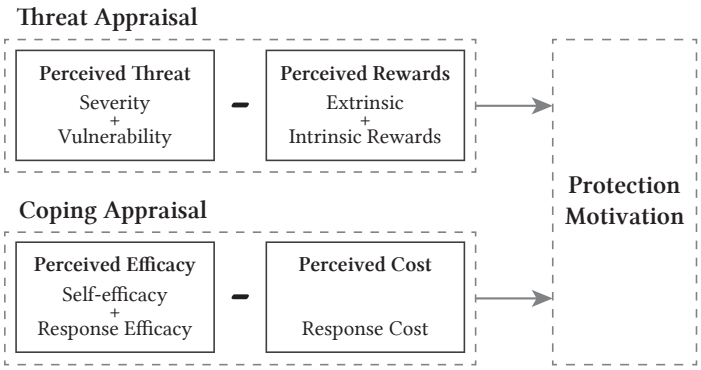


Figure 6.2: Protection Motivation Theory (PMT): Users' protection motivation builds on two cognitive processes: the *Threat Appraisal* and the *Coping Appraisal*. While perceived severity and vulnerability of a threat, as well as perceived efficacy are positive components, perceived maladaptive rewards and perceived cost are negatively impacting users' protection motivation. Figure adapted from [131].

PMT in the Smart Home Context The PMT factors can serve as predictors for consumer behavior related to smart home devices. In particular, users are willing to engage in privacy protection as long as they consider themselves able to (efficacy) and the response cost is not too high [57]. Moreover, users who secure their home networks are significantly impacted by their perceived severity, response efficacy, self-efficacy, and response cost [222].

6.1.2 Nudging in Privacy and Security Contexts

Thaler and Sunstein introduced *nudging* as a means to predictably alter users' behavior by subtly changing the "choice architecture" [127]. This idea has been adopted in a plethora of HCI research in multiple contexts, including personal health, sustainability, privacy and security [31, 70]. In privacy and security contexts, nudging can help users to act according to their preferences and needs [201]. In particular, nudges with clear information can support privacy and security decisions [4, 109] (e.g., creating secure passwords or choosing secure cloud services [235]), and ultimately lead to more secure behaviors. Nudges can be employed, e.g., in the form of warning messages to remind users to navigate securely online and to be aware of possible threats [25, 211]. In the context of smart homes,

nudges displayed in a smartphone interface can influence users' energy-saving behavior [118]. We consider smart homes as a security and privacy critical context and aim to nudge users to more secure and privacy-protecting decisions.

PMT-Inspired Nudges Prior research designed *nudges* inspired by the PMT constructs to evoke users' protection motivation, and to, e.g., resolve misconceptions towards privacy tools [202], and to foster the adoption of security-enhancing technologies (e.g., mobile payment) [201].

6.1.3 Research Questions

In this chapter, we focus on increasing smart home users' motivation to actively protect their homes against threats. In particular, using the Protection Motivation Theory (PMT), we designed nudges to motivate them and help them take more secure decisions during a smart home setup procedure. We derive the following research questions:

RQ_{CO}1.a: How do PMT-inspired nudges impact users' **configuration choices** in the smart home context?

RQ_{CO}1.b: How do PMT-inspired nudges impact users' **protection motivation** in the smart home context?

In the following, we present our concept for PMT-inspired nudges (Section 6.2), and report our online experiment (Section 6.3) and results (Section 6.4). We conclude with implications for the design and deployment of nudges in the smart home context (Section 6.5).

6.2 PMT-Inspired Nudges for Secure Smart Home Configurations

To target users' protection motivation in the context of smart homes, we created two types of text-based nudges, with LOW and HIGH level of detail (see Table 6.1).

Nudges targeting the PMT constructs can be an efficient means to foster secure behavior and the adoption of security-enhancing technologies [201, 202]. Moreover, previous work found the combination of both, threat and coping appraisal, to be more effective than targeting just one dimension [176,211,212]. Hence, we designed

both nudge versions to particularly target users' perceived threat severity and vulnerability (by, e.g., providing concrete examples of risks and consequences), as well as perceived efficacy and response cost (by, e.g., describing necessary steps to employ appropriate countermeasures and estimated time).

For three sample devices, we created LOW DETAIL nudges providing a short and general message, and HIGH DETAIL nudges with longer descriptions. The LOW DETAIL versions are closely adapted from related work [211, 212].

Prior work showed that abstract risks (as shown in the LOW DETAIL version) are often perceived likely, but only moderately severe [80]. At the same time, raising users' risk perception can increase their protection motivation in the context of smart homes [55]. Combining nudges with educational information about *why* users are being nudged can foster active decision-making in cybersecurity [235]. These findings motivate our HIGH DETAIL nudge version. Following Story et al.'s suggestion that nudges should be designed in such a way that they can help users protect from *well-defined* threats [202], we added concrete real-world examples to the HIGH DETAIL versions. We also emphasize the efficacy of the proposed countermeasure [202] by showing concrete steps and estimated time.

In summary, our nudges address the PMT components as follows (cf. Table 6.1):

Low Detail Nudge To target users' *threat appraisal*, this nudge illustrates potential threats (*severity*) and their high likelihood (*vulnerability*) for poorly configured devices. As for the *coping appraisal*, this nudge provides basic instructions to mitigate threats (*self-* and *response efficacy*).

High Detail Nudge In addition to the information from the low detail version, this nudge provides the following details: For *threat appraisal*, it comprises concrete examples for threats (*severity*) and consequences (*vulnerability*) using web articles on cyberattacks towards the respective device. Additionally, we used information about social expectations ("norm nudging" [21]) to indicate the desired behavior and minimize *maladaptive rewards*. For *coping appraisal*, it provides detailed instructions for appropriate countermeasures (*self-* and *response efficacy*) and estimated time (*response cost*).

6.3 Method

In a randomized online experiment ($N = 210$), we tested the effects of our nudge designs (LOW vs HIGH DETAIL) on participants' smart home protection motivation.

	Threat Appraisal	Coping Appraisal
Low Detail	**Smart Speakers are risk-prone:** Poorly configured smart speakers are very likely to be hacked. Potential risks are leakage of personal data and/or financial damage.	**You can easily minimize the risk yourself:** Best practices include e.g. changing the manufacturer's default configurations.
High Detail	**Smart Speakers are risk-prone:** Poorly configured smart speaker devices are likely to be hacked. Potential consequences can be severe for the end-users. Read here what happened to other users: [web links] **But users are active:** Over 77 percent of smart home device owners in your area are actively protecting themselves with proper configuration of their smart speaker.	**You can easily minimize the risks yourself:** Best practices for smart speakers are: • connect to a secure network • review & adjust privacy configurations • change the default wake word **Effort for a secure setup:** The additional time needed for a secure configuration is approximately three minutes.

Table 6.1: Example Nudge Texts for the Smart Speaker: Nudge content for both PMT components, threat and coping appraisal, in the low and high detail version.

6.3.1 Apparatus

To test our hypotheses and measure the impact of nudges on user behavior, we developed a web-based smart home setup simulation using Directus[1], React[2], and Material Design[3] (Figure 6.1). The simulation replicated the standard procedures of smart home setup processes and implemented a storyline covering three common smart home devices and a total of 15 different configuration options. The setup procedures comprised both, security-enhancing configuration options (*Secure Actions*), and options with no direct security impact (*Additional Actions*[4]). Table 6.2 shows an overview. Three smart home devices were simulated in the experiment – a Wi-Fi router, a smart speaker, and a smart light bulb. The devices were selected considering popularity, vulnerability to risks, and options for security measures. The respective setup procedures were derived from real devices. During the simulation, a smartphone app guided participants through several setup steps (Figure 6.3).

Collected Data

During the simulation, we collected multiple data points. We recorded which *secure actions* were taken, the *password strength* chosen, the *time spent* configuring devices, and a pre-/ post-experiment assessment of participants' smart home protection motivation using a questionnaire.

[1] `https://directus.io/`, last accessed June 01, 2021

[2] `https://reactjs.org/`, last accessed June 01, 2021

[3] `https://material.io/design`, last accessed June 01, 2021

[4] Note: some of the *Additional Actions* might have an indirect impact on security that we did not consider in our analysis.

	Secure Actions	Additional Actions
router	change default password create guest network refresh WPA key	change network name change connection type change timezone
smart speaker	adjust privacy settings select segmented Wi-Fi change wake word	register/ login adjust language change timezone
smart bulb	update firmware select segmented Wi-Fi	change device name change timezone

Table 6.2: Configuration Options: Overview of the configuration options for each smart home device in the simulation including both, *Secure Actions* and *Additional Actions*.

Secure Actions Participants could perform several configuration steps for every smart device. To assess their motivation to secure their smart home devices, we recorded how many *Secure Actions* participants performed during the simulation. Table 6.2 provides an overview of the possible configuration options.

Password Strength The configuration of the smart speaker required the creation of a user account. Reflecting participants' motivation to secure their accounts, we tracked the strength of the selected password. Using a popular npm package[5], we assigned passwords numerical categorical values (0 = Too weak, 1 = Weak, 2 = Medium, 3 = Strong). The algorithm considers diversity (lowercase, uppercase, numbers, symbols) as well as length. The strength was calculated locally in participants' browsers and only the final scores were stored.

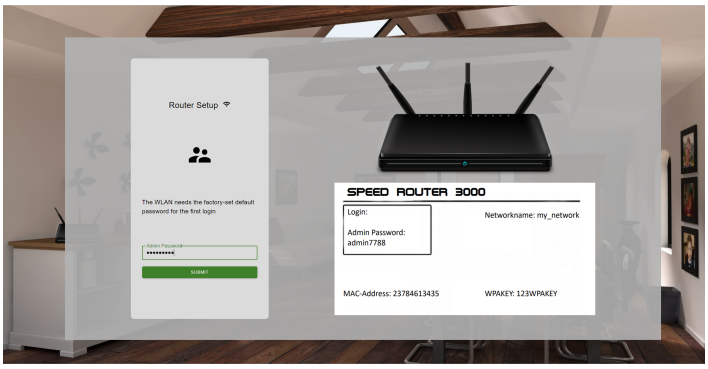


Figure 6.3: Smart Home Configuration Simulation: The web-based application showed a simulated smartphone app (left) and the device under configuration (here: router).

Time We tracked participants' time spent in the simulation as an indicator for motivation. Since different types of nudges were of different length, the time spent reading nudges was excluded, i.e. we recorded the time between "Start Setup" and "Finish Setup".

[5] `https://.npmjs.com/package/check-password-strength`, last accessed June 01, 2021

Smart Home Protection Motivation Grounding our experiment in the Protection-Motivation-Theory (PMT), we hypothesize that nudges would affect participants' motivation to secure their smart devices. To understand how the different PMT constructs would be influenced, we adapted a survey instrument by MacDonell et al. to the smart home context [133]. Answers were collected on a 7-point Likert scale ranging from "completely disagree" to "completely agree", with one item per PMT construct (see Table 6.3).

Question	PMT construct
If my smart home devices was hacked, it would have severe consequences for me.	Severity
There is a high chance that my smart home devices are targets of cyberattacks.	Vulnerability
Leaving the default settings on my smart home devices saves me time and energy.	Maladaptive Intrinsic Rewards
It is common to leave the standard settings set by the manufacturer.	Maladaptive Extrinsic Rewards
I know how to configure my smart home devices securely.	Self-efficacy
Secure configurations of my smart home devices are good protection against cyberattacks.	Response Efficacy
Secure configurations of smart home devices are a great effort for me.	Response Cost

Table 6.3: PMT-Questionnaire: Questions to assess users' smart home protection motivation pre- and post-experiment. Questions adapted from MacDonell et al. [133].

6.3.2 Experimental Design

To investigate the influence of nudges on users' configuration behavior, we implemented a between-subjects design [122] with one independent variable (*type of nudge*) which could take one of three forms: NO nudge (control group), LOW DETAIL nudge, and HIGH DETAIL nudge. Participants were exposed to only one type of nudge throughout the study. Thus, we designed six nudges: one LOW DETAIL and one HIGH DETAIL nudge for each of the three smart home devices (router, smart speaker, smart light bulb). The control group was shown no nudge. Participants were randomly assigned to one of the groups prior to the start of the simulation.

As *dependent variables* we measured the total number of *Secure Actions* participants applied during the simulation, the *time* participants spent for the configuration, and the *password strength* for the smart speaker's account.

6.3.3 Procedure

The experiment was administered online and could be accessed through a web browser using a desktop computer. All data was collected anonymously. The detailed procedure was as follows (see Figure 6.4):

1.) **Scenario Description.** To immerse participants in the scenario, we provided a textual description. They should imagine that they just bought a couple of smart home devices and their task was to now set them up in their home.

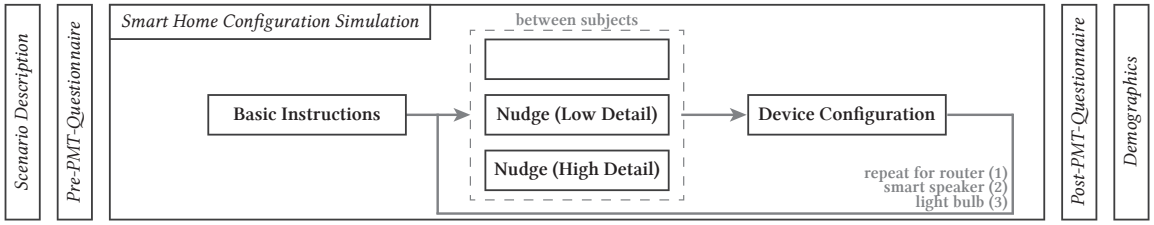


Figure 6.4: Experiment Procedure: Participants (1) were introduced to the scenario, (2) filled the PMT-questionnaire, (3) completed the simulation, (4) filled the PMT-questionnaire, and (5) provided demographics and prior smart home experience.

2.) Pre-PMT-Questionnaire. Participants then filled in the PMT-questionnaire (see Table 6.3) to assess their protection motivation.

3.) Smart Home Configuration Simulation. The setup simulation comprised the configuration of three devices, namely (1) router, (2) smart speaker, and (3) smart light bulb, in this exact order. We assumed this order to align with real-world setup procedures. Before participants could start setting up each device, they were exposed to the treatment of our experiment – they were shown a nudge on the simulated smartphone screen.

4.) Post-PMT-Questionnaire. We again collected participants' protection motivation using the PMT-questionnaire (Table 6.3).

5.) Demographics. We additionally collected demographic information and data on past smart home and cyberattack experiences.

Participants were randomly assigned to one group (control, LOW DETAIL, HIGH DETAIL) and exposed to the same type of nudge throughout the complete simulation. The order of the PMT-questions was randomized to avoid order effects bias.

6.3.4 Participants

We recruited our sample via Prolific[6], an online service specialized on providing a subject pool for research [160]. Participants were required to have a desktop computer and be fluent in English. Our final sample consisted of 210 participants, out of which 115 (55%) were female, 89 (42%) were male, two indicated "other" and four participants preferred not to say. The average age was 25.3 years ($Min = 18$, $Max = 69$, $SD = 11.9$). A total of 117 participants stated to own at least one smart home device and 11 participants reported having experienced cyberattacks. Attacks

[6] `https://prolific.co/`, last accessed September 01, 2021

mainly targeted their social media ($N = 6$), gaming ($N = 1$), or banking ($N = 1$) accounts. Two participants reported attacks towards their devices (one computer, one smartphone), and one reported a phishing attack.

6.3.5 Limitations

Our sample is rather young (mean age 25.3) and based in western countries. Hence, our results may not apply to the general public and to other cultures. We conducted the study online using a simulation. Thus, we can only make limited assumptions about actual behavior as privacy and security preferences may differ from actual behavior (cf. the "privacy paradox" [79]). However, online studies have been shown to be an effective means in HCI research [214].

6.4 Results

This section presents the result of our experiment. Given the between-group design, our sample can be divided into three groups: (1) control group, which saw NO nudge ($N = 70$), (2) LOW DETAIL group, which saw the low detail versions of the nudges ($N = 70$), and (3) HIGH DETAIL group, which saw the high detail versions of the nudges ($N = 70$). All statistical tests are conducted with $\alpha = 0.05$ as threshold for statistical significance. Moreover, with a sufficiently large sample size per group (>30), the central limit theorem allows us to assume a normal distribution for all statistical tests in the following [1].

6.4.1 $RQ_{co}1.a$: Configuration Choices

Addressing $\mathbf{RQ_{CO}1.a}$, we look into users' configuration choices during our simulation. In particular, we analyzed the number of *secure actions*, *time* spent for the configuration, and *password strength*.

Secure Actions

Participants' number of performed secure actions during the simulated setup procedure differs between the three groups (cf. Table 6.4). In particular, participants in the control group performed on average the fewest number of secure actions ($M = 2.51$), followed by participants in the low detail group ($M = 2.93$). Participants in the high detail group performed on average the most secure actions ($M = 3.79$). A Levene's-Test [128] showed significant difference in variance between the groups

Group	Mean	SD	Median	Min	Max
control	2.51	1.45	2	0	6
low detail	2.93	1.62	3	0	7
high detail	3.79	2.21	4	0	7

Table 6.4: The number of *Secure Actions* per treatment group.

$(F(2,207) = 13.019, p < 0.001)$, violating the homogeneous variance assumption required to use ANOVA [53, 65]. Hence, we used Welch's ANOVA, which relaxes the homogeneity of variance assumption [53].

Testing with Welch's ANOVA showed that the number of secure actions taken differed significantly between the groups $(F(2,134.62) = 8.0468, p < 0.001)$. Since Welch's ANOVA only states the existence of a difference, we conducted an additional pair-wise post-hoc analysis between the groups. We used a Games-Howell post-hoc test as it is suited for comparing groups with unequal variances [75, 177]. The analysis revealed a significant difference between the number of secure actions between the HIGH DETAIL and the control group $(p < 0.001)$ and between the HIGH DETAIL and LOW DETAIL group $(p = 0.027)$. The difference between the control group and the LOW DETAIL group was not statistically significant $(p = 0.252)$. Table 6.5 provides an overview of the pairwise comparison.

	control	low detail	high detail
control	–	–	–
low detail	0.252	–	–
high detail	**0.000***	**0.027***	–

Table 6.5: Results of the pairwise comparison of the number of secure actions between groups. P-values marked with a * denote statistically significant differences.

Time

Participants in the high detail group spent on average the most time on device configurations ($M = 3.12$ mins, $SD = 1.36$, $Min = 0.43$ mins, $Max = 7.19$ mins), while participants in the low detail group spent less time on average ($M = 2.90$ mins, $SD = 1.07$, $Min = 0.99$ mins, $Max = 5.88$ mins). Participants in the control group spent on average the least time ($M = 2.73$ mins, $SD = 1.06$, $Min = 0.28$ mins, $Max = 5.20$ mins). A Levene's-Test [128] showed no significant difference in variance between the groups $(F(2,207) = 1.2341, p = 0.293)$. An ANOVA showed no statistical differences between the groups $(F(2,207) = 4.71, p < 0.056)$.

Password Strength

Looking at the average password strength, the descriptive results are less clear. The control group shows the lowest average password strength with a score of 1.32

($SD = 0.92$, $Min = 0$, $Max = 3$), followed by the high detail group with a mean of 1.37 ($SD = 0.98$, $Min = 0$, $Max = 3$). The most secure passwords were entered by participants from the low detail group achieving an average strength of 1.53 ($SD = 0.94$, $Min = 0$, $Max = 3$). A Levene's-Test [128] showed no significant difference in variance between the groups ($F(2,207) = 0.0292, p = 0.971$). We, therefore, used ANOVA. The results showed no statistical differences between the groups ($F(2,207) = 0.083, p = 0.774$).

6.4.2 $RQ_{co}1.b$: Protection Motivation

In addition to participants' configuration choices, we collected participants' smart home protection motivation with a survey in a pre-/post-experiment assessment. After a visual inspection, we conducted a more detailed analysis for each PMT construct. We compared the answers to each item before and after exposure to the treatment during the experiment. We used the Wilcoxon-Signed-Rank-Test to test for statistically significant differences for each treatment group. The results are described in Table 6.6.

In the control group, no statistically significant difference was found in any dimension. For the low detail group, the Wilcoxon-Signed-Rank-Test showed a significant change in perceived intrinsic (-0.58, p=0.0013) and extrinsic maladaptive rewards (-0.31, p=0.0041), as well as self-efficacy (+0.34, p=0.0299) and response efficacy (+0.31, p=0.0172). In simple words, after being exposed to the experiment, participants of the low detail group felt less intrinsic and extrinsic rewards from not changing their behavior. They felt more able to configure their smart home devices securely, and believed that configuring devices would be an effective response.

For the high detail group, the Wilcoxon-Signed-Rank-Test showed a significant change along the following dimensions: vulnerability (+0.55, p=0.0024) increased, intrinsic maladaptive rewards decreased (-0.24, p=0.0052), self-efficacy increased (+0.86, p<0.001), response efficacy increased (+0.68, p<0.001), and response cost decreased (-0.35, p<0.0281). In simple words, after being exposed to the experiment, participants of the high detail group felt it was more likely their devices could be targets of cyberattacks and perceived less intrinsic rewards from not changing their behavior. They felt more able to configure their smart home devices securely, believed that configuring devices would be an effective response, and were less inclined to think that doing so would be a great effort for them. Figure 6.5 shows an overview of participants' answers pre- and post-treatment for the high detail group.

	Pre-Experiment		Post-Experiment		
	Mean	**Median**	**Mean**	**Median**	**p-value**
Severity	5.07	5.50	5.11	5.50	0.7115
Vulnerability	3.76	4.00	3.93	4.00	0.1421
Intrinsic Reward	4.51	5.00	4.50	5.00	0.9597
Extrinsic Reward	5.79	5.00	4.83	5.00	0.9762
Self-Efficacy	4.79	5.00	4.84	5.00	0.7939
Response Efficacy	5.43	6.00	5.57	6.00	0.4402
Response Cost	5.00	5.00	4.81	5.00	0.5192

(a) **NO Nudge** (control group)

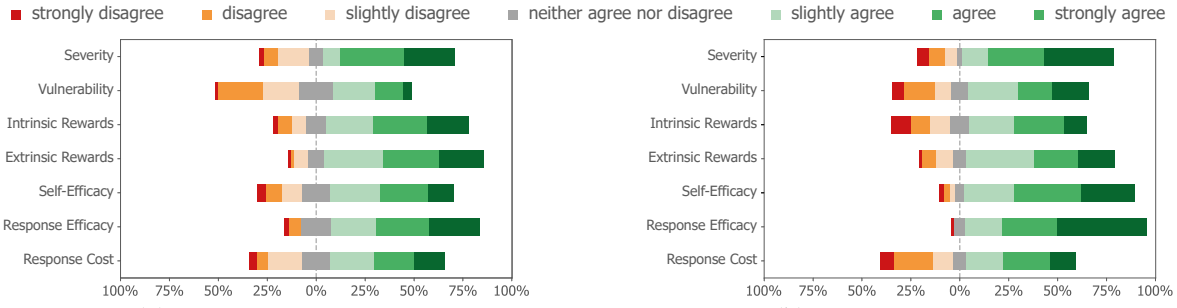
	Pre-Experiment		Post-Experiment		
	Mean	**Median**	**Mean**	**Median**	**p-value**
Severity	5.16	5.00	5.17	5.00	0.8616
Vulnerability	3.96	4.00	4.13	4.50	0.3624
Intrinsic Reward	4.87	5.00	4.29	5.00	**0.0013***
Extrinsic Reward	5.11	5.00	4.80	5.00	**0.0041***
Self-Efficacy	4.99	5.00	5.33	6.00	**0.0299***
Response Efficacy	5.73	6.00	6.04	6.0	**0.0172***
Response Cost	4.43	4.00	4.30	5.00	0.5508

(b) **LOW DETAIL Nudge**

	Pre-Experiment		Post-Experiment		
	Mean	**Median**	**Mean**	**Median**	**p-value**
Severity	5.13	5.00	5.37	6.00	0.1400
Vulnerability	3.94	4.00	4.59	5.00	**0.0024***
Intrinsic Reward	5.13	5.00	4.49	5.00	**0.0052***
Extrinsic Reward	5.41	6.00	5.09	5.00	0.0658
Self-Efficacy	4.73	5.00	5.59	6.00	**0.0000***
Response Efficacy	5.43	6.00	6.09	6.00	**0.0000***
Response Cost	4.69	5.00	4.34	5.00	**0.0281***

(c) **HIGH DETAIL Nudge**

Table 6.6: Comparison of the Pre-/Post-PMT-Questionnaire per Group. The results are as follows: a) no statistically significant differences in the control group (NO nudge); b) significant differences for the intrinsic and extrinsic maladaptive rewards, self-efficacy, and response efficacy dimensions in the LOW DETAIL group; c) significant differences for vulnerability, intrinsic maladaptive rewards, self-efficacy, response efficacy, and response cost in the HIGH DETAIL group.



(a) Pre-PMT Questionnaire (b) Post-PMT Questionnaire

Figure 6.5: Participants' smart home protection motivation in the high detail group before and after the experiment.

6.5 Discussion

We found that both types of nudges resulted in desirable behavior change compared to the control group, with statistically significant changes in the HIGH DETAIL group. In the following, we summarize and discuss these results, including potential future designs and deployments of nudges for the smart home context.

6.5.1 Overview

In line with related work [201,202], we found that PMT-inspired nudges can increase users' protection motivation: the pre- and post-assessment of protection motivation shows changes along all dimensions for participants in the LOW DETAIL as well as the HIGH DETAIL group. In particular, negative components (e.g., response cost) were perceived lower, while positive components (e.g., self-efficacy) were perceived higher after exposure to the nudges.

Looking at our specific context, i.e. configuration of a smart home setup, the descriptive statistics showed increased means in the desired direction along all observed categories in both groups with nudges (low and high detail): more secure actions, longer configuration time, stronger passwords (see Table 6.7). While longer configuration time might seem undesirable, related work showed that such delays are acceptable for users as long as the threat is clear to them [60]. As such, our HIGH DETAIL nudges (including specific risks [80] and educational content [235]) led to statistically significant improvement of the number of secure actions. We speculate that the more concrete descriptions in the high detail version helped participants relate the potential security threats back to themselves, by increasing their perceived vulnerability and severity according to the PMT.

	NO (control group)	LOW DETAIL	HIGH DETAIL
Secure Actions	2.51	2.93	3.79
Time Spent	2.73 mins	2.90 mins	3.12 mins
Password Strength	1.32	1.53	1.37
Severity	+0.04	+0.01	+0.24
Vulnerability	+0.17	+0.17	**+0.55***
Intrinsic Reward	-0.01	**-0.58***	**-0.24***
Extrinsic Reward	-0.04	**-0.31***	-0.32
Self-Efficacy	+0.05	**+0.34***	**+0.86***
Response Efficacy	+0.14	**+0.31***	**+0.68***
Response Cost	-0.19	-0.13	**-0.35***

Table 6.7: Summary of Results: Both, user behavior (secure actions, time spent, password strength) and the pre-/post-experiment change rate of PMT items (measured smart home protection motivation), moved in the desired direction.

To summarize, our results show that designing PMT-inspired nudges resulted in a) changes in user behavior – i.e., more secure configuration actions taken during

the setup procedures, and b) change in users' perception of both, threat and coping appraisal, in the context of smart homes. In the following, we discuss practical implications and map out paths for future research.

6.5.2 Designing Nudges for Smart Homes

In line with related work [176, 201, 202, 211, 212], our results indicate that nudge designs targeting the PMT components (threat and coping appraisal) can be effective in increasing users' protection motivation. Moreover, we found that high detail nudge designs including specific risks [80] and educational content [235] were highly effective in provoking secure actions and decisions. In particular, our high detail nudge version provided graspable details on possible consequences and concrete suggestions for countermeasures, while still being concise with low reading effort. In contrast, the low detail nudge design with rather abstract content was not as effective.

Hence, we argue that future nudge designs should address both, threat and coping appraisal, in sufficiently high detail to achieve high protection motivation. Also, providing concrete examples of possible consequences can help to increase awareness, perceived severity, and vulnerability. By providing a simple estimate of required time and detailing required steps, users' perceived response cost, self- and response-efficacy can be addressed (i.e., increase efficacy while decreasing perceived response cost).

In our web-based simulation, we tested text-based nudge content enhanced with web-links. Future nudge designs could explore other visual designs, as these can enhance users' understanding of privacy- and security-related aspects [112]. Audio-based content could be employed in cases a display is not necessarily available, e.g. for the configuration of smart speakers or door locks. Other nudge designs could use personalized examples [87] or adapt to users' characteristics [92]. For instance, nudges could adapt to users' general protection motivation: for users with low default motivation, higher effort would need to be taken to convince them to adapt secure behaviors. For users who are highly motivated per se, nudges can help them to act according to their privacy and security needs.

Finally, such nudges can be designed for various contexts. Threats are increasingly ubiquitous with advances in technology, and effective threat prevention is required in many contexts. For instance, in private environments such as the home, nudges can help lay users to employ effective threat prevention in their own environment. Nudges could also be employed to help users who visit foreign public or private environments, to increase their awareness and motivation to counteract threats. In office environments, where usually dedicated persons are in charge of employing threat prevention, nudges can help them to protect others.

6.5.3 Deploying Nudges for Smart Homes

In our study, users were exposed to the nudges in a web-based simulation of a stringent smart home setup with a fixed order: router, smart speaker, light bulb. While we assumed this to be in line with a natural smart home configuration storyline, we cannot assume that users employ these devices in that exact order in a similarly short time frame. Rather users might start with one device and only step by step add more. This raises the question as to *when* and *where* to deploy such nudges.

Timing

Timing needs to be considered for nudges to be effective [4]. Information that is presented in a clear way and in time (i.e., when users actually make a decision), can foster privacy-protecting behavior [109].

In the smart home context, nudges might be employed during a device's *setup procedure* (one time). Another opportunity is to employ nudges on a regular basis, e.g., every time users *interact with a device*. In these cases, users could be nudged to adjust security and privacy settings or perform new secure actions such as updating the firmware. Lastly, nudges could support users recovering from threats. Supposing the smart home system could recognize threats automatically, nudges could come up to help eliminate the cause as far as possible (by, e.g., fostering firmware updates or changing passwords).

Modality

Another essential question is where to employ the nudges, and who is responsible to do so. First and foremost, nudges can be employed with the actual device or respective companion application, and, hence, be directly included in the device's setup procedure. However, this relies on the cooperation of manufacturers and/or legal regulations. In case this is not available, nudges can still be employed by third parties in the form of, e.g., mobile applications [4]. For instance, our nudges could be employed on users' personal devices (e.g., smartphones) as a helper application, that users could consult when needed. Such an application could, however, also act proactively. For instance, it could detect new devices in the ecosystem, and provide help for the configuration. A more sophisticated version of such an application could detect moments in which users would be free to take time for their device configurations (e.g., if a smartphone or smartwatch would detect users being idle). As another modality, nudges could be displayed in augmented reality glasses to provide in-situ guidance, or on devices within the home that provide displays.

6.6 Summary & Conclusion

In this chapter, we present nudges as a means to increase users' motivation to employ effective threat prevention (i.e., secure configurations) in smart homes. In particular, we present two nudge designs, with low and high level of detail, targeting the components of the Protection Motivation Theory (PMT). Our online experiment, which simulated a smart home setup procedure, showed that participants employed significantly more secure configurations when being provided with detailed nudges. In particular, with nudge content targeting the threat as well as the coping appraisal, we could confirm prior work and successfully applied the PMT in the sensitive context of smart homes. While our work can help to increase threat awareness in general, it can also support the design of means to increase users' motivation to actively take countermeasures. In particular, we suggest including concrete and concise details on vulnerability and consequences, as well as required steps to employ countermeasures to successfully increase users' protection motivation in smart homes. However, device configuration is usually in the hand of the device owner and, hence, not accessible for other roles such as *guests*. We argue that this target group should likewise be enabled to actively take control over privacy and security settings. We suggest a respective mechanism in Chapter 7.

Detailed nudges can foster secure configurations.

The key contributions in this chapter are:

- **Concept:** We present two nudge designs based on the Protection Motivation Theory (PMT) with low and high level of detail, respectively. These nudges target the secure and privacy-preserving configuration of smart home devices.
- **Artifacts:** We implemented a web-simulation for a large-scale remote experiment using Directus and React. Users could access the simulation via their browser and were randomly assigned to one study condition. During the simulation, users would configure a set of standard smart home devices using mock interfaces, while being exposed to either (or no) type of nudge.
- **Method:** Using the web simulation, we conducted a large remote study ($N = 210$).
- **Empirical Insights:** We found that detailed nudges targeting both, threat and coping appraisal, led users to significantly more secure configurations of devices.

While our work could support manufacturers to improve guidance in setup procedures of smart home devices, it could also be employed by third parties to support users securing their "castles". Moreover, such nudges could also foster secure and privacy-preserving configurations beyond the smart home context, e.g. for devices in offices.

7

PriKey– Enabling Privacy Control for Visitors

This chapter is based on the following publication:
Sarah Delgado Rodriguez, **Sarah Prange**, Christina Vergara Ossenberg, Markus Henkel, Florian Alt, and Karola Marky. *PriKey* – Investigating Tangible Privacy Control for Smart Home Inhabitants and Visitors. In *Nordic Conference on Human-Computer Interaction (NordiCHI '22)*. https://doi.org/10.1145/3546155.3546640

In the previous chapter, we showed how to motivate end-users to control and configure their devices in a secure and privacy-protecting manner, which is absolutely necessary for threat prevention. However, guests cannot easily manipulate respective device settings and, hence, their privacy and security is put at risk by smart devices and sensors in their surroundings collecting data about them [43,78,93].

At the same time, the design of privacy mechanisms that a) scale to smart home settings with potentially high numbers of devices and sensors, and b) address smart home inhabitants and visitors guests is challenging (see Section 2.4).

Figure 7.1: In this chapter, we present *PriKey*, a tangible smart home privacy mechanism that enables *inhabitants*, but particularly also *guests* to communicate and execute their privacy choices. It groups privacy choices by sensor type (video, audio, and presence sensing) and room (e.g., kitchen), and is hence more scalable and reduces workload compared to mechanisms that target single devices. **© Sarah Delgado Rodriguez**

While related work suggested software-based privacy mechanisms addressing multiple user types [7, 72, 77, 96, 147], such mechanisms are rarely adopted. Potential reasons for this are mechanisms being too complex, non-intuitive, non-engaging, or suffering from a lack of trust, especially among guests or less tech-savvy individuals. To address these challenges, prior work suggested *tangible privacy mechanisms* [7, 147], referring to mechanisms that enable individuals to manipulate privacy-related settings through direct and tangible interactions. However, such mechanisms have rarely come beyond a conceptual basis, or do not target more than one specific device or sensor (e.g., jamming (hidden) microphones in users' surroundings [37]).

To close this gap, we suggest *PriKey* as a concept for tangible privacy mechanisms. *PriKey reduces complexity* as it groups privacy settings by sensor type and room, rather than by single devices. Moreover, *PriKey* does not only target smart home inhabitants but more importantly also *guests*. In particular, we introduce the concept and our Wizard-of-Oz prototype. We employed the prototype in a remote user study ($N = 16$) in which we investigated inhabitants' and guests' perception of *PriKey*, and how it addresses their individual needs. We found that *PriKey* enabled users to control sensors in the environment according to their privacy needs, while being intuitive, easy to use, and engaging. Guests especially appreciated *PriKey* in *unfamiliar* environments. Based on our results, we discuss open questions for the design of smart home privacy mechanisms that (also) target guests.

In this chapter, we

1. conceptualize and implement ***PriKey* – a tangible privacy mechanism** that reduces complexity by grouping sensor types and rooms,
2. present the results of our **exploratory study** in which we investigated the usability, perceived trustworthiness, and hedonic quality of *PriKey*,
3. **discuss open questions** and challenges for the design of future smart home privacy mechanisms for visitors.

7.1 Research Approach

Smart home devices collect data about all persons in range, including *guests* [43, 62, 135, 191]. Hence, there is a need for privacy mechanisms that support all involved users to communicate and execute their privacy choices. With *PriKey*, we aim at equalizing power imbalances between primary users and other individuals, including more experienced, tech-savvy, or risk-aware users and other affected individuals. *PriKey* provides all involved individuals with equal means to become aware of privacy intrusions and enforce personal privacy choices in an accessible, easy-to-use and *tangible* manner.

7.1.1 Tangible Privacy

With *tangibles*, digital data can be manipulated using physical objects [173]. As such, they offer a number of advantages over software-based solutions, especially when it comes to the implementation of privacy controls. In particular, *tangible privacy mechanisms* can provide enhanced usability, reduced complexity, and social compatibility, also for less tech-savvy users [144]. Moreover, such mechanisms can communicate state and capabilities of smart home devices, and support their configuration [7]. According to a framework suggested by Mehta et al., tangible privacy mechanisms should be a) *embodied* in daily life objects; b) *direct* by providing intuitive action and feedback; c) *ready-to-hand*; and d) *customizable* for different contexts. Prior work suggested tangible privacy mechanisms targeting specific types of sensors such as armbands that give vibration feedback on potential location tracking and can be used to deactivate it [145] or that jam microphones in the users' vicinity [37], and a hat to mute the microphone of a smart speaker by covering it [206].

7.1.2 Research Questions

This chapter is guided by the following research questions:

RQ_{CO}2.a: How would users **adopt** privacy control as enabled by *PriKey*?

RQ_{CO}2.b: How does *PriKey* account for **individual privacy needs**?

To address these research questions, we first set out by describing the *PriKey* concept and its opportunities (Section 7.2). We then present our tangible implementation sample (Section 7.3), a first tangible wizard-of-oz prototype, and its evaluation in an exploratory user study (Section 7.4). We specifically explored the usability, perceived trustworthiness and hedonic quality of *PriKey*. We discuss our results in Section 7.5 and conclude the chapter with discussing open questions for the design of future privacy mechanisms for visitors (Section 7.6).

7.2 The *PriKey* Concept

In the following, we illustrate basic requirements and resulting design considerations for *PriKey*.

7.2.1 Device-Independent Configuration

We deliberately did not want to restrict *PriKey* to certain devices or sensors as this is a limitation of existing mechanisms. Instead, *PriKey* should be applicable to various *types* of smart home devices that might comprise *diverging* sensors. Hence, we analyzed the capability – in particular: built-in sensors – of devices on the top 50 smart home bestseller list on Amazon[1]. Based on this analysis, we chose *microphones* (14 devices), *cameras* (10 devices), and *presence* sensors (9 devices) as sensors that should be controllable through *PriKey*.

7.2.2 Reduced Complexity

PriKey should be applicable to multi-device environments without overwhelming users. For mechanisms that allow controlling each and every device independently, the amount of information and privacy decisions to make increases rapidly with

[1] top 50 bestsellers in the category "smart home" on `https://www.amazon.de/`, as of April 13, 2021

the number of devices. Hence, we limit *PriKey*'s control functionality to devices in range of individuals, as these carry sensors posing an actual current privacy threat. Moreover, instead of enabling control on a per-device basis, we group *PriKey*'s control options by *type of sensor*. As such, users can decide to accept or deny nearby *audio*, *video*, or *presence* recordings independently or turn *all off*. Within smart home scenarios, we define "nearby" as the *room* users are currently in. With this approach, *PriKey* is less complex and more direct than, e.g., a smartphone application where users would need to unlock their personal device, install/open a specific application, search for specific devices, and then change the respective settings.

7.2.3 Tangible Interactions

With tangible interactions, control of sensor states and communication of data is *direct*, *integrated*, and *meaningful* [213], which is the ideal basis for privacy control functionalities [146, 147]. Tangibility can help to make the abstract concept of privacy graspable, directly manipulable, and, hence, can support users' mental models and reduce cognitive load. To address this, *PriKey* offers dedicated hardware controls (switches and buttons) to explicitly allow or deny single sensor types or any data collection in range.

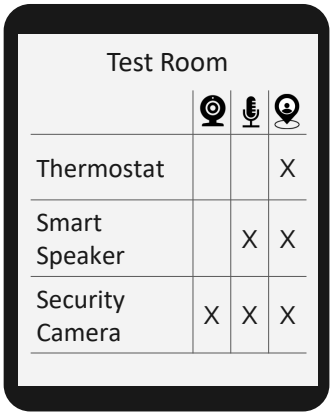
7.2.4 Enabling Control for Various Roles

While data collection by smart home devices affects all individuals in range, not all of them might have access to and/or be allowed to manipulate respective settings. Thus, *PriKey* should enable control for users regardless of their role within the smart home scenario. This includes *primary users* (device owners), *co-inhabitants*, and *visitors* in familiar or unfamiliar environments. Hence, we designed *PriKey* to enable control for users who might not have access to device configuration options due to physical, technological or social limitations.

7.3 Implementation Sample

Following a modular approach, our Wizard-of-Oz implementation comprises two parts: 1) the *PriKey*-tangible (Figure 7.2a) that allows to directly execute privacy decisions and provides immediate feedback visualizing the effect on nearby sensors; 2) the *PriKey*-station (Figure 7.2b) that provides detailed information about devices in the current room, built-in sensors and their states. While the tangible is in users' hands, we imagine the station to be permanently located near the entrance of a room, providing transparent information on demand.

(a) The *PriKey*-tangible. The configuration states are: video recordings accepted, others denied (left), and "all off", which denies all data collection by nearby sensors (right).



(b) Mockup of the *PriKey*-station for a "test room" with three devices ("X" indicates the respective sensor being built-in the device).

Figure 7.2: Wizard-of-Oz Implementation of *PriKey* comprising two components: a) the *PriKey*-tangible and b) the *PriKey*-station. **© Sarah Delgado Rodriguez**

7.3.1 *PriKey*-Tangible

We designed our *PriKey*-tangible to match the shape of a key, as we assumed this metaphor to engage users in protecting their privacy, and to also help them form a mental model of its functionality (Figure 7.2a). As suggested by Mehta et al. [146], the privacy-related interactions with the *PriKey*-tangible are based on force and space. Hence, we used the *key's teeth* as sliders with mild resistance to control the data collection by respective sensors in nearby devices. Furthermore, the tangible also provides attribute-related feedback [146] on current states of the different *sensor types* (indicated with simple icons) in the form of *green Light Emitting Diodes (LEDs)* (i.e., dark/off vs bright/on). The *"All off"*-button shines in *red* when activated and denies any data collection of all nearby sensors. We made sure that our tangible is lightweight, compact, and robust. It includes an ATtiny 84a[2] to control its interactive components and is supplied by a 3 volt CR2032 coin cell battery.

7.3.2 *PriKey*-Station

To not only enable control, but also increase awareness and transparency in the first place, we complemented our implementation with the *PriKey*-station. The station could be realized as a medium-sized touch screen display located at the entrance of every room within the smart home (see Figure 7.2b for a mockup). It should list all devices installed in the current room, included sensors from the respective

[2] `https://www.microchip.com/wwwproducts/en/ATTINY84A`, last accessed September 06, 2021

group, and the current sensor states. We envision that the station would be the central control component of *PriKey*, meaning that it is able to recognize devices and *PriKey*-tangibles in the rooms, and to take actions as communicated through the tangible. As such, it should be able to execute the deactivation of single sensor types (by, e.g., jamming microphone signals).

7.4 Exploratory User Study

Using our implementation sample, we conducted an exploratory user study to investigate the adoption and perception of *PriKey* among users in various roles, particularly *visitors*. Participants tried out our *PriKey* prototype and should imagine using it in various scenarios.

7.4.1 Smart Home Scenarios

We used four scenarios covering different roles: 1) *primary user* and 2) *co-inhabitant* in a shared flat; and 3) *visitor in familiar environments* (visiting a friend in their smart home) and 4) *visitor in unfamiliar environments* (in a rental apartment). Most scenarios assumed participants being alone in the smart home, except for the *familiar environment* (scenario 4), where the friend would be present with them (see Appendix C.1 for full scenario descriptions).

Rooms/Tasks

In every scenario, we covered four *rooms* of a typical apartment, in which participants would have certain main *tasks*. Tasks slightly differed depending on the participant being alone or a friend being present (scenario "visitor in familiar environment"): 1) talking to a friend (over the phone when alone) in the *living room*, 2) going to the *bathroom*, 3) cooking and having dinner (together) in the *kitchen*, and 4) using a laptop in the (friend's) *bedroom* to look at photos of a (shared) memory.

Smart Home Devices

Every room comprised a sample of smart home devices that we consider representative. We chose these based on a current bestseller list (cf. Section 7.2.1) and rated them according to their *privacy intrusiveness*. Our idea was that *additional* sensors (of other types) included in a device increase its privacy intrusiveness. As such, we did not directly compare privacy risks of different sensor types, which ensures the validity of our scale regardless of single sensor's particular risks. We distributed devices equally across the rooms, i.e., every room contains a device of each privacy intrusiveness level (Table 7.1 provides an overview).

Sensors	Possible Devices	Living Room	Bathroom	Kitchen	Bedroom
	Thermostat, Universal Remote Control, Scale, Door Lock	Door Lock	Scale	Thermostat	Universal Remote Control
	Smart Speaker, Sleep Meter, Decoration/Light	Smart Speaker	Decoration/ Light	Smart Speaker	Sleep Meter
	Security Camera, Smart Display	Security Camera	Smart Display	Security Camera	Smart Display

Table 7.1: Sample of Smart Home Devices: According to our privacy intrusiveness scale (first column), we equally distributed devices across the rooms (last columns).

7.4.2 Apparatus

For the study sessions, we used three major components: 1) the *PriKey*-tangible to enable actual input and give (simulated) feedback using its LEDs (physically sent to participants); 2) mockups of the *PriKey* station; and 3) a visualization of a typical flat layout with living room, bathroom, kitchen, and bedroom. The mockups and visualization were included in a *click-prototype* used by the experimenter to guide participants through the smart home scenarios. The click-prototype was realized using Microsoft PowerPoint and its animation features (see Figure 7.3). In every scenario, participants would communicate their privacy choices using the *PriKey*-tangible, and the experimenter would adjust the station mockup accordingly to provide (simulated) detailed feedback.

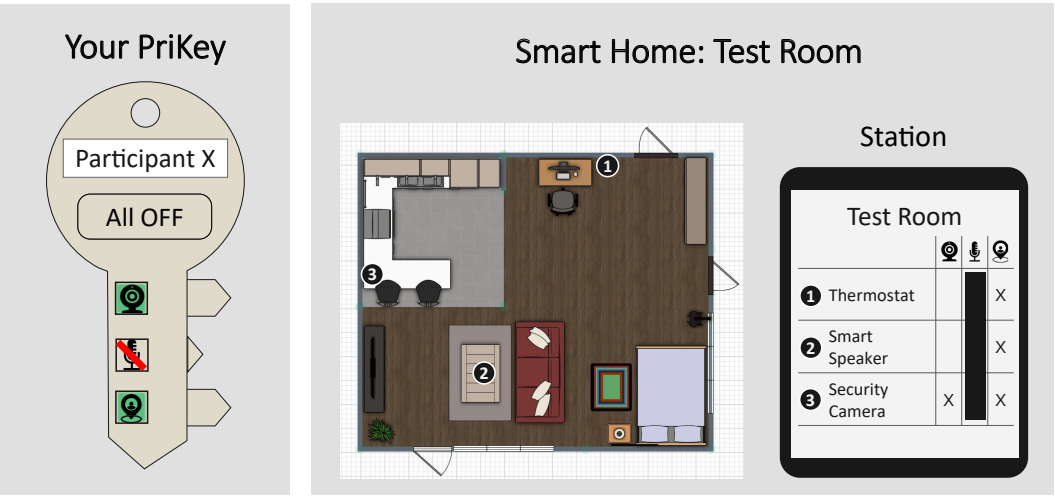


Figure 7.3: Click-Prototype for the Smart Home Simulation: The simulation shows the current state of *PriKey* (left) as well as the current room of the scenario, including the station (right). The experimenter can adjust this visualization as participants interact with their *PriKey*.
© Sarah Delgado Rodriguez

7.4.3 Study Procedure

We conducted the study online using Zoom. Participants received their personal *PriKey*-tangible via postal mail prior to the study session. A session took 60 minutes and comprised four phases (see Figure 7.4 for an overview):

1.) **Introductory Presentation.** After welcoming participants and gathering their consent, we started with an introductory presentation on the general topic of smart homes. We assessed participants' prior expertise and created a common knowledge base for the remainder of the study.
2.) ***PriKey* Trial.** We then guided participants through an exploration of *PriKey*. In particular, we asked them to interact with all functionality while thinking aloud. We also asked for their opinions regarding both components, the tangible and the station.
3.) **Smart Home Scenarios.** Next, we presented every participant with two scenarios (cf. Section 7.4.1). In particular, we randomly assigned participants to be either *visitor* or *inhabitant*. As a consequence, participants either conducted both inhabitant scenarios (i.e., primary user and co-inhabitant) or visitor scenarios (i.e., in familiar and unfamiliar environments) in counterbalanced order, respectively. To create a consistent storyline, we did not counterbalance the order of the tasks (rooms) within the scenarios.
4.) **Final Questionnaire & Interview.** Lastly, participants filled the SUS [29], the Raw-TLX [90, 91] and the HCTS [85] to assess the usability and trustworthiness of *PriKey*. We complemented the session with a semi-structured interview, where we asked for participants' opinions towards our concept and implementation sample, also in comparison to an equivalent smartphone application. Lastly, participants provided demographics and filled the IUIPC scale [134] to assess general privacy concerns (cf. Section 1.3.2 for details on scales).

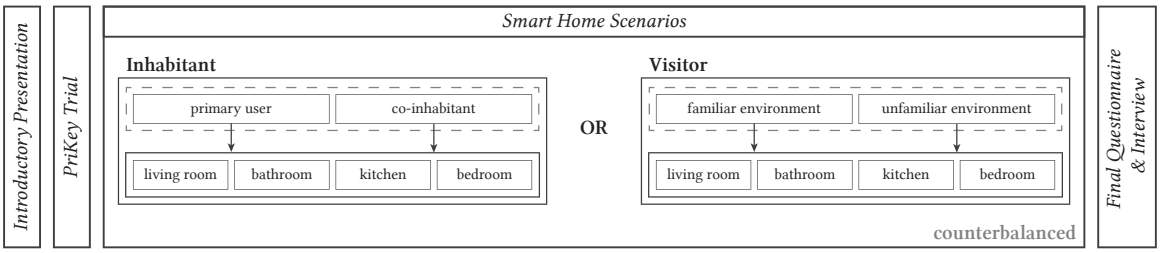


Figure 7.4: Exploratory Study Procedure: Our exploratory study comprised three parts: 1) introductory presentation, 2) *PriKey* trial, 3) two smart home scenarios per participant in one of the roles (*inhabitant* or *visitor*) with four rooms (tasks) each, 4) final questionnaire and interview.

7.4.4 Recruitment

We recruited 16 participants via social networks and a university mailing list. We sent every participant a *PriKey*-tangible prior to the actual session. A session lasted around 60 minutes and took place online via Zoom. Participants were compensated with a 15 € voucher or study credits.

7.4.5 Participants

Participants were 20 to 66 years old ($mean = 33.2$, $sd = 17.2$), half (8) identified as male and half as female. Most (11) participants were university students, two retired, two employed, and one self-employed. Regarding their living situation, six participants reported living with their parents and siblings, four with their partner and children, three alone, and three lived in a shared flat (see Table C.1 in Appendix C.2 for details).

Prior Smart Home Experience

Most participants reported having prior experience with smart home devices. In particular, seven participants owned or previously owned a smart home device, and eleven participants reported having used such devices before. Five participants never used a smart home device before.

We also asked participants to define their understanding of smart homes. Most ($N = 14$) participants mentioned the control of other devices within the home, e.g. remotely ($N = 7$) or via a smartphone app ($N = 12$). According to their understanding, this technology would support users ($N = 5$), by, e.g., intelligent automation ($N = 4$). As concrete sample devices, participants frequently mentioned smart speakers ($N = 11$), devices for energy management or home automation (e.g., plugs, thermostats, and lights, $N = 11$), or entertainment systems (e.g., smart TVs or streaming sticks, $N = 5$). Some also knew about smart surveillance technology (e.g., cameras, door locks, or window sensors, $N = 5$) or health care gadgets (e.g., scale, $N = 1$).

General Privacy Concerns

We also assessed participants' general privacy concerns using the IUIPC scale [134]. In particular, participants expressed a strong wish for *Control* over their data online ($M = 6.19$, $SD = 0.74$, $Mdn = 6.17$, and high concerns regarding the *Collection* of their data ($M = 6.29$, $SD = 1.02$, $Mdn = 6.67$). Participants, however, expressed varying *Awareness* of potential privacy risks ($M = 6.29$, $SD = 1.02$, $Mdn = 6.67$).

We complemented our assessment of privacy concerns within the specific context of smart homes during the interviews. We found that most ($N = 13$) participants were actually *concerned* in this context, e.g.:

> *"Personally, I do not mind so much to disclose information. But when it really is about (...) one's own home, it (...) is a bit different. So, I don't mind giving out my address (...), but if you record or [create] audio [recordings] in (...) my home, then it is different."* (P4)

Also, participants reported feeling *observed* ($N = 8$) and were worried about *unauthorized parties* accessing their personal data ($N = 4$). Some also felt *uninformed* ($N = 4$) regarding privacy risks coming with smart devices or expressed *mistrust* towards device providers ($N = 4$):

> *"(...) once something is on the internet, it usually stays on the internet, even if you (...) delete it, it is still there somewhere. And [a smart home device] uses a cloud, which means that the (...) [data is stored] somewhere, and (...) there are security gaps where people might be able to access it. Or maybe the company that (...) [provides the cloud services] is not as trustworthy as you thought and sells the data."* (P4)

Some participants stated not having purchased such technology in the first place or actively removed installed devices due to privacy concerns ($N = 6$). However, participants also indicated that privacy concerns related to smart home technology might be highly individual ($N = 7$).

7.4.6 Data Analysis

We transcribed all recordings into written form and applied thematic analysis [27] to the transcripts. First, two researchers familiarized themselves independently with the whole dataset. Next, they conducted open coding – one researcher on all transcripts, the other on half of the transcripts – to establish an initial codebook. Then, the two researchers met, discussed their codes, and agreed on a codebook that was used for the final round of coding. Questions, new codes and disagreements were directly solved by discussion during this process. Hence, we do not report measures of inter-rater agreement due to the exploratory focus of our study [141]. The final codebook can be found in Appendix C.3.

7.4.7 Limitations

Our sample is skewed towards young students (mean age 33.2 years). However, we believe this age group to be among the early adopters of smart home technology

in Germany [196]. In our study, participants used *PriKey* for the first time and only during this one session. Hence, we cannot make assumptions about the long-term usage and adoption of *PriKey*. Moreover, *PriKey* might be implemented in different ways beyond our sample, which remains subject to future work.

7.5 Results

We now summarize and discuss the findings of our study. While some results are highly related to our implementation sample of *PriKey*, we will also highlight overarching opinions towards our concept.

7.5.1 $RQ_{co}2.a$: Adoption of *PriKey*

Overall, *PriKey* received positive feedback in our study. In particular, *PriKey*'s usability was rated as *excellent* according to the SUS scale with a score of 87.66 ($Min = 70$, $Max = 100$, $SD = 7.72$, $Mdn = 87.5$) [18, 29] and using *PriKey* came with *very low* cognitive workload according to the Raw-TLX scores ($M = 24.17$, $Min = 10.0$, $Max = 44.17$, $SD = 8.04$, $Mdn = 23.75$) [83, 90].

Participants valued our concept. They found privacy protection important ($N = 14$), and highlighted *PriKey* as a means to *execute control* over their own privacy ($N = 14$) as well as to increase privacy *awareness* ($N = 7$). Many participants emphasized that *PriKey* empowers smart home *visitors* ($N = 8$) to employ personal privacy choices:

> *(...) even if the person I am visiting (...) informs me about it, there is bound to be something – even without intention – that gets forgotten (...). And I find it very pleasant when I can simply take care of it myself.* (P2)

Participants also appreciated the tangible form factor as being intuitive ($N = 12$), fun or interesting ($N = 9$), and also liked the key metaphor ($N = 5$):

> *"(...) it symbolizes privacy because [it is] the key, so to speak, to your own privacy. And you can decide for yourself how much you want to reveal or not."* (P4)

Trustworthiness

According to the HCTS scale, participants considered *PriKey* as rather *trustworthy* with an overall average score of 50.29 ($Min = 41$, $Max = 58$, $SD = 5.09$, $Mdn = 52$). Looking at the detailed subscales, the *perceived risk* of using *PriKey* was assessed with 1.77 on average ($SD = 1.02$, $Mdn = 1$); *PriKey*'s *benevolence* with

4.18 ($SD = 0.96$, $Mdn = 4$); *PriKey*'s *competence* with 4.42 ($SD = 0.79$, $Mdn = 5$); and participants' *trust* in *PriKey* with 4.06 ($SD = 0.84$, $Mdn = 4$). Two participants even stated to trust *PriKey* more than a comparable smartphone application:

> *"(...) it seems very much as if no one could tinker with your system. It seems very external."* (P9)

Only few ($N = 5$) participants stated to *mistrust PriKey*:

> *"(...) it is also a matter of trust whether what I configure there actually happens. (...) I can't confirm it (...)."* (P16)

Use Cases

Participants stated they would use *PriKey* to protect their privacy in various environments ($N = 10$), especially as a *visitor* ($N = 15$) in unfamiliar households ($N = 3$), but also within the own home ($N = 13$, e.g., if it was shared, P7). However, four participants considered their home a place where they would configure their devices themselves, prevent access by strangers, and, hence, would not use *PriKey* there.

Participants also mentioned further places beyond the home such as public spaces ($N = 7$, e.g., restaurants or malls), hotels ($N = 4$), workplaces ($N = 3$), doctors ($N = 2$), or simply "everywhere" ($N = 4$). Two participants mentioned specific target groups that could benefit from *PriKey*, such as older adults (P7) or people in professions with particular privacy risks (e.g., teachers, government employees, P9). However, participants could also imagine scenarios where control over sensors should *not* be enabled through *PriKey* ($N = 7$), such as, e.g. for security cameras of restaurants or shops. In such cases, P4 suggested raising *awareness* of intrusion rather than enabling control.

Comparison to Smartphone Application

On one hand, some participants explicitly stated to prefer a smartphone application with equivalent functionality ($N = 8$), as this would not require an additional device ($N = 6$) and they are used to have their smartphone close by ($N = 3$):

> *"(...) I always have my smartphone with me anyway - my bag is always full, so the less I have to carry around, the better."* (P14)

On the other hand, some participants would prefer *PriKey* due to its tangible form factor, being ready-to-hand and more direct than privacy control via a smartphone app ($N = 4$):

> *"(...) I would prefer PriKey because it's so easy to use. With the smartphone, I would have to swipe around, then look for the app, and then it could be that the battery is empty (...)."* (P10)

Moreover, carrying the tangible can serve as an explicit reminder and increase privacy awareness (P6). Three participants were undecided and would try both.

7.5.2 $RQ_{co}2.b$: Accounting for Individual Needs

Participants deactivated sensors using *PriKey* in all scenarios, but with varying frequency. In particular, they applied on average 10.88 deactivations[3] ($Min = 0$, $Max = 22$, $SD = 6.25$, $Mdn = 10$). Across all participants, 180 of 384 possible choices were "deactivate". Looking at the sensor groups, *video* was overall deactivated most frequently (77 of 128 options), followed by *audio* (61) and *presence* (42). We illustrate individual privacy choices, considerations, and perceived responsibility in the following.

Individual Privacy Choices

We found that participants' privacy choices highly depended on their *role* and *familiarity* to the environment, as well as on the *room/task* they were currently in. In particular, *visitors in unfamiliar environments* applied the most deactivations to nearby sensors using *PriKey* (62 of 96 options[4]), followed by *visitors in familiar environments* (54 of 96). *Primary users* employed 28 deactivations and *co-inhabitants* 36. Looking at the sensor groups, video was again deactivated most frequently in all roles (13 to 23 times), followed by audio (11 to 20 times) and presence sensing (4 to 19 times).

Considering the various *rooms (tasks)* within the scenarios, sensing was most often turned off in the bathroom (60 of 96[4] choices were "deactivate"). Likewise, participants did want to prevent data collection in the living room (56 deactivations) and bedroom (38 deactivations), but less frequently in the kitchen (26 deactivations). Again, video was the most frequently deactivated sensor across all rooms (17 to 22 times), usually followed by audio (13 to 22 times) and presence sensing (8 to 12 times), except for the kitchen (presence sensing: 7 times, audio sensing: 6 times).

Privacy Considerations

Participants were willing to *accept* the collection of personal data to use a device and its functionalities ($N = 9$). Others reported accepting the data collection due to

[3] The total number of choices (i.e., activate/deactivate sensor) per *participant* is 24: every participant conducted two roles/scenarios with 12 sensors in each.

[4] The total number of choices (i.e., activate/deactivate sensor) per [*role/scenario* | *room/task*] is 96: every role/scenario (12 sensors, 4 rooms with 3 each) was presented to half of the participants (8); every room/task (3 sensors) was presented twice to all 16 participants.

a lack of concerns ($N = 9$), convenience ($N = 3$), or they believed their data would be shared anyway ($N = 3$). In contrast, many participants *deactivated* the collection of personal data to protect their privacy ($N = 15$) or the privacy of others (the person on the phone, P9). Participants would also deactivate data collection for devices that they do not currently need ($N = 7$). Three participants particularly mentioned the convenience of the "all off"-button, e.g.:

> *"For simplicity's sake, because I probably don't want to do it individually (...) I will probably just hit 'all off' and then it's done."* (P2)

Sensors Regarding the sensor groups, video recordings caused concerns for most participants ($N = 12$), e.g.:

> *"I would perhaps be a bit skeptical (...)[regarding] cameras, but I would maybe not even install that (...). But [for] everything else, (...) I would be willing to tolerate it because it simply makes my everyday life more pleasant (...)."* (P1)

Moreover, many participants found audio recordings critical ($N = 8$). Presence sensing was considered less critical and only mentioned by four participants.

Devices Besides the sensors that can be controlled through *PriKey*, participants also considered the specific devices. As such, many asked about the purpose of a device ($N = 10$) or the effect on basic device capabilities (e.g., controlling light, $N = 8$) prior to their decision. Here, smart speakers were of particular concern ($N = 6$):

> *"(...) if there is an Alexa in the room, I would like the Alexa to be completely off. Alexa should not even know that I am in the room."* (P8)

Roles Participants' role, as well as their relation to the device owner, also played an essential role in their privacy choices. Participants considered their *trust* towards the device owner ($N = 8$). Some mentioned that only that person was able to access the data ($N = 6$) while having high interest in the device being fully functional ($N = 2$). In the role of the primary user, participants mentioned implicitly having consented to data collection when purchasing devices ($N = 3$) or to having configured devices according to their preferences anyway ($N = 4$).

Rooms (Tasks) Participants also perceived the rooms within our scenario differently. In particular, most participants stated the *bathroom* to be an intimate environment where they would not accept video ($N = 11$) or audio sensing ($N = 4$):

> *"Why does the bathroom have a camera? That certainly is a voyeur camera."* (P8)

Similarly, the *bedroom* was considered an intimate space ($N = 4$), where devices installed by someone else (e.g., the co-inhabitant) would not be acceptable ($N = 2$):

> *"This time, I would also block the camera and the microphone, because this is my refuge in the shared flat and no one should be able to look inside."* (P10)

Also the bedroom task (looking at photos) was considered protect-worthy by participants ($N = 6$). In the *living room*, participants wanted to protect their conversation ($N = 10$). In contrast, the *kitchen* with preparing and having dinner was not perceived as sensitive ($N = 6$):

> *"[In the kitchen] I would just leave [everything] on. It doesn't bother me when people see that I am eating."* (P2)

Threats Few participants were concerned about threats arising from using *PriKey* ($N = 4$), as the mechanism itself needs access to personal user data to work. Attackers who gained physical access to the tangible could manipulate users' settings and, e.g., accept all data collection against users' preferences.

Responsibility

One important question of our concept is *responsibility*, i.e. who is responsible for providing users with an individual *PriKey*? While most participants considered themselves individually responsible for getting a *PriKey* ($N = 14$), some also saw the device owner (inhabitant) in charge of providing tangibles for their visitors ($N = 5$). Of those, three participants would additionally get their own *PriKey* to be on the safe side. In any case, participants wished for the inhabitant to disclose potential privacy intrusions transparently ($N = 3$). Moreover, some participants raised a potential for *conflicts* among the various roles (i.e., primary users and visitors, $N = 6$). Few participants also mentioned specific coping strategies ($N = 2$) such as informing the primary user (here: a friend) first:

> *"(...) I would talk to [my friend] and indicate that I do not want to be recorded."* (P14)

7.6 Future Implementations of *PriKey*

Our results show that most participants would use *PriKey*, especially for visits of (foreign) smart homes. They found it intuitive, easy to use, and trustworthy, and appreciated the form factor and metaphor of the key. We discuss further opportunities and open questions of our concept in the following.

7.6.1 Contextualizing *PriKey*

PriKey enables individual control over the collection of privacy-sensitive data collected by video, audio, or presence sensors. However, our study revealed some factors that could serve as input to automatically adapt *PriKey* to individuals' current context. For instance, individuals' *familiarity* with the environment crucially influenced their privacy decisions. In particular, *PriKey* was used less often with increasing familiarity to the environment, confirming prior work [139]. Moreover, in spaces considered intimate such as the bathroom and bedroom, sensing was frequently deactivated. However, as in previous research [62], our results also indicate that individuals considered the *purpose* of single sensing technologies. For example, in the kitchen, where the task was to prepare dinner, audio sensing was frequently accepted to, e.g., allow for voice interaction while hands are occupied.

Considering such aspects, *PriKey* could act similarly to personalized privacy assistants by proactively making recommendations or even acting fully autonomously [44]. An interesting question for future work will be: *How can PriKey dynamically adapt to users' preferences and context, while keeping them in control over their individual privacy?*

7.6.2 Responsibility, Action & Timing

Participants in our study mainly saw themselves in charge of getting their individual *PriKey*, rather than the key being provided by the device owner. This approach would especially empower *guests* to take control over their privacy, assuming that *PriKey* would work independently of the device owner and manufacturer. However, the "station" with detailed information on device sensors would still need to be installed by the smart home inhabitant(s). It remains to be clarified *who is responsible to distribute and maintain PriKey and its components?*.

Another interesting question will be *how to motivate users to actively use PriKey?* The previous chapter of this thesis indicates that increased threat and coping appraisals, including the perceived severity of threats and perceived knowledge and effectiveness of coping strategies, can lead to increased motivation. An addition to *PriKey* could hence inform users about potential privacy intrusions by nearby devices, and offer the tangible key as effective and easy coping strategy.

As a next step, it remains to be investigated when and how the interaction with *PriKey* should be initiated in real-world situations. Within our scenarios, we explicitly prompted participants to use their *PriKey* to act according to their privacy needs. Future implementations of *PriKey* could, on one hand, follow an *on demand* approach, meaning that users would be responsible to use their *PriKey* if being in range of potential privacy intrusions. On the other hand, *PriKey* could actively *prompt* users in privacy critical contexts [44] or at adjustable timings [66, 147], such

as when entering spaces considered intimate. The question is: *When and how should PriKey prompt users to take control over their privacy?*

7.6.3 Range & Conflicts

With *PriKey*, we aimed to reduce complexity by grouping privacy decisions by sensor type, being applied to all devices in the user's vicinity (*user-centric*). Confirming prior work [35, 231], we found that audio and video recordings were indeed considered highly intrusive and thus were deactivated frequently. However, some participants also wished for control over single specific devices (*device-centric*). At the same time, not all devices do actually pose privacy risks. Moreover, as privacy is highly individual, there is a potential for conflicts if multiple parties set privacy preferences differently in the same surrounding, which opens a need for *cooperative control mechanisms* [226].

Future work should investigate: *What is the ideal range for PriKey (device-centric vs user-centric) and how can PriKey help to mitigate conflicts among individuals?*

7.7 Summary & Conclusion

In this chapter, we present *PriKey*, a concept for tangible privacy mechanisms that especially target visitors in (foreign) smart homes. We illustrate the rich opportunities of our concept and a concrete implementation sample, a Wizard-of-Oz prototype. We used this prototype in a remote user study ($N = 16$), in which we explored *PriKey*'s usability, perceived trustworthiness, and how it accounts for individual needs. Participants appreciated our prototype and its key metaphor for being easy-to-use, engaging, and intuitive. We also found a number of factors that influenced users' privacy decisions as communicated through *PriKey*, such as their familiarity to the environment or the specific space they were currently in. We discuss open questions for the design of privacy mechanisms that *enable control* for inhabitants, but more importantly also visitors in (foreign) smart homes, to help both roles protect their individual privacy. To also protect users' access to devices and, more importantly, personal user data, in daily life use, the next part of this thesis will look into *usable authentication mechanisms* for smart homes.

***PriKey* empowers privacy control.**
The key findings in this chapter are:

- **Concept:** We present *PriKey*, a concept for tangible privacy mechanisms for the smart home context. *PriKey* aims at particularly empowering guests to take control over privacy and security in their own hands, while reducing complexity.
- **Artifact:** We implemented a modular Wizard-of-Oz prototype: a tangible that allows executing privacy configurations for nearby sensors; and a display that provides details on device states.
- **Method:** We conducted a "hybrid" study where the tangible was in participants' hands, while the detailed visualization was remote with the experimenter.
- **Empirical Insights:** Participants found *PriKey* intuitive and easy-to-use. Privacy decisions were influenced by common factors such as participants' familiarity with the environment as well as specific spaces that were considered more intimate than others.

The results of this chapter can inform the design of tangible privacy mechanisms that empower device owners, but more importantly also incidental users to communicate their privacy preferences to nearby devices. This can particularly be useful in (unfamiliar) smart homes, but also in other places such as, e.g., at work or online.

IV

Designing Usable Authentication

PART IV – DESIGNING USABLE AUTHENTICATION

Last but not least, authentication is an effective means to protect smart home systems and access to personal user data and devices' services in daily use. Many current smart home devices do not provide any form of authentication, or mechanisms are of limited usability and user experience [33–35, 93, 135]. As such, this thesis investigates how usable authentication for the context of smart homes can be designed, considering not only the multitude of devices but also the complex interplay of *various users*.

- **Chapter 8** investigates usable authentication for *(co-)inhabitants* of smart homes. Based on an interview study using the story completion method and a focus group with security experts, we derive design considerations for usable authentication within the home.
- **Chapter 9** investigates usable authentication for *guests* in smart homes. We discuss challenges that arise when they want to use sensitive smart home features requiring authentication. We also present and investigate one concrete idea, which is using conversational security questions based on shared knowledge to authenticate guests.

8

Design Considerations for Usable Authentication in Smart Homes

This chapter is based on the following publication:
Sarah Prange, Ceenu George, and Florian Alt. Design Considerations for Usable Authentication in Smart Homes. In *Mensch und Computer 2021 (MuC '21)*.
https://doi.org/10.1145/3473856.3473878

The previous chapters highlight a need for protecting smart home devices as they collect and provide access to sensitive user data, while at the same time being prone to threats. Important steps are increasing users' awareness (Part II) and enabling control over privacy and security settings (Part III). This last building block of this thesis will look into *usable authentication* in the context of smart homes.

As of now, means for authentication provided by smart home devices are scarce [135] and/or limited in security and/or usability [34]. For example, devices a) only require credentials once upon setup, b) rely on additional devices such as the user's smartphone as a proxy or c) transfer desktop metaphors [93] and require

users to employ conventional authentication via unsuitable input modalities (e.g., passwords on a TV's remote control).

To address this, the users' perspective on smart home authentication needs to be better understood, with the ultimate goal of supporting the design of usable mechanisms. Obtaining such knowledge is important in this particular context, since this environment contains personal devices as well as devices shared by multiple people. As a result, knowledge from devices that are exclusively used by one person, such as smartphones, cannot easily be applied.

To close this gap, we conducted 20 interviews with users and non-users of smart home devices, using the story completion method [42]. We chose this method, since it fosters users to think beyond state of-the-art and imagine how smart devices may be used in the future. The story covered: choice of certain devices, setup process, interaction with the device, authentication, and potential issues that might arise by shared use with various roles (i.e., multiple users in shared households, children, guests). Our approach is complemented by conducting a focus group with security experts (N=10), where findings from the story completion method were discussed and further factors influencing the design of usable authentication for smart homes were identified.

Users and experts would design authentication mechanisms depending on the *task* for which devices are used, the *data* they are protecting, and the *frequency* of using the to-be-protected device. However, while users considered certain devices (e.g., cleaning robots) less critical and would thus not employ authentication, security experts were more sensitive as to which threats are possible and would employ authentication for these as well.

Based on the obtained insights from users and security experts, we discuss implications for the design of usable and secure authentication mechanisms for smart homes as well as directions for further research. In particular, the devices' modalities, access to functionality and data, and users' roles are of high relevance when designing authentication. Our work is useful for researchers as well as practitioners concerned with usable security in smart homes.

In this chapter, we

1. investigate **end users'** perception of **usable authentication** in the home using the story completion method ($N = 20$),
2. discuss and complement our findings in a **focus group with security experts** ($N = 10$) from academia,
3. present and discuss **design considerations** for usable authentication in smart homes.

8.1 Research Approach

The design of authentication mechanisms for smart home contexts is challenging due to several reasons, including the increasing number of devices accessing sensitive data, potentially limited input modalities, frequent use (i.e., time-consuming mechanisms are not feasible), and finally, multi-user households in which sharing the authentication secret might be desirable in some, but not in other cases. To address these challenges, we explore how future authentication mechanisms for smart homes can be designed to be usable as well as secure. In particular, we investigated which mechanisms end-users would imagine *usable* in a smart home (study I, Section 8.2) and assessed *security* in a subsequent expert focus group (Section 8.3). This chapter is guided by the following research question:

$RQ_{AU}1$: How can **authentication** for smart home (co-)**inhabitants** be designed to be usable as well as secure?

8.2 Study I: Story Completion

To understand the requirements for future smart device's authentication mechanisms, we set out to capture users' opinions and desires with regard to smart home interactions. In particular, we chose to conduct a story completion study [42]. This method provides participants the beginning of a story and then asks them to complete it as to their imagination.

Our choice was motivated by two factors: Firstly, we wanted users to imagine future scenarios without being limited by state-of-the-art smart devices. Secondly, although the smart device market is continuously growing, it has not penetrated all households yet [170], hence allowing us to include both, users and non-users.

We extended the original methodology by Clarke et al. [42] to allow shifting the focus towards potential problems and issues related to privacy and security, and in particular authentication. Similar to the original method, participants were given the start of a story. However, in our design, we guided users' stories in the further course of the interview by suggesting pre-defined story changes. Later parts of the story were based on the device participants chose in the beginning. Changes were introduced in the same order to all participants to form a consistent storyline (see Section 8.2.2 for details). We wanted to immerse all participants in the scenario, device choice, and functionality before thinking about authentication and potential problems. Note that this study particularly focused on mechanisms that are *usable*

as imagined by participants. As for the *security* perspective, we conducted a focus group with security experts (see Section 8.3).

8.2.1 Motivation for Stories

The motivation for our stories is two-fold. On one hand, current smart home systems rarely provide security mechanisms (such as, e.g., access control) [135], but are at the same time prone to new threats [232] from within or outside the smart home [93]. If existing, security mechanisms for smart devices are of limited user experience [33, 34]. Hence, our stories not only cover device choice (part A), but also (imagined) functionality and usability (part B), and authentication mechanisms (part C). On the other hand, challenges arise from shared device scenarios within households (cf. [77, 78]) with a potential for inside attacks [93] (part D). In particular, we cover the following roles: shared use within a relationship [77, 229] (D1), and visitors [7, 138, 226], including children [142, 210, 229] (D2-3).

8.2.2 Stories

We created a scenario around Lara and Tim, a couple who recently moved together in their house and is interested in buying a smart home device (cf. Appendix D.1 for full interview guide). The interviewees had to complete the story. To focus the story towards challenges of shared use and authentication, we implemented structured changes. We describe those changes in the following.

A. Choice First, participants needed to decide on a *specific smart device*, motivate their decision as well as describe expectations and potential use cases. We intentionally left this choice to the participants to help them immerse in the story. The following parts are based on this device.

B. Functionality & Usability After they ordered and received their smart device, they needed to describe how they set up the device in their home infrastructure. This included the setup process, functionality, and interaction modalities. We wanted to understand if participants see setting up an authentication process as part of the initial setup (as it is the case, e.g., for mobile devices).

C. Authentication Mechanisms As smart devices may collect and store personal data, they should describe a suitable authentication mechanism for the device, considering how frequently it would be used. This part of the story should encourage participants to brainstorm concrete mechanisms.

D. Shared Use Prior work identified various types of users that share smart home devices, including spouse, children and friends [77]. Hence, we included D1-D3 to provoke stories with specific user types to understand whether authentication mechanisms differ depending on types of users sharing the device.

D.1. Couple Problems may arise within the household, as Lara and Tim share the smart device. We asked participants to come up with such problems that are a result of sharing, and to also include potential solutions.

D.2. Children As children (Lara's nieces/nephews) visit their home, Tim gets worried as IoT devices pose a privacy risk for children [142, 210] and consequences of children playing with devices are unknown. The story should comprise negative aspects and countermeasures.

D.3. Worried Guest A very privacy concerned friend is visiting Lara and Tim. They want to convince their friend about their smart device and, thus, their home still being secure and privacy-preserving (e.g., from surveillance).

8.2.3 Recruiting & Procedure

Participants were recruited and interviewed in a public park close to the local university and compensated with one free, non-alcoholic drink. After agreeing to take part in the study, participants were given a short introduction to the topic of the interview and information on our research and data collection. Independent of their prior knowledge, this included a description of the setup and a list of possible smart devices. They were then asked to sign a consent form. Next, they were introduced to the concept of the story completion exercise. For the main part of the study, participants were given the beginning of Lara's and Tim's story and asked to complete it. The rest of the interview was structured according to the story changes described in Section 8.2.2. After the story completion exercise, we gave participants the opportunity to give feedback or ask questions. We audio-recorded all sessions.

8.2.4 Participants

We recruited 20 participants. The majority (15) was between 20 and 29 years old (2 below, 3 above this age), 9 identified as female (others as male), mainly students (11) or employees (6). Five had at least one smart home device. Out of those, all had a smart TV, 2 had an Amazon Alexa, 1 a Sonos music system, and 1 a smart thermostat. We did not count smartphones, although they were mentioned by two participants. On a 5-point Likert scale (1=do not agree at all; 5=strongly agree), participants perceived their technical affinity as rather high ($M = 4.6$, $SD = 0.6$).

8.2.5 Limitations

The study was completed among students in Germany, with the majority being below 30 years old. Results may thus only apply to a similar target group. However, smart home technology is popular among this age group in Germany [196]. Also, our sample size is limited ($N = 20$). Note, however, that only little new information is gained beyond 20 participants [149].

Participants may have been influenced by experiences with smart devices. However, we believe this to be a minor limitation, as (a) there were only five participants who already owned a smart device, and (b) we did not notice any differences in stories between users and non-users. Changes to the story were based on hypothetical situations users might encounter. We ordered the changes based on how we expected them to naturally occur (e.g., purchasing the device, setting it up, choosing an authentication mechanism, shared use). Generally, shared use could occur before setting up authentication. We acknowledge that we did not consider this case.

Finally, experimenter bias is a known limitation for qualitative studies. As such, alternative themes or names may have been given to certain sections. However, we believe that this would not influence the resulting design considerations.

8.2.6 Data Analysis

We conducted 20 interviews with an average length of 20 minutes. One participant data was excluded due to technical issues with the audio file. We transcribed all other interviews. Results were analyzed through thematic analysis [27] by two experimenters.

Firstly, we independently went through half of the dataset each. Secondly, we merged our codes and iteratively found sub-themes. We went through each story part (A-D) and analyzed top-level aspects as directly derived from our interviews. This includes which **A** choice participants made (*Appliances*) and why (*Reasons*), **B** how they imagine the device in terms of *Functionality*, *Setup* and *Interaction Modalities*, and which **C** *Authentication Mechanism* they would imagine. We further looked into which *Problems & Concerns* may arise from **D** *Shared Use* depending on type of user, namely, **D.1** couples, **D.2** children, and **D.3** guests, including potential *Solutions*. Sublevel themes resulted from our iterative analysis. We found and included *Attacks & Threats* as an additional top-level theme, as participants voiced those without our guidance. To provide a descriptive overview of our data, we give counts for device choice and authentication mechanisms. Appendix D.3 shows the full list of codes. Quotes were translated from German. We cite participants (P) with their self-chosen ID. We explicitly mark quotes of device owners with, e.g., $\text{P27}_{\text{owner}}$.

8.2.7 Results

Appliances & Reasons (A)

Participants mentioned various devices. Most popular were *household* devices (21 mentions; including vacuum cleaning robots, fridges, washing machines, coffee machines, dishwashers, heaters, lights), followed by *entertainment* (7; including smart voice assistants and TVs), and *security* (3; front door camera and door lock). Some also included multiple devices. Note that only one of the current smart home users chose the device they already have (smart voice assistant, $P19_{owner}$) for their story.

Participants described reasons for purchasing a particular smart device mainly with increased *comfort*. They mentioned *priority* and *frequency of use*, *societal benefits* and *control* over their home to motivate their device choice. The aim of this part was to immerse participants in the story rather than to explore actual appliances and reasons. Hence, we will not include them in the later discussion. However, they are included in our results. Overall, these confirm prior work that explored reasons for smart home usage [98].

Functionality, Setup & Interaction (B)

To further immerse participants in the story, we asked them to describe (desired) *functionality* and *interaction modalities*. With this part, our aim was to provoke thoughts around the device, its access to data, and a potential need for authentication, including available modalities.

Functionality Many household devices should take over usual tasks, including, but not limited to, ordering groceries (P33, P80), managing shopping lists (P33), or vacuum cleaning (P42, P71). P36 would have liked if their hoover plays music to drown out the cleaning noise. P71 would have wished for an "all-round" hoover, including indoor (vacuum cleaning) and outdoor (lawn mowing) use, playing music, being waterproof and pre-programmable.

Interaction Modalities For the respective devices, stories included multiple interaction modalities, mainly via *voice* and *touch* input, but also using *companion apps* on smartphones, and others. Note that some participants did not include a concrete modality, and some also mentioned multiple interaction modalities for one device (e.g., a display at the device as well as a companion app, P80). While voice was most prominent, P5 explicitly mentioned that it might be challenging for food orders. P53 and P80 involved an additional *smart assistant* as proxy for interaction. P26 described a (limited) list of voice commands for their smart device to hang up in a prominent shared place like the kitchen. P42 and P71 mentioned *no interaction*, as the device is acting *autonomously*. P71 further mentioned *"indirect" interaction*,

i.e. *"close the doors of rooms which it [the vacuum cleaner robot] should not enter"*. Interaction modalities being (not) available may have a strong impact on the design of authentication.

Setup Necessary steps for the *initial setup*, as described by participants, included the connection of the smart device to both, the Internet and/or other devices within the home. While some participants would simply "plug and play", others would read the manual first. Regarding *authentication*, participants mentioned that it might be necessary to enter credentials (P69, P80), login on the device via a second factor (i.e., downloading a code and entering it on the device, P14) or authenticate the new device automatically, depending on other devices within the home ($P19_{owner}$, P21).

Authentication Mechanisms (C)

We asked participants to add an authentication mechanism to protect personal data as collected or being accessed by their chosen device from illegitimate access. In case participants mentioned multiple authentication mechanisms per device, we considered the final mention. Table 8.1 provides a descriptive overview.

Authentication Mechanisms		
Biometrics	fingerprint	11
	face scan	6
	voice (commands, recognition)	6
	other (iris, hand)	2
Token	proximity of smartphone	1
Knowledge	PIN	3
Other		5
Modalities	at the device itself	11
	via an app / the smartphone	7
	at an additional device	4

Table 8.1: Authentication mechanisms participants mentioned in their stories.

Participants mainly referred to biometric mechanisms. They appreciated that such mechanisms would be easy and convenient to use (e.g., *"you just need to approach the device and it recognizes you [via face recognition]", P24*). *Other* mechanisms included two-factor authentication (by sending a code to the smartphone, P21) or encryption of the collected data using a public/private key pair (P42). P42 would also deactivate the Internet connection completely when a device is not in use rather than employing authentication.

Many participants would use the smartphone as a proxy for authentication, or another additional device such as a remote control for smart TVs ($P27_{owner}$) or a voice assistant (P69, cf. Table 8.1, *Modalities*). At the same time, $P39_{owner}$ states that *"a vacuum cleaning robot may anyways not be that privacy relevant"* and using an app (incl. the phone's unlock mechanism) may be enough protection.

We found differences in *when and how often* participants would authenticate. Examples include *once upon setup*; unlocking *when entering the home* (e.g., *"Maybe it's only when they enter their flat. As soon as they touch the door handle, the whole household is unlocked as it is by then clear that it's the legitimate owner."* , P53) or *per use* (e.g., prevent children or party guests from ordering food via the smart fridge, P1).

Challenges Furthermore, some participants raised *challenges* with potential authentication mechanisms without being explicitly asked for it. Examples include technical limitations, such as fingerprints not working (*"It [fingerprint authentication at the smart fridge] is unpractical if the fingers are wet during cooking."*, P1), thus preferring another mechanism (face scan in the case of P1), and unwillingness to share biometric (i.e., fingerprint) data with the device provider (P22). $P39_{owner}$ mentioned face recognition would need to work with multiple faces in a shared household scenario (whereas FaceID on their phone can only store one face, $P39_{owner}$). Furthermore, in family-shared scenarios, voices and faces are similar by default, which may lead to false positives. Another challenge is authentication at doors of smart homes. Memorable passcodes may be too easy to guess for potential attackers (e.g., family member names) and voice recognition too unstable (e.g., when user is hoarse) or too easy to mimic (compared to, e.g., fingerprint, $P27_{owner}$).

Problems & Concerns of Shared Use (D)

Although some problems were user type specific, the majority can be applied to all. Hence, we mainly focused our analysis on overarching themes of problems and concerns that directly or indirectly open a need for suitable authentication mechanisms and are thus included in our design implications (e.g., the frequency of usage and related issues, see Section 8.4.2, or the presence of multiple users and/or bystanders, see Section 8.4.3).

Users & Bystanders Some problems involved only *one user* and the smart device. As an example, $P19_{owner}$ and P5 mentioned possible *"response delays"* that they might find annoying. The second, more prominent problem group included *bystanders* (e.g., children/visitors). Shared use was problematic, as it involved shared data access (e.g., *'The partner can see when lots of meat is ordered, although they decided to be vegan together."*, P24) and changing settings (*"Users with similar voices might accidentally change settings."*, P69). Similar concerns were voiced by $P19_{owner}$ and P22, who said that not differentiating users over time leads to annoyance.

Several problems with *children* were identified: Firstly, children could *"break"* (P22) something, *"lock access"* (P21) or *"order too much [online]"* (P1). However, the more severe consequence of misuse was possible physical harm (e.g., *"Kids are only a problem when the smart device is something that can hurt someone, e.g. windows that can break, jalousies that fall on someone's head, etc."*, P24).

Furthermore, *visitors* might not like (P5) or not agree to the use of smart devices (P5, $P19_{owner}$). $P19_{owner}$ specifically asked whether *"co-located people gave consent?"* when asked about how they would interact with smart devices and P1 asked *"who is responsible for creating trust [towards the device]?"*

Responsibilities & Ownership As our story protagonists will share the smart device by default, participants mentioned issues regarding *responsibilities* and *ownership*. For example, they mentioned that preferences may interfere, leading to annoyance of users, but also to unclear device settings ($P19_{owner}$, P22, P33, and $P39_{owner}$). Furthermore, in case of the device being able to place orders, double purchases may occur (P80), leading to monetary loss. Especially for such cases, permissions seem to be unclear, e.g. *"Who is allowed to do what? Can Lara use Tim's PayPal account?"* (P42). From a technology perspective, sharing devices oftentimes means managing multiple user accounts. Some participants mentioned this might be limited, e.g., a smart coffee machine may not be able to store enough profiles (P53).

Frequency Problems, as illustrated in our stories, may occur at various *frequencies*. While problems from sharing the device with other inhabitants may occur daily, problems with guests may only emerge occasionally. Another factor might be the *frequency of interaction*. If interaction (e.g., based on voice commands) fails during a frequent task (e.g., cooking), it might be more annoying than on rare tasks.

Frequency also had a subjective component. P71 perceived *"changing of the Roomba bin bag"* to be a frequent problem, as it was *"tedious and fault prone"*. Another comment describing a *maintenance* problem was the *"management and extension of [data] storage/space"* (P14). Participants had different opinions as to how this should be handled. P22 suggested data should *"stay on the local device"* until the owner decides what to store *"on the internet on a monthly basis"*, whereas P14 suggested this needs to be done when *"the storage is full"*. For a smart fridge, $P23_{owner}$ expected to be informed *"every time my girlfriend orders tons of vegan food"*.

Attacks & Threats

Although we focused the storyline mainly around usability aspects, we found participants specifically raising concerns regarding potential threats and attacks. As threats are an important aspect to consider for the design of authentication mechanisms, we included this additional theme.

Inside Potential "attackers" might appear *inside* the smart home in several ways. *Mimicry* attacks [110] might occur in such a way that children could impersonate their parents (i.e., actively try to trick a voice recognition system, $P27_{owner}$). However, *similarity* might also lead to an unintended threat, as relatives sound similar to each other by nature (i.e., confusing the voice recognition without intention). As a consequence, children might get access to improper content (P5, $P27_{owner}$) or place

undesired food orders (P1). Furthermore, users might want to prevent (potentially drunk) party guests from ordering food (P1) or changing settings of smart devices. Finally, a feeling of surveillance (P36) or fear of dependence on technology (*"life not possible without a smart home"*, $P27_{owner}$) are potential threats within smart homes.

Outside Attacks might also come from *outside* the smart home. While this may occur in the form of physical attacks (i.e., burglary, P71), others may also be purely digital/cyber-based. Types of attacks participants mentioned ranged from hacking (P36, P42), via (undesired) permanent video recording and transfer from unexpected devices (e.g., from a webcam to the smart TV, P36) to complete surveillance ($P27_{owner}$). For these types of attacks, consequences are severe, as somebody with illegitimate access *"could control my whole house"* (P36). P42 further stated that *"bad guys make it public on the Internet that and how it is possible"*, which may foster further outside attacks on smart homes.

Misconceptions On one hand, we found participants describing security measures on smart devices as unnecessary, as a hoover might not be privacy invasive ($P39_{owner}$). However, we consider such data indeed protect-worthy as, for example, recent data leakage of such vacuum cleaning robots mapping home's floor plans shows[1]. On the other hand, we found overly skeptical participants who would disconnect devices from the internet completely (P42, P66) or even put them in the freezer to stop tracking (P71).

Solutions

Participants suggested various solutions when facing problems (cf. story part D) or, more precisely, threats (cf. previous section). We grouped them into two categories which we describe in the following.

Empowerment through the Technology In some stories, improving technology resolved the threat or gave users more power to avoid it before it happened. P14 suggested that smart devices should automatically log users off if they have not used them for a while. P21 described a "kids sensor" to disable access for children. Participants had great expectations towards the device, considering its "smartness" (e.g., *"device sends alarm [when faced with a threat]"*, P36). An extension of internal storage (P14) or improved voice recognition (P69) could solve some of the problems. Participants were expecting the smart device to automatically detect and deal with a possible threat or problem.

[1] `https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html`, last accessed June 3, 2021

Empowerment through the User Users also provided solutions such as unplugging the device (P27) and even putting it in the freezer (*"In the freezer it cannot harm anyone [...] I would not be able to get unwanted spam if it is in the freezer"*, P71) to stop privacy invasion. Having rooms that are free of smart devices and, hence, *"safe"* ($P23_{owner}$) was another alternative. In $P23_{owner}$'s story, the male protagonist was able to *"see the girlfriend's orders"* and had the *"power"* to make changes to it. Having access to data and being able to edit and delete it, seemed to be linked to a sense of power over the device (and its users). A recurring theme was *education* – for oneself but also for guests (e.g., *"Getting a live demonstration of how easily something is hacked would help me understand how to be more secure in interacting with a smart device."*, P42 and *"[...] guests should be educated about what data is being stored and captured. Of course this is a difficult conversation but if you explain it carefully and with facts, they will listen to it [...]."*, $P39_{owner}$).

8.2.8 Summary

Participants mainly chose known devices for known purposes (cf., e.g., [137] for an overview). However, we used this part of the story (A-B) to immerse participants in the scenario and to be able to focus on authentication mechanisms that are specific to smart home devices rather than to ubiquitous devices in general.

Independent of whether participants owned a smart home device or not, they mentioned authentication mechanisms and problems equally. Notably, device owners mentioned aspects not specific to their devices. For instance, $P19_{owner}$ mentioned the device they already have (smart voice assistant), but elaborated the story beyond what is currently common for it (i.e., the users' phone as token for authentication). Other device owners mentioned different devices in their stories, e.g. $P27_{owner}$ owns a smart TV, but illustrated a smart voice assistant and voice based authentication.

To summarize, all stories of all participants raised aspects that open a need for authentication, e.g. the potential for attacks from within the smart home [93]. Examples from prior work include children who are misusing the smart home for their gain [77] and smart lights that left shared users in the dark when the owner left the house [78]. To respond to issues of shared use, participants mentioned the need to create multiple profiles. This would empower them to give rights to specific groups of users and educate them about their profile. Geeng and Roesner [78] discuss this in the context of "relationships" between the owner and the user, implying that the person who buys and installs it might not necessarily be the user, again opening a need for authentication.

Finally, access control [93, 159, 209] and shared use [77] have been subject to prior work. However, we specifically focused on users' perspective of potential problems and threats that may occur in the smart home and, in consequence, impact the design of suitable authentication mechanisms. In contrast to prior work, we

also assessed these findings from a security perspective in a focus group. In particular, our findings from users' stories informed the questions we discussed with the focus group experts (e.g., potential threats in smart homes and authentication mechanisms for particular devices).

8.3 Study II: Expert Focus Group

We conducted a focus group ($N = 10$) to assess our findings from a security experts' perspective. We chose this method to encourage discussions among participants with various competencies in the field of IT/usable security. Experts were recruited among PhD students ($N = 7$), post-docs ($N = 2$), and professors ($N = 1$) from our research institute on cyber defense (CODE). Participants were experts in different subfields of IT security, including network security, software security, as well as usable security. The purpose of the focus group was twofold: (1) we were interested in how the views of end-users and security experts match, to validate our findings; (2) we complemented our initial investigation with further insights that ultimately shaped the design implications presented in Section 8.4.

8.3.1 Procedure

The session took one hour. After explaining the purpose of the focus group, we presented insights from the story completion exercise and discussed these. Discussions were complemented with a brainstorming about solutions to aspects identified in the first study. The focus group evolved around the following topics: threats, threat recognition, awareness of data tracking, sensitivity of data collected by smart devices, and suitable authentication mechanisms for particular devices (see Appendix D.2 for the detailed protocol).

8.3.2 Results

We now summarize the results from our focus group. We cite experts (E) with randomly assigned IDs (range 1-10).

Attacks & Threats

Experts discussed potential attacks and threats emerging from smart devices.

Physical Harm Analogous attacks may potentially be transferred to or be supported by smart devices, resulting in physical attacks on the home, or even cause physical harm to the user. Examples included eavesdropping sensitive information (manually or supported by, e.g., a smart speaker), burglary, lock out scenarios, fire (via, e.g., a smart oven), or creating strobe effects by turning lights on and off at high frequency, which might cause seizures.

Network & System Attacks A single smart device may serve as a "jumping point" for other devices. Hackers may further attack the home via DDoS (distributed denial of service) attacks or read sensitive data from network traffic (e.g., if the user is at home). The experts further questioned how the system might react in case of unforeseen events (e.g., guests present in the home). Devices might get "out of control". Adversarial attacks were mentioned in case access to the device includes machine learning (such as face recognition).

Data Access & Privacy Further potential attacks on users and their smart homes included privacy breaches and surveillance issues. Interestingly, experts not only saw guests' privacy at risk (as we discussed for our stories in study I), but also owner's privacy in case a visitor comes to the owner's home with tracking technologies.

Automatic Threat Recognition

For some threats, the security experts found solutions that detected threats automatically. Experts suggested that usage pattern may be used to detect a) intrusion or b) harmful behavior of the smart system. These "survey systems" (E3) need to be independent to the main smart device.

Increase Awareness of Data Tracking

To increase the awareness of data being tracked, experts suggested visualizations (e.g., in augmented reality), and notifications (e.g., on the user's smartphone or smartwatch). A further suggestion for awareness of Alexa currently tracking was to explicitly ask her "Do you still hear me?". All experts agreed that it is the lawmakers' responsibility to enforce means to increase tracking awareness, such as, e.g., physical signs (cf. signs in areas under video surveillance according to national data protection regulations). For smart devices, this may also mean to propose regulations to limit the reach of tracking. For example, E2 said *"if users knew that microphones on smart devices were limited to track within 2 meters, they may not need visualizations or notifications every time they face a new smart device"*. Another suggestion was to let users *"see or hear what the system tracks"* (E4). E3 highlighted that it might be of interest to distinguish devices being on vs recording. Finally, the consensus was that the system should adapt to the user's perception of privacy rather than the other way round. Thus, the system should recognize users' (dis)comfort regarding

data tracking and sharing rather than the user hiding from certain devices or taking extreme measures such as putting it in the freezer to have a private moment.

Authentication Mechanisms

Finally, to investigate the need for varying authentication mechanisms and to brainstorm their conceptualization, we discussed concrete device types, namely smart hoovers, fridges, lights and voice assistants, which are among the most mentioned from study I. Most ($N = 5$) experts considered voice assistants most critical (i.e., highly protect-worthy), followed by lights and the fridge. Two experts emphasized that it depends on the specific device's capabilities rather than general device types.

Experts further suggested concrete mechanisms for smart fridges, coffee machines, and voice assistants, considering that the authentication secret might (not) be shared with other (adult) members of the household, children, or guests. Examples included biometric (E5) or continuous (E10) authentication, further mechanisms such as rights or access management (e.g., main owner ultimately approves orders via the smart fridge), and multi-factor authentication.

8.4 Design Implications & Reflection

Based on the findings from our two studies, i.e. the users' and security experts' perspectives, we now discuss and summarize the implications for the design of usable authentication for smart homes. Note that, while participants' stories and experts' suggestions evolved around concrete mechanisms for concrete devices, we base the following implications on overarching themes that emerged from our analysis. We hope these to be useful for researchers and practitioners when it comes to a) implementing novel authentication mechanisms for smart homes and b) evaluating the suitability of existing mechanisms for smart homes.

From a usability perspective, we suggest considering the (potentially multiple) *device(s)* and respective modalities, the user's current *main task*, as well as the involved *user(s)* (Figure 8.1 provides an overview). Moreover, users' *preferences* and *technical capabilities* should be considered. Further security factors are the (potentially sensitive) *data* as well as potential attackers and threats (cf. Figure 8.2 for an overview).

8.4.1 Range & Input

Participants described various smart devices in their stories. Those come with various built-in interaction modalities. While this opens opportunities for novel authentication techniques (based on, e.g., voice), it is also limiting the feasibility of conventional authentication on novel smart home devices. As an example, P42 described

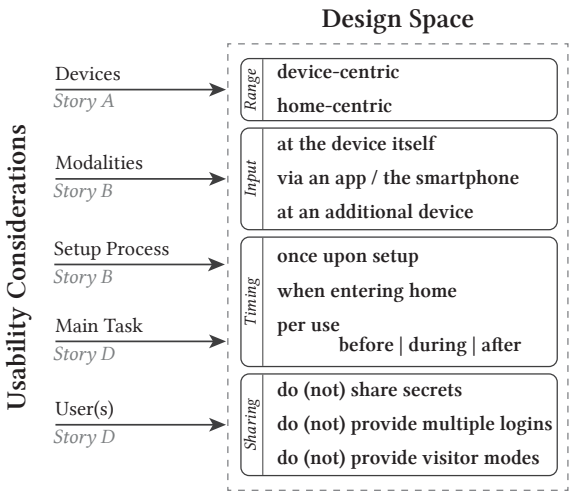


Figure 8.1: Usability considerations as derived from our story completion interviews (parts A, B, and D) informing the design of authentication mechanisms for smart homes.

that they would like to have the possibility to enter passwords on their hoover, hence added a keyboard to the imaginary device within their story. P26 described an additional touchpad, which allows for biometric authentication and adjustment of the hoover's settings.

This opens two main directions for the design of authentication mechanisms for smart devices. On one hand, the feasibility of relying on *the device*'s modalities for the user to employ (explicit or implicit) authentication could be further explored. On the other hand, it might be even better to involve *a second (third, fourth, ...) device* for authentication as many participants mentioned the smartphone as additional device or proxy for the authentication. Another approach could be to not employ device-centric, but home-centric authentication (see Section 10.1.3).

8.4.2 Timing

Participants' stories indicated that they would authenticate at different times. Some participants indicated that they would authenticate *once upon setting up* the device. Another opportunity was to authenticate *when entering home* – i.e., if the legitimate user arrives, the smart home would be unlocked.

We also found several *tasks* during which participants would use (and hence, potentially need to authenticate with) smart devices. A common, "problematic" scenario was cooking as hands may be occupied or dirty, hence limiting interaction possibilities (e.g., P1). Authentication is always a secondary task [182]. Especially in home

scenarios, users want to benefit from the comfort and features of smart devices and focus on their main task rather than on security.

This opens several directions for the design of authentication mechanisms. Authentication could, e.g., be employed *before* an actual task. P53 suggests authentication when entering home (i.e., at the door handle). Other possibilities could include authentication when entering certain rooms (e.g., the kitchen) or explicitly before starting a task (e.g., cooking). Such approaches align with the way in which authentication is currently implemented for smartphones or desktop computers, i.e. users authenticate once and then get full access to all features and data.

For authentication *during* a task, limited interaction and cognitive resources of users need to be considered. Continuous authentication mechanisms (E10) open a chance to authenticate users unobtrusively and effortless, e.g, based on users' physiological and/or behavioral features (e.g., voice, gait) while interacting with their smart devices. Finally, it might also be necessary to authenticate only *after* a task. As an example, authentication could be employed at the end of the actual food ordering process at a smart fridge to prevent children or party guests from ordering.

Furthermore, the *frequency* of using a device and related concerns appeared in participants' stories. Especially if a device is being used frequently, authentication overhead should be reduced by, e.g., employing implicit mechanisms that only occasionally require explicit approval by users.

8.4.3 Sharing

Smart home devices are likely to be shared between household inhabitants. As discussed within our stories, problems may arise from sharing the device. This, on one hand, opens a need for managing authentication by multiple legitimate users, who may have varying permissions. As an example, users might want to actively share the authentication secret to, e.g., let guests control the music or subtenants to control the heating. However, these types of users should have limited permissions (e.g., only short-term changes of settings). On the other hand, certain user groups could be restricted from access to, e.g., let children not use the smart oven without supervision. Regarding the device's setup, some participants would log in to the smart device as a first step. At the same time, they were struggling with the complexity of the overall setup process (P22) and wished for it to be as intuitive as possible (P53). Thus, authentication could be made a mandatory part of the initial setup process. However, contrary to smartphones, this process also needs to consider multiple users by default while balancing the complexity of the overall setup.

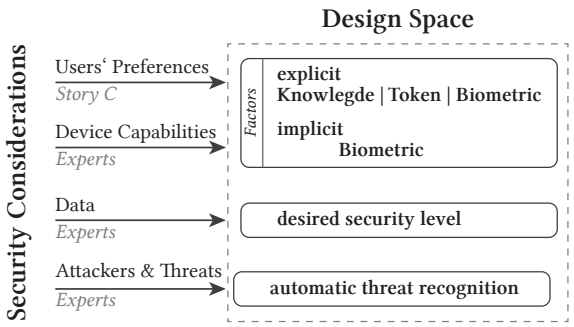


Figure 8.2: Security considerations as derived from our story completion interviews (part C) and expert focus group informing the design of authentication mechanisms for smart homes.

8.4.4 Authentication Factors

Among the three main authentication factors (knowledge, token, or biometric [158]), users in our stories mainly wished for biometric mechanisms, as they found it intuitive and easy to use. Among those, fingerprint scans were especially popular, as well-known from current smartphones. However, not every device carries the capability to scan and process fingerprints or other biometric data itself. In such cases, the smartphone could serve as a workaround and handle biometric authentication – this however requires users to switch to an additional device. Another option is to leverage device capabilities for a suitable authentication mechanism (e.g., using a smart devices' input modalities to enter a secret). Apart from biometric authentication, experts suggested continuous (i.e., implicit) mechanisms as another option. These are effortless for users as they can run in the background and do not require users to remember a secret at all. Illegitimate users such as visitors can be locked out once detected.

8.4.5 Data

We found various (personal) data as being accessed by smart devices. Additionally, we found misconceptions in participants' stories regarding what data devices have access to and how privacy-sensitive this data is. Sensitive data is also collected where unexpected (e.g., floor plans mapped by vacuum cleaner robots). Consequences of illegitimate access and data leakages can be severe (e.g., "control my whole house", P36 and attackers potentially changing access credentials to lockout the main user, E10). For the design of authentication mechanisms, we propose to consider the sensitivity of the involved data. This may have an impact on the acceptable effort for authentication, but also on the choice of authentication with

regard to security. As an example, the desired security level for devices capable of placing orders might be higher than for devices that control lights.

8.4.6 Attacks & Threats

Independent of the type of threat, users want the smart device to recognize a threat and deal with it (e.g., *"It [the smart device] logs all users and recognizes them, so it should know when there is a threat [guest, child, unwanted user]."*, P5). We assume that this expectation is grounded in two factors: Firstly, there is more space available to add additional hardware (e.g., sensors). Compared to a smartphone that is limited by its affordance to be handheld, a smart home device may be larger. Secondly, participants are aware that the device tracks a lot of different kinds of data. Although they did not voice this explicitly, they mentioned various types of data that was captured and expected it to be used to personalize and automate household activities.

An alternative approach could let an additional system track usage patterns to *double-check* whether a particular smart device is being externally manipulated or whether the user's behavioral patterns match the ones of legitimate owners, as previous work shows that such patterns can identify users [223].

8.4.7 Reflections on Methodology

Using the story completion method, we assessed users' choice of authentication mechanisms that they consider *usable*. We argue that this is in line with authentication setup procedures on, e.g. smartphones, where the assessment of security is not in users' hands: users can choose from a number of *secure* mechanisms as suggested by the provider.

After all, our aim was not to create a comprehensive list of design considerations, but rather explore themes that are valuable from a user's and a security expert's perspective. These could be validated and further extended by iteratively developing specific prototypes that were designed based on our considerations, and testing those in-the-wild, i.e. in users' homes. Note that design options still need to be carefully chosen per case and that the same considerations may lead to the design of various mechanisms. Future work could investigate their design, potential implementations, usability and security, including authentication for specific devices as well as for smart homes as whole. Lastly, another focus group with experts from not only academia, but also professionals might lead to further valuable insights.

8.5 Summary & Conclusion

In this chapter, we explore design considerations for usable authentication mechanisms for future smart homes. Interviews with non-expert end users ($N = 20$) using the story completion method provided insights on choices for devices and motivational factors, potential authentication mechanisms as well as problems with various stakeholders. We complemented our findings by a focus group with security experts ($N = 10$). Ultimately, we derived implications for the design of authentication mechanisms, which we hope to be useful for researchers and practitioners. In particular, the available modalities of devices, their access to data and functionality, as well as multiple users and their roles essentially impact the design of smart home authentication that is usable as well as secure. In both studies, we focused on authentication for (co-)inhabitants within the smart home. In the following, we will shed light on authentication for *guests*.

Authentication needs to consider device features and user roles.

The key contributions in this chapter are:

- **Method:** First, we conducted semi-structured interviews with end-users using the story completion method. By providing participants the beginning of a story, we fostered them to think beyond state-of-the-art and consider a future scenario in a (shared) smart home. Second, we conducted a focus group with security experts from academia to complement our initial findings.
- **Empirical Insights:** We derive and discuss considerations for the design of usable smart home authentication from the perspective of end-users' and security experts.

The findings of this chapter can help to design novel authentication mechanisms for smart home scenarios, but also to evaluate the feasibility of existing mechanisms. Moreover, our results can also inform the design of mechanisms for other multi-user scenarios such as, e.g., authentication for shared virtual reality setups.

9

Exploring Usable Authentication for Smart Home Visitors

This chapter is based on the following publication:
Sarah Prange, Sarah Delgado Rodriguez, Timo Döding, and Florian Alt. "Where did you first meet the owner?" – Exploring Usable Authentication for Smart Home Visitors. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '22 Extended Abstracts).* https://doi.org/10.1145/3491101.3519777

The previous chapter (Chapter 8) explored design considerations for usable authentication in the smart home. However, with these, we targeted those who are the main users: device owners and (co-)inhabitants. They usually have direct access to related device interfaces and accounts with associated services.

However, device owners might want to provide access to certain devices and features to their *visitors* [7,135,138,226]. For instance, primary users might allow others to employ short-term changes to, e.g., temperature, but keep exclusive rights for automation rules (e.g., regulating temperature overnight).

Figure 9.1: In this chapter, we explore design challenges for usable authentication for visitor scenarios in smart homes. In particular, visitors can have varying relations and visit at varying frequencies; the smart home environment may provide various functionalities and comprise the presence of bystanders; and authentication can be designed in various ways with regard to timing and responsibility for authenticating, and the concrete mechanism (authentication factor and modality).

Another example are features that require a (paid) user account such as, e.g., streaming music. To allow visitors to use these features, either on the owners' or even their own accounts, they need to authenticate. At the same time, they might not have access to the device's configuration interfaces and should not interfere with the device owners' access rights and configurations.

In this work, we explore challenges for the design of usable authentication for smart home visitors, evolving around the visitors themselves, the smart home environment, and opportunities for authentication (cf. Figure 9.1). Moreover, we present one concrete idea as an example, that is the use of *security questions* to authenticate smart home visitors. Questions could cover, e.g., the relationship to the owner, and could be employed as voice interface via, e.g., a smart speaker to be accessible for visitors. We assessed the perception of both, smart home owners and visitors, towards this approach in an exploratory interview study. We used a Wizard-of-Oz voice interface to simulate the authentication procedure. We found that participants in both roles appreciated the idea and found the mechanism easy to use. However, they also raised a potential for attacks towards the mechanism and our sample questions. We suggest mitigating these by employing personalized or dynamic security questions for visitor authentication. Based on our exploration, we discuss possible directions for future work.

In this chapter, we

1. consolidate **design considerations** for visitor authentication based on related work,
2. present and evaluate ($N = 10$) one concrete initial idea, that is the use of **security questions** to **authenticate smart home visitors**,
3. discuss our initial findings and **directions for future research**.

9.1 Research Approach

The design of usable authentication mechanisms poses a challenge in multi-user, multi-device smart home contexts (see previous Chapter 8). While visitors have been recognized as potential attackers [135, 162], it is unclear if and how legitimate visitors should authenticate to access features that device owners permitted to them. In this chapter, we consider *authentication for smart home visitors*. In particular, we make use of *security questions*, which usually serve as a fallback mechanism for primary users to reclaim access to their own accounts. In our scenario, we take this approach to a conversation between smart home owner, visitor, and authentication mechanism (employed, e.g., on a voice assistant). By answering a number of questions that cover, e.g., aspects of their relationship, visitors can authenticate to access device features as permitted by the owner.

9.1.1 Security Questions

Security questions are a popular means for fallback authentication [16, 23, 51, 106, 171]. Typically, questions are fixed (by the provider), open (freely chosen by users), or a mix of both [105] and often come into play once users loose access to their primary credentials. However, questions are often chosen poorly [171], hence, can easily be forgotten or guessed [184], and many chosen questions have low entropy answers [106]. Moreover, users often provide fake answers to mitigate guessing, which in turn compromises memorability and security as it decreases the distribution of answers [23]. One approach to mitigate this is to base security questions on personal (potentially changing) information. These *dynamic security questions* are easy for users, while being harder to guess for attackers [16, 86]. Questions can, e.g., be based on personal internet activities [16], on personal daily memory captured through users' smartphones [51], or on device usage behavior (e.g., app usage or calls) [86]. However, questions need to address a trade-off between usability and security [86] as the most secure questions come with the worst memorability [23]. Questions based on shared knowledge among friends can increase usability while being hard to guess for strangers [207]. Lastly, asking multiple questions can increase security [106] and accuracy [86].

9.1.2 Research Questions

This chapter targets the following research question:

$RQ_{AU}2$: How can usable **authentication** for smart home **visitors** be designed?

To address this question, we first explore challenges for the design of authentication for smart home visitors based on related work (Section 9.2). Moreover, we present and investigate one initial idea, which is the use of security questions for visitor authentication (Section 9.3). We conclude the chapter with opportunities for future research on (dynamic) security questions in the smart home context (Section 9.4).

9.2 Design Challenges

Based on related work, we derive and discuss challenges for the design of authentication for visitors in smart homes. Figure 9.1 provides an overview.

9.2.1 Visitor Types

Visitors in smart home scenarios can be characterized by the following attributes:

Relation to Owner

The relation between visitors and device owners is crucial when it comes to privacy decisions in smart home environments [138]. Similarly, this aspect also comes into play when owners decide which features should be accessible for visitors [93]. The relation might range from *very close* visitors (e.g., family members who live in different households) to *strangers* (e.g., subtenants or maintenance workers), and fluently cover any type of relation in between.

Visit Frequency

To assess authentication overhead, the usage frequency of a smart home device needs to be considered (cf. Chapter 8). Similarly, the frequency in which a visitor is present in the respective smart home is an interesting aspect. This may range from one time visits to very frequent visits every other day.

9.2.2 Environment & Setting

Other interesting aspects are the devices' functionalities, as well as the presence of one or both, owner and visitor.

Access to Functionality

Smart devices' functionalities can be grouped in different categories [103], which can serve as a basis to define access permissions [93,229]. Moreover, visitors should

generally have limited access to devices and only be able to access functionalities while they are physically present in the home [93, 135, 229]. We suggest that, depending on owners' preferences and specific capabilities, visitors should (not) be able to authenticate for using the respective feature:

Basic For basic features, *authentication is not necessary*. This particularly holds true for functionalities that can be acquired through physical switches [93, 103, 229] and by anybody in physical vicinity of the respective controls such as, e.g., turning on lights or opening jalousies.

Restricted For other features, owners might want to make them available for visitors, but *authentication is necessary*. For instance, visitors might be allowed to play music on the owners' smart speaker, but would need to authenticate (potentially with their own streaming account) first.

Forbidden Lastly, some functionality might not be accessible for visitors and, hence, *authentication is not possible* for visitors. Examples include, but are not limited to, changing automation rules or security settings in the home network [93, 103].

Presence

The scenarios might differ in terms of who is currently present in the smart home. First and foremost, *both*, owner and visitor, could be present when it comes to using the owners' device features (e.g., visiting a friend and watching a movie on the smart TV). However, it might also be that *owners only* are present, in case they provide remote access to certain visitors (e.g., friends who can access files on a shared file system in the home network). Moreover, it could be the case that *visitors only* are present (e.g., tourists in a rental apartment who aim to use smart devices in place), which potentially means to (temporarily) restrict owners' access to protect visitors' privacy [135]. Lastly, the presence of bystanders, e.g. visitors who are not the ones currently authenticating, is an interesting aspect [162]. For instance, they might observe or eavesdrop the authentication procedure which puts a risk on both, owner and visitor.

9.2.3 Authentication Mode

The authentication mechanism itself could be implemented in various ways. We discuss some considerations in the following.

Timing

In the previous chapter (Chapter 8), we suggest that smart home authentication could be employed before, during, or after a main task or device use. In line with this suggestion, visitors could authenticate *before* they actually use any feature within the smart home (e.g., directly upon arrival), *during* their visit (e.g., upon first use of any device or at a specified time), or *after* their visit (e.g., in case visitors placed an order or changed crucial settings, to verify if these should persist and on which account).

Responsibility

Another interesting question is who is responsible to trigger the actual authentication procedure. For instance, the *visitor* could *actively request* a specific device functionality or feature and, hence, authentication would be initiated. Another option would be that the *owner asks visitors* to authenticate. Lastly, the *smart home* could initiate the authentication procedure *automatically*, e.g. at specific times (based on, e.g., a calendar entry indicating guests in the home) or when recognizing non-inhabitants being present (based on, e.g., new personal devices such as smartphones being in range of the smart home network).

Factor

Authentication can be based on one (or a combination) of three main factors: knowledge, token, or biometrics [158]. A *biometric* mechanism, while being convenient and effortless, would require visitors to share biometric data with the device owner and/or potentially unknown devices and providers, which might be undesirable (cf. results in previous Chapter 8). Looking at *token* based authentication, the question arises as to who would be responsible to provide and carry these tokens (i.e., owners or visitors themselves), and when these would be handed out (e.g., upon first visit). *Knowledge-based* mechanisms, as being highly familiar to users and still widely applied, could be easily implemented for visitors as well. For instance, they could set a personal password or PIN for their visit.

Modality

Lastly, it should be considered that visitors might not have access to devices' configuration and/or authentication interfaces, especially if these are available in companion applications only. As a result, visitors who need to authenticate in a foreign smart home should be able to do so via, e.g., *the device itself* or *their personal devices*.

9.3 Security Questions for Visitor Authentication

In the following, we present and discuss one concrete idea to authenticate (also) visitors in smart homes: using *security questions*. Such a mechanism would put a number of questions to both, owner and visitor. In our setting, owners would then accept or deny the visitor's answer rather than the system verifying answers automatically. Questions should be designed in such a way that they are easy to remember for users, but hard to guess for attackers [86]. For instance, questions could cover aspects of the relationship between owner and visitor (e.g., *"Where did you first meet?"*). To make the mechanism accessible for visitors, it could be employed as voice interface (e.g., on a smart speaker) and, hence, be included in a conversation between the two.

9.3.1 Exploration Study

To assess users' general opinion towards this idea in a smart home context, we conducted interviews with pairs of owners and visitors using a Wizard-of-Oz voice interface for the questions.

Apparatus

Wizard-of-Oz Interface To support our interviews, we built an interface with basic text-to-speech features, to simulate interaction with a voice interface for participants. Using the Web Speech API[1], the experimenter could generate voice output for the security questions and responses by manually reacting to participants' answers. Participants only heard the audio output while not seeing or directly interacting with the actual (click) interface.

Visitor Access	Sample Functionalities
basic no authentication necessary	turning smart lights on/off opening/closing smart jalousies setting a temperature on the smart heating
restricted visitor authentication necessary	streaming music on the smart speaker streaming a movie on the smart TV personalized coffee (smart coffee machine)
forbidden visitor authentication not possible	obtaining admin rights accessing the history of voice commands setting routines (e.g., shutters up when sun rises)

Table 9.1: Sample Smart Home Functionalities: We chose a set of functionalities with basic, restricted (using their own accounts), and forbidden visitor access.

[1] `https://developer.mozilla.org/en-US/docs/Web/API/Web_Speech_API/Using_the_Web_Speech_API`, last accessed January 4, 2022

Functionalities & Questions We chose various sample functionalities to cover *basic* (e.g., lights on), *restricted* (e.g., play music via own streaming account), and *forbidden* (e.g., configuring routines) visitor access (cf. Section 9.2.2 and Table 9.1). Moreover, we choose a set of 9 security questions in three different categories (3 each, see Table 9.2 for sample questions): easy (covering basic facts about the relationship), medium (more in depth questions with rarely changing answers), and hard (about ongoing activities with answers potentially changing frequently).

Question Category	Sample Security Questions
easy	When did the both of you first meet? In which city did the both of you meet the first time? Which hobby do you have in common?
medium	What binds you two together? How many smart home devices do you own together? What was your first activity together?
hard	Where did you meet last time? Which restaurant have you visited most together? What was the furthest place you have been to together?

Table 9.2: Sample Security Questions: We chose a set of easy, medium, and hard questions. Questions address the visitor while referring to the owner of the smart home.

Study Design

We conducted a within-subjects study with two independent variables, FUNCTIONALITY (cf. Table 9.1) and QUESTION (cf. Table 9.2). We recruited pairs of visitor and owner. All participant pairs went through all sample FUNCTIONALITIES. We counterbalanced the order of visitors access (basic, restricted, and forbidden) and conducted three rounds per pair to cover all functionalities. For each functionality requiring authentication (restricted), participants had to go through three security QUESTIONS: one easy, medium, and hard in counterbalanced order. As such, every participant pair answered and assessed every security QUESTION.

Procedure

After participants agreed to take part in the study, they were sent a consent form, information on the general procedure, instructions on the authentication mechanism, and a link for the Zoom meeting.

We started the actual session with assigning participant pairs to one owner and one visitor role. We then guided them through three rounds (to cover all functionalities and questions in counterbalanced order). After every round, participants filled in Likert scales on the perceived security and usability of the current security questions (5-point scale, 5: strongly agree):

- It was fine for me to say the answer out loud.
- It was fine for me that the system knows and collects my answer.
- It was easy for me to answer the question.
- Someone who knows the *visitor* can answer the question correctly.
- Someone who knows the *owner* can answer the question correctly.
- Someone who knows *both* can answer the question correctly.
- A *stranger* can answer the question correctly.

We complemented the session with separate interviews with both participants (using Zoom's "Breakout Rooms"[2]) and questionnaires (including demographics, affinity for technology, and general privacy concerns) filled in separately. We gave both participants the option for questions and further feedback.

Recruitment & Participants

We recruited a total of 24 participants (12 pairs) through university mailing lists and social media. Pairs of participants were required to know each other well while not living in the same household, as this is a common relation in smart home contexts [43]. At least one of the pair should own at least one smart home device (to take the role of the owner in our study). A session took around 60 minutes, and they received online shopping vouchers at 10 € or study credits per person.

Participants were 18 to 35 years old ($M = 23$, $SD = 4.01$). 12 of them identified as female, others as male. Most of them were students ($N = 21$), 2 were full-time employees, and 1 was an apprentice. Participants were generally aware of privacy concerns as assessed through the 10-item IUIPC questionnaire [134]: they rated their wish for *Control* ($M = 6.01$, $SD = 1.24$), *Awareness* of data practices ($M = 6.56$, $SD = 0.90$), and *Collection* of personal data vs benefits ($M = 5.51$, $SD = 1.51$). Moreover, their affinity for technology was rather high following the ATI scale [71] (ranging from 1 to 6, overall: $M = 4.37$, $SD = 1.27$; owners: $M = 4.62$, $SD = 1.11$; visitors: $M =$ =4.13, $SD = 1.36$)[3]. Most participants already owned smart devices, mainly smart TVs (7 visitors, 9 owners), smart speakers (2 visitors, 6 owners) and smart lights (2 visitors, 4 owners). They also had experience with sharing their device with co-inhabitants ($N = 6$) and visitors ($N = 4$). However, they did not employ authentication for visitors and/or shared their own accounts.

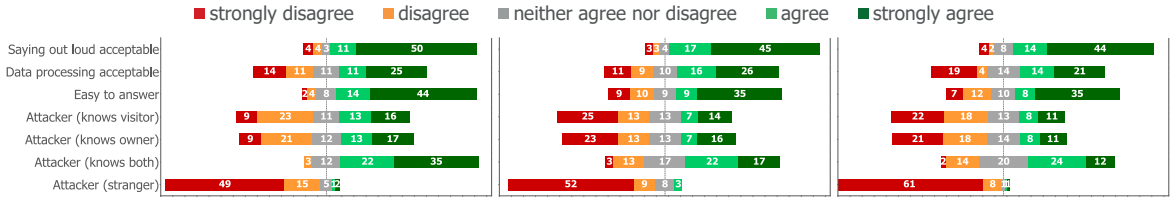
9.3.2 Results

We conducted 12 sessions with a total of 108 security questions (9 per session). The vast majority ($N = 101$) of questions was answered correctly, according to owners'

[2] `https://support.zoom.us/hc/en-us/articles/206476093`, last accessed January 4, 2022

[3] see Section 1.3.2 for details on standard scales

approval. Also, both, visitors and owners, were generally positive towards our idea. The usability of our concept was assessed as good according to the system usability scale [18,29] (overall: $M = 77.40$, $SD = 12.92$; owners: $M = 73.54$, $SD = 9.65$; visitors: $M = 81.25$, $SD = 14.52$)[3].



(a) Easy (b) Medium (c) Hard

Figure 9.2: Study Results: Summary of participants' assessment of the security questions per category (5-point Likert scales, 5=strongly agree). Note that every participant ($N = 24$) assessed three security questions per category, hence the total number of responses is 72. Plots for the single questions can be found in Appendix E.

Perception of Mechanism and Questions

We assessed participants' opinion of our chosen security questions on 5-point Likert scales (5: strongly agree, see Figure 9.2 and Table 9.3 for an overview). In particular, it was acceptable for participants to say the answers loud (overall $Mdn = 5$ for all question categories) and that the system would collect the necessary data and process the answers (overall $Mdn = 4$ for easy and medium, $Mdn = 3$ for hard). Furthermore, it was perceived easy to answer the questions (overall $Mdn = 5$ for easy, $Mdn = 4$ for medium and hard). Regarding the authentication procedure, participants found it efficient and perceived low effort (5 visitors, 6 owners): *"I really like it, because it prevents strangers from accessing personal data"* (P1, visitor). Four owners highlighted the categorization of functionalities as useful: *"I found it very thoughtful: (...) as soon as data is involved, authentication is required (...)"* (P8, owner).

Privacy & Security Concerns

In terms of potential attacks, participants agreed that known individuals (either to the owner, the visitor, or both) could answer the questions correctly (see Figure 9.2 and Table 9.3). However, they rather disagreed that strangers could provide correct answers ($Mdn = 1$ for all question categories). Nevertheless, participants mentioned a potential for attacks (3 visitors, 2 owners) by, e.g. overhearing the answer or finding it on social media. Few participants found the questions too personal and felt uncomfortable sharing the answers (3 visitors, 4 owners): *"I do not like the system to know where I was"* (P6, visitor). One owner mentioned that an attacker could simply confirm every answer and provide access to illegitimate visitors.

	easy				medium				hard			
	Md (V)	SD (V)	Md (O)	SD (O)	Md (V)	SD (V)	Md (O)	SD (O)	Md (V)	SD (V)	Md (O)	SD (O)
Saying out loud acceptable	5	1.43	5	0.35	5	1.26	5	0.62	4	1.31	5	0.53
Data processing acceptable	3	1.47	5	1.48	4	1.49	4	1.38	3	1.47	4	1.57
Easy to answer	5	1.13	5	1.48	4	1.46	5	1.49	3	1.49	5	1.29
Attacker (knows *visitor*) can answer correctly	2	1.39	4	1.26	2	1.55	3	1.47	2	1.38	3	1.37
Attacker (knows *owner*) can answer correctly	2	1.35	4	1.26	2	1.55	3	1.51	2	1.39	3	1.36
Attacker (knows *both*) can answer correctly	4	0.87	5	0.85	4	1.14	4	1.16	3	1.06	4	1.07
Attacker (*stranger*) can answer correctly	1	0.86	1	0.92	1	0.76	1	0.93	1	0.68	1	0.66

Table 9.3: Study Results: Assessment of easy, medium and hard security questions on 5-point Likert items (5=strongly agree). In particular, we report the median (Md) and standard deviation (SD) for participants in the visitor (V) and owner (O) group.

Adoption & Improvement

Many participants would adapt the mechanism in the future (6 visitors, 5 owners). Six participants in the visitor role stated they would also use it if they were the owner of the smart home, and nine owners would use it as visitor. Some participants raised suggestions for improvement. For instance, some suggested that the security questions should be customizable (2 visitors, 7 owners) or more relationship specific (1 visitor, 3 owners) to be more resistant against attackers. Two visitors suggested not requiring owner's approval, but instead verifying answers with stored data or using a preset PIN instead of questions. Two owners suggested adapting to context by, e.g., not reading the questions out loud in case of bystanders being present.

9.4 Future Work: (Dynamic) Security Questions

To explore our idea, we chose a set of fixed questions that we believed to cover easy, medium and hard questions. Prior work suggested the use of *dynamic security questions* based on (changing) personal data (e.g. "Who did you call last week?") [86]. Some of our security questions also have the potential to change over time (e.g., "Where did you meet last time?"), making it harder for attackers. Participants assessed these "hard" questions as easy to answer as static/simpler questions, making them promising candidates for such an authentication mechanism. At the same time, privacy needs to be considered when designing such questions. As such, the question content should not reveal too much personal information [86]. Authenticating visitors should not invade their, the owners', or bystanders' privacy. Moreover, retrieving personal information is becoming increasingly easy (e.g., through

social media), potentially supporting attackers in gaining answers to security questions [171]. The main challenge that remains is to design questions that are easy to answer, hard for attackers, and keep the privacy of both, owner and visitor [86]. Future work should look into how security questions can be designed to be *relatively easy for both, visitor and owner, while keeping their privacy towards each other and be resistant against attacks*.

9.5 Summary & Conclusion

In this chapter, we explored design considerations for usable authentication for *visitors* in smart homes, including various types of visitors, device functionalities, and authentication modes. We present and discuss one concrete sample idea, which is the use of security questions to authenticate visitors. Questions covering the relationship to the owner were well accepted by participants in our exploratory study. We discuss further opportunities around using (dynamic) security questions for visitor authentication.

Visitor authentication is particularly challenging.

The key contributions in this chapter are:

- **Concept:** Based on related work, we explored the challenges that arise for the design of usable authentication for smart home visitors. We also present one concrete sample idea, that is the use of security questions based on shared knowledge.
- **Artifacts:** We implemented a click-prototype using text-to-speech features, to simulate a conversation between inhabitant, guest, and a smart voice assistant.
- **Method:** We conducted an online study where the mock voice interface was controlled by the experimenter, while participant pairs were remote (separately).
- **Empirical Insights:** Both, inhabitants and guests, appreciated the idea and found our mechanism easy to use. However, they raised a potential for attacks.

With the findings of this chapter, we hope to spark future work around designing usable authentication for smart home visitors.

V

Implications & Conclusion

PART V – IMPLICATIONS & CONCLUSION

- **Chapter 10** discusses the broader implications of the results of this thesis, including the interconnection of the suggested measures, the interplay of smart home inhabitants and guests, and a broader reflection on research methods in the context of smart homes.
- **Chapter 11** concludes with a summary of contributions, an outlook to future work and final remarks.

10

Reflection & Broader Implications for Usable Privacy and Security in Smart Homes

In this thesis, we argue for three necessary steps to mitigate threats within smart homes: 1) increasing awareness, 2) enabling control, and 3) employing usable authentication mechanisms.

However, these steps are a) not always distinct (e.g., a control mechanism also increases awareness by its pure existence), and b) need to be actively employed to be effective. Moreover, with the number of devices increasing, and devices becoming more and more sophisticated while not increasing privacy and security standards, novel attacks may arise. In the following, we discuss the interconnection of the suggested mitigation steps and implications for the design of privacy and security mechanisms in the context of smart homes (Section 10.1). Moreover, we will look at the interplay between smart home inhabitants and guests in more detail (Section 10.2). Lastly, we will reflect on research methods in the sensitive context of privacy and security in smart homes (Section 10.3).

10.1 Designing Privacy & Security Mechanisms for Smart Homes

In the following, we summarize and discuss broader implications for the design of privacy and security mechanisms for the sensitive smart home context.

10.1.1 From Awareness to Understanding

Our results in Chapter 4 show that even a rather high level of sophistication in users' mental models is not sufficient to correctly assess data collection and storage in smart home ecosystems. However, this understanding would be particularly relevant for privacy and security. More generally, this indicates that awareness is not enough: even if users are generally aware of devices being connected to each other, their understanding of further implications on privacy and security is limited. In our study, this mental model was particularly prominent among *visitors* of smart homes, indicating that they do not have sufficient knowledge about privacy and security implications. While mental models must be sound enough for users to be able and enjoy to interact with a technology [119], this apparently does not mean that they fully understand all implications on privacy and security.

Hence, we suggest making users aware by means of, e.g., visualizations (cf. *PriView*, Chapter 5). However, making users aware might not be enough, and it might be necessary to verify that users *understand* the implications for their personal privacy and security, especially in contexts they encounter as frequently as their home. Kurze et al. show that reflection on smart home data can foster inhabitants' awareness and understanding [120]. Moreover, awareness mechanisms such as device locators could also serve learning about devices [194]. *PriView* could integrate educational features and, e.g., inform users about concrete implications or even ask questions to verify users' understanding of the visualization. Nudges that guide users to configure their devices securely (cf. Chapter 6) could likewise comprise such educational questions and potentially adapt future content to users' newly gained knowledge.

After all, awareness is an essential first step, and additionally fostering understanding can be a powerful means to urge users to act upon privacy and security within their homes. In other contexts that users encounter less frequently, a simple indication to increase awareness on data collection being in place might still be sufficient, enabling users to, e.g., avoid the area if possible.

Increasing Awareness. In this thesis, we show that awareness of privacy and security implications in the context of smart homes is currently limited (Section 4.2), but is an essential first step to threat mitigation. Awareness can be increased, e.g., through AR-based visualizations (cf. *PriView*, Chapter 5). The desired **amount of information** being transmitted through such mechanisms **depends on the context**. Information needs to be rich enough to increase privacy and security awareness, but simple enough to avoid cognitive and visual overload (e.g., in crowded places).

10.1.2 Empowerment & Motivation

All the mechanisms presented in this thesis more or less rely on being actively employed by users to ensure privacy and security. At the same time, acting upon security and privacy is usually considered a secondary task, interrupting users on the way to their main goal. As a consequence, users must not only be aware but also be *motivated* to use the respective mechanisms when necessary [182].

Motivation & Risk Perception The more severe a threat appears to users and the more specific they perceive the risk, the higher their motivation to take action tends to be [80, 175, 182]. As such, targeting users' risk perception can potentially serve as a means to urge users to take action. This can potentially be reached by creating general awareness for privacy and security as discussed in Section 10.1.1. However, we also specifically targeted this by providing users with details on severe risks, as well as steps to mitigate these during a simulated smart home setup procedure (Chapter 6). We found that participants who received these details employed significantly more secure configurations as compared to participants who only received basic instructions. This highlights the need to provide information that is of sufficient detail to make users aware of specific privacy and security risks, to ultimately increase their motivation to take action.

Protection Motivation. We found that targeting users' protection motivation can foster acting upon privacy and security. We, thus, argue that it is necessary to **target users' protection motivation** and/or risk perception to make sure privacy and security mechanisms are effectively employed by them.

Opportune Moments Another means to drive users to actively take action is making use of *opportune moments*, i.e. identifying ideal points in time to prompt users with privacy- and security-related tasks or decisions. Ideally, users are then willing

and have the time to react and care immediately. Such prompts should consider if users *can* be interrupted (based on, e.g., current cognitive state and mood), and if they *want* to be interrupted depending on the necessity to make a decision [45]. In the context of smart homes, reacting to an immediate threat such as, e.g., bystanders being present when a smart speaker asks for sensitive information, calls for immediate action to avoid private information being revealed to third parties. Less severe issues such as, e.g., updating automation rules to match a new working schedule, can potentially be postponed and only interrupt users at a later point in time. One option could be to prompt users when being idle within their home (by means of, e.g., low activity data acquired by their devices), supposing they then have time to take care of their home's privacy and security.

> **Opportune Moments.** To make sure privacy and security mechanisms are being used, they could **prompt users in opportune moments** depending on, e.g., their current context or emotional state.

10.1.3 When, Where and Why to (not) Authenticate

We also argue for usable authentication within the home, as a powerful means to mitigate threats and protect smart home systems in daily device use. As smart homes cover a wide range of functionalities and provide access to personal data and associated services, authentication within this ecosystem is not only complex but also likely to create a huge overhead. Currently, single services (e.g., a video streaming platform used on a smart TV) require users to create accounts and log in with their credentials to access paid content. However, a smart TV might also have access to various streaming providers, each of which requires users to authenticate. Further devices, such as smart fridges that are able to place orders at various grocery stores, or smart hubs that collect sensitive data from within the home, (should) likewise require authentication.

In contrast, basic functionality such as, e.g., turning on lights or opening jalousies, is less critical as compared to, e.g., permanent changes to light and jalousie automation routines. To avoid authentication overload, such "simple" functionality should be available without requiring to authenticate, while other, more sensitive functionality definitely should call for authentication. This particularly holds true for guests, who should not even be able to access sensitive functionality [43, 93, 115, 229] such as, e.g., permanently changing critical configurations [103]. Guests should, however, authenticate for functionality they are allowed to use, but at the same time be able to use basic functionalities as normal (cf. Section 9.2.2). However, the line between these different functionalities is thin, especially when they are accessible through the same interface. This makes it challenging to draw a proper distinction.

It could, thus, be interesting to move from a device- or service-focused authentication approach to a more *home-focused* approach. For instance, users could be authenticated when entering their home, as suggested by participants in Section 8.2. This could be integrated with opening the door, which in itself forms a traditional way of token-based authentication with a physical key. Other possible mechanisms include gait or palm vein recognition at the door handle [143]. This would also most likely match users' current expectations. However, while locking the physical door to the home serves as a physical barrier, it does not protect access to users' digital smart home valuables such as personal data. A more specific approach could be to employ authentication at a particular room that users consider sensitive (e.g., the bedroom), to avoid illegitimate access to devices or services within this specific space. Another opportunity is to require authentication when a specific device setup or set of functionalities is used, e.g. a home movie kit, to unlock all available streaming services as well as associated configurations of light and sound systems.

A more extreme approach to avoid any overhead could be to not require any form of conventional authentication, but instead assume that whoever has physical access to smart devices and/or their controls, is allowed to use it [229]. While this is apparent for basic functionality such as turning on lights, it becomes more critical for devices that are, e.g., able to place orders at the owner's expense. Also, this approach reaches its limits as illegitimate users gain physical access. This could include, e.g., children or former room-mates who should not be able to execute sensitive or monetary actions.

> **Smart Home Authentication.** The design of usable authentication in the context of smart homes is challenging due to the heterogeneity of devices and functionality, and the complex role and permission system. Authentication mechanisms, thus, should follow a **home- or functionality-focused** approach.

10.1.4 Active vs Passive Mechanisms

Mechanisms for privacy protection in smart homes can be classified by their degree of proactivity (low, medium, high), with users preferring mechanisms that are simple and proactive, but still offer them control [102]. This thesis presents both, mechanisms that are *passive* and such that have the potential to be more *active* in supporting users to protect their privacy and security.

PriView (cf. Chapter 5), as being employed on personal devices (e.g., smartphones or glasses, cf. Section 5.3.2), creates awareness of specific risks (i.e., areas of data collection) using augmented reality. It is thus rather *passive*. However, it could also *actively* send notifications in case an area of data collection is entered. Users would

then have the opportunity to actively react by, e.g., avoiding the area completely or turning off devices if possible. Furthermore, as AR is a useful tool during privacy decisions [20], such an awareness mechanism could also be integrated directly with means for control [112, 205]. For instance, *PriView* could provide an integrated control interface (cf., e.g., *PARA* [20]) or be combined with other, independent control mechanisms such as the *PriKey*.

Nudges, as suggested in Chapter 6, are in itself rather *passive*, but aim at targeting users' *actions*. As timing is crucial for nudges to be effective, they could be employed in a proactive manner and, e.g., prompt users when detecting new devices to help set them up, or prompt users regularly to secure their existing setup by using respective settings and updates (cf. Section 6.5.3). For the *PriKey*, we explicitly called participants to use the available settings in our study scenarios (Section 7.4). However, in real-life scenarios, providing the tangible in itself might create awareness, but does not actively call for action (it is, thus, *passive*). To remind users of employing their desired settings, *PriKey* could behave more *active* and, e.g., vibrate or emit sounds in case new sensors are detected that users might want to deactivate. It could also remind users when entering privacy critical contexts [44], or at fixed adjustable timings [66, 147] (cf. Section 7.6.2).

Another opportunity to support users in protecting their smart homes could be to employ fully *active* mechanisms. In particular, privacy and security settings could be adjusted based on users' preferences or desired standards, *automatically* and/or *autonomously*. However, this creates a trade-off between privacy awareness and control with potential overload on one hand, and a loss of control, but also decreased awareness on the other hand [44]. Many users prefer a certain degree of control as compared to a fear of increasing device autonomy, while others rather accept automation to avoid cognitive overload [44], which would support the design of *passive* mechanisms. Privacy and security mechanisms should at least allow users to configure their desired level of automation, and how *active* the mechanism is allowed to behave. Mechanisms that help configure smart home setups could learn from users' preferences and consequently act autonomously for, e.g., new devices being added to the setup. Other characteristics that could serve as input for such *active* mechanisms could be users' default protection motivation [175] (i.e., the lower users' default motivation, the more could be taken over by the mechanism and vice versa) or users' privacy persona [56] (i.e., the mechanism would actively apply settings according to users' profile).

As for authentication, explicit mechanisms would *actively* prompt users to authenticate in cases they try to access a smart device or service. This makes authentication different from mechanisms that target awareness, which can be employed less frequently, and control, which can be set to opportune moments. As such, an interesting opportunity is to embed authentication implicitly (i.e., *passively*) in users' current tasks. For instance, interaction and behavioral patterns within the home could potentially serve as input for authentication [117, 167].

> **Active vs Passive Mechanisms.** In this thesis, we show that passive mechanisms supported users in protecting their privacy and security. However, in our study scenarios, we actively called for their use. Depending on the current context, mechanisms could also **actively** react to protect users' privacy and security in the context of smart homes (e.g., in critical cases, mechanisms could alert users or react immediately, while staying passive otherwise). Thinking further, a mechanism could stay aware, assess and understand the situation, and make (**passive**) suggestions or react **actively**.

10.1.5 Further Considerations

With designing privacy and security mechanisms for the smart home context, care needs to be taken to not introduce new threats with the mechanisms being employed. In particular, an awareness mechanism that highlights devices employed by others would need to also provide information about their own devices to others, again putting the privacy of all involved parties at risk. As such, individuals should be made aware of not only privacy intrusions by others, but also about personal information being revealed to others with a chance to opt out or at least anonymize this data reveal. As for control, it should not be possible for individuals to employ less secure and less privacy-preserving settings than the device owner. Usable authentication mechanisms should be designed to suit the device and purpose, and avoid users employing workarounds such as, e.g., noting down passwords.

> **Threat Mitigation.** Privacy and security mechanisms should not introduce new threats to the sensitive smart home context.

Lastly, employing such mechanisms should maintain the primary device functionality, while ideally avoiding side effects on privacy [43]. For many devices, it would still be possible to fulfill their primary purpose if the "smartness" was turned off (temporarily) for privacy and security reasons. For instance, a smart fridge would still be able to keep groceries fresh without monitoring its content or communicating with a grocery store. However, other devices, such as, e.g., a smart voice assistant, become unusable once the main sensor (here: microphone) is deactivated. The mechanisms presented in this thesis act differently regarding the devices. While *PriView* can be employed independently without affecting functionality, the *PriKey* deliberately affects built-in sensors to avoid sensitive data being collected. Moreover, the *PriKey* in itself needs sensors to identify devices in the users' vicinity. Authentication mechanisms do not necessarily affect the device functionality per se, but might still interfere with the intended user experience.

> **Device Functionality.** Privacy and security mechanisms should preserve the primary device functionalities as far as possible.

10.2 Residents vs Guests of Smart Homes

In this thesis, we focused on two target groups: *inhabitants*, as those who live in a smart home and have the power to purchase, configure, and primarily use devices; and *guests*, who might be temporarily present within the home, and are, hence, actively or passively, affected by smart devices and built-in sensors. In the following, we will discuss the variety of relations, the potential for conflicts, and responsibility.

10.2.1 Visitor Relations & Access

Visitors in smart homes might have diverse relations with the owner and, as a consequence, a variety of permissions [43,78,93,135,226,229]. In Chapter 9, we recruited user pairs who knew each other well (while not living together). Hence, it would be likely that they, in a visitor-owner-scenario, would provide access to device features to each other. However, relations within and from outside smart homes are more complex in real-life, posing a challenge to the design of access control [93]. For instance, smart home owners could invite close family members to their place, or new acquaintances. Consequently, they might (not) want to provide access to their guests. Moreover, relations between individuals are fluid and might change over time (cf. [78] and Section 9.2.1). For instance, someone who is foreign to the environment on their first visit might become familiar during following, frequent visits. With increasing trust, owners might be more willing to give access to their guests. In contrast, access should be revoked for visitors who are not welcome anymore (e.g., ex-partners).

In any case, providing full access to (trusted) others is not ideal. For instance, visitors playing music via a streaming service would break the owner's music history and suggestions, and reveal (uncommon) music preferences to each other [78]. Access to critical configurations (e.g., security settings or automation routines) should exclusively be kept to the main device user. Both could be handled by authenticating visitors within the smart home, enabling them to use streaming services on their own accounts, while preventing them from accessing critical functionality. An interesting question for future research is how to handle *visitors of various types* (cf. Section 9.2.1) with *various access permissions* (cf. Section 9.2.2)? How should permissions adapt to the fluent transition between a foreign and known visitor?

10.2.2 Authentication for Visitors

As illustrated in Chapter 8, authentication for certain smart home features should be enabled for some, but not all users possibly in reach of a smart device or service. Another interesting dimension is the duration of the visit, accompanied by device usage. Short visits, during which devices are not used, might not require guests to authenticate, but they should be made aware that they are potentially affected by data collection. Longer visits with frequent device use, however, might require guests to authenticate more frequently.

Another question is the design of the actual authentication procedure. The security questions we suggest in Section 9.3 addressed common experiences of owner and visitor. However, such content might not exist (yet) for first-time visits or rental apartment scenarios. A biometric mechanism, while being convenient and effortless, would require guests to share personal biometric data with a home that is not theirs, which might be undesirable as well (see Section 8.2.7). Another possible way to authenticate visitors is token-based authentication. However, the question then is who would be responsible to provide the token (similar to Section 7.6).

Interesting questions for future research include the *ideal modality* for authenticating guests, as well as *how frequently should guests authenticate*?

10.2.3 Tensions & Conflicts

While this thesis focuses on visitors' privacy and security being at risk in (unfamiliar) smart homes, this does not capture the whole picture: It might also be the case that owners are at risk if guests bring unknown sensing technology in the form of, e.g., smartphones or wearables, to their private environment. Guests, however, might not even be aware they are currently entering a "smart" home, let alone the concrete devices, their precise position, and built-in sensors. While awareness mechanisms such as *PriView* could address this, it is critical to sacrifice the device owners' privacy to meet bystanders' privacy needs [205], by providing them with information on devices. Participants in Chapter 5 and Chapter 7 mentioned mistrust and discomfort that could arise as soon as they become aware of devices. They tended to dislike being recorded by devices they did not install themselves. If visitors are comfortable interacting with the owners' devices, each other's privacy and security need to be protected. To achieve this, devices could provide visitor modes [229]. For instance, visitors could interact with a smart voice assistant to play music, but without recording their commands, nor accessing the owner's music history [78].

Also, when employing privacy and security mechanisms, there is a risk of creating (additional) mistrust between owners and visitors as an undesired side effect. For instance, while owners might require visitors to authenticate to protect against third

parties, visitors might interpret this as an offense towards them and their relationship. Moreover, if privacy and security preferences differ, tensions can arise if both, owners and visitors, employ control over settings. While in this thesis we argue that privacy and security mechanisms should be made available to both, owners and visitors, it should be transparently disclosed which devices are present, and what *measures could be taken to find a compromise between both of their preferences*.

Lastly, conflicts can also arise beyond privacy and security, for instance, if visitors do not know how to achieve basic functionality such as turning on lights [43], or if they would break device owners' routines if they use, e.g., regular light switches [115].

10.2.4 Responsibility

All mechanisms presented in this thesis raise questions w.r.t. responsibility.

Who should (not) be aware? Generally, anybody who is in range of data collection by smart home sensors should be made aware of this and potential implications on privacy and security. However, it is unclear who should be responsible to ensure this. In multi-user households, there is usually a "smart home driver" who takes the initiative to install devices, and, as a consequence, has access to functionalities of as well as information on devices [78]. As such, it would be most straightforward to have the device owner – as the one who purchased and installed it – informing others, which is also the case for, e.g., public surveillance systems where the owner is obliged to transparently inform passengers about the tracking. However, co-inhabitants as well as guests would then need to rely on this person to hand out the respective information, without any (current) legal framework. Related work highlighted that users learn from external sources about devices and threats, rather than from the device owner (in this case: the landlord) [35]. Another option are indicators at devices themselves, but these are only limited effective (cf. Section 3.1.2). Instead, a mechanism such as *PriView* could be available to anyone on their personal devices, to shift the responsibility of gathering information to anyone's self. While this would still require *PriView* to be able to scan the environment as well as to collect and share information on devices, it ensures that this information is available to those being affected by the devices. This, however, neglects that there might be other stakeholders who should *not* at all be made aware of smart devices being in place. For instance, a mechanism that shows the location of every security in the home should not be in the hand of burglars, as this would compromise the security of the house [226]. Awareness should thus be increased among trusted parties, while not handing out information to untrusted parties.

Who should (not) have control? While this thesis argues that anybody within the context of smart homes should have control over privacy and security, ubiquitous

means for control also put responsibility into question. For instance, when visiting a smart environment, the question is who should be responsible to hand out the control to guests. Also here, the most straightforward solution would be to see the device owner responsible to provide control interfaces to guests. However, to really keep them in control over their privacy and security, it might be the better choice to actually provide anyone with, e.g., a *PriKey*, to be able to use it whenever necessary. In contrast, with providing novel means for control, care needs to be taken as to who gets hold of these. For instance, while control should be enabled for anyone whose privacy and security are affected, passengers should probably not be able to turn off smart devices that have been placed for security purposes. In these cases, a compromise could be to anonymize collected data, to keep critical security and privacy systems in place and functional.

Who should initiate authentication? As for authentication, it is most likely the system prompting anyone trying to access sensitive functionality with the need for authentication. However, owners might want to reduce authentication overload and, thus, choose to stay logged in or otherwise remove authentication for non-critical features (e.g., playing music on a prepaid subscription). Guests, however, should still need to authenticate, even for these features.

The interesting question is who should then be responsible to initiate the authentication procedure. Should it be the owner actively requesting it from guests? This, however, could generate mistrust. At the same time, guests themselves might likewise be hesitant to do so to avoid social awkwardness. Authentication could, thus, still be initiated by the smart home system, supposing it could detect relevant instances, such as, e.g., guests being present and aiming at using devices.

10.3 Reflections on Methodology

Within this thesis, the sensitive context of users' homes is at focus. Ideally, we would collect data within users' actual homes. This, however, is challenging as a) homes are users' most private and secure place, and collection of (additional) sensitive data might be undesirable, and b) smart home technology has not reached the majority of households yet, particularly in Germany where all research forming this thesis was conducted. Moreover, we conducted evaluations with early-stage prototypes, which were not ready for in-the-wild deployments (yet). As such, this thesis applied various methods to assess users' perceptions and evaluate early prototypes, and to collect rich and meaningful data also beyond users' homes. We reflect on these criteria and details in the following. Table 10.1 provides an overview.

10.3.1 Overview: Smart Home Privacy & Security Studies

Several opportunities were used in this thesis and prior research to investigate privacy- and security-related aspects in the smart home context. In particular, users' perceptions and opinions can be acquired by asking them directly through interviews. In this thesis, we supported interviews by means of a drawing exercise or a story completion task (cf. Section 10.3.2). For evaluating prototypes, studies can be conducted using simulations in the lab or by means of hybrid settings (e.g., with an online prototype and participants being at home, cf. Section 10.3.3). Lastly, studies can be conducted in users' very own home environments (cf. Section 10.3.4).

These studies differ in terms of the quality and location of the *prototype*, the locations of *participants* and *researchers*, related *intrusiveness* and *effort*, and the *number of scenarios* that can be covered during the study. Table 10.1 provides an overview of how the studies presented in this thesis match these criteria and includes samples from related work for at-home studies.

Participants For conducting the studies, participants can be invited to the *lab*, or stay *at home* for an online or at-home study.

Researcher The researcher can either be with participants in the *lab*, be *remote* (in the case of hybrid setups), or actually enter *participants' homes*.

Prototype To be employed *in users' homes*, prototypes needs to be *highly developed* and *fully functional*. An alternative is to employ *early stage*, *low fidelity* prototypes *in the lab* or *online*.

Intrusiveness The closer the research comes to users' actual homes, *the more privacy intrusive* it probably is. For instance, an interview that is not conducted in users' private environment is less intrusive than a study with data being collected in their actual homes.

Effort The effort of conducting a study is in line with the study setup and stage of the prototype. For instance, lab studies without any prototype or online studies with low-fidelity prototypes might be *less effort*. Lab studies with prototypes might be more time-consuming, while at-home studies with fully-functional prototypes are of *high effort*.

Scenario(s) At-home studies can cover *one scenario*, i.e. users within their actual living environment (potentially with co-inhabitants/family members). With studies conducted online and/or using simulations, we can cover *multiple scenarios* in one study, e.g., living in and visiting a smart home (cf. Section 4.2) or visits of familiar and unfamiliar smart environments (cf. Section 5.4).

	Asking Users	Simulation Studies	Hybrid Studies	At-Home Studies
participant	lab	lab ∣ remote	at home	at home
researcher	lab	lab ∣ remote	remote	remote, access to home
prototype	–	early-stage (lab ∣ online)	low-fidelity (online)	high-fidelity (home)
intrusiveness	low	low	medium	high
effort	low	medium	medium	high
scenario(s)	multiple	multiple	multiple	one
Examples	Mental Models (4.2), Story Completion (8.2), Expert Focus Group (8.3)	lab: *PriView* Exploration (5.4), remote: Setup Simulation (6.3)	*PriKey* Exploration (7.4), Security Questions (9.3)	e.g., [35,78,120,187]

Table 10.1: Research Methods: In this thesis and prior work, several methods were applied that can be categorized as *asking users*, *simulation*, *hybrid*, or *at-home* studies.

10.3.2 Asking Users: Assessing Perceptions & Opinions

For the mental model drawings in Section 4.2, and the story completion interviews in Chapter 8, we used stimuli to immerse participants in the scenario: a living in or visiting a smart home scenario prior to the drawing exercise (Section 4.2); and the beginning of a story around a couple in a (future) smart home for the interviews (Section 8.2). As such, we were able to collect users' opinions as direct as possible, while keeping potential privacy intrusions to a minimum (as users' actual homes were not involved). Within this thesis, we also conducted a focus group with security experts from academia (Section 8.3). However, we did not immerse them in a concrete scenario but rather introduced them to the general topic of smart devices, homes, and the need for authentication for the same.

> **Asking Users.** Assessing users' perceptions directly is a common means in HCI research, though often too hypothetically or suffering from recall issues [122]. In this thesis, we used **descriptive scenarios** as a powerful means to foster **users' imagination and immersion**, and ensure **rich and valid results**.

10.3.3 Evaluating Prototypes

Simulation Studies (Away from home) For investigating *PriView* (Section 5.4), we simulated several scenarios (including visits of known and foreign smart homes) using virtual reality. As such, participants were with the prototype physically in the lab rather than in their homes. However, we immersed participants in the (VR-based) scenarios as best as possible while experiencing our prototype. Hence, we did not need to enter any of the scenarios (e.g., visiting a friend) in the real world, protecting the privacy of all stakeholders. Yet, this allowed us to investigate and compare multiple scenarios in one session with comparably low effort. To investi-

gate the effect of nudges (Section 6.3), we simulated a smart home setup procedure in a web application that users could access from their homes or anywhere else. Again, this allowed us to investigate a specific scenario with comparably low effort and high flexibility (reaching a large number of participants via the web).

> **Simulation Studies.** Using simulations (VR- or web-based) allowed us to explore and compare **specific, controlled scenarios** in depth using **early-stage prototypes**.

Hybrid Studies (Partly at home) For some of the studies presented in this thesis, participants were in their home, while the prototype and/or researcher was remote. In particular, we investigated the *PriKey* as follows (Section 7.4): we sent a physical prototype to users' homes, while the researcher, as well as an additional part of the prototype, were remote. This allowed us to, on one hand, explore participants' opinions while being in their environment. On the other hand, we could remotely simulate the effects of the tangible in users' hands with relatively low effort. Also, with no personal contact to participants and their home environment, we protected their privacy, security, and safety (during the Covid-19 pandemic). During our trial of security questions for visitor authentication (Section 9.3), both, owners and visitors, were in their respective homes, while the researcher and prototype simulation were remote. Similarly, this allowed us to explore our concept with a low-fidelity prototype controlled by the experimenter, while participants could stay private and secure and their own environment.

> **Hybrid Studies.** By means of hybrid studies, we could investigate **low-fidelity prototypes** in depth, while leaving **participants in their own trusted environment**.

10.3.4 Excursus: Longitudinal At-Home studies

While not conducted within this thesis, the other, ideal end of the spectrum would be studies fully conducted within users' actual homes. Examples from related research within the home include technology probes [120, 187], a longitudinal diary study with devices being set up exclusively for this period [35], and experience sampling with native smart home inhabitants [78]. However, these types of studies come with high effort for both, researchers and participants, along with high privacy intrusions (as data collection would actually enter participants' homes). Moreover, it would require fully-functional prototypes for long-term, in-the-wild deployments. In contrast, research in this thesis focused on investigating early-stage prototypes (such as, e.g., the *PriKey*), specific scenarios, and users' general opinions and perceptions.

11
Conclusion and Outlook

This chapter concludes the thesis with a summary of the contributions presented (Section 11.1), open challenges and directions for future research (Section 11.2), and closing remarks (Section 11.3).

11.1 Summary of Contributions

This thesis contributes to three overarching research questions, targeting users' awareness, empowering control, and usable authentication in the context of smart homes. We summarize the respective contributions in the following.

RQ$_{\text{AW}}$: How can users' privacy and security **awareness** be increased?

In Chapter 4, we investigated privacy mental models of smart home *inhabitants* and *visitors*. We found that both groups, albeit having a sound mental model of smart

home technology, lack awareness of implications regarding their personal data being collected by devices.

With *PriView* (Chapter 5), we contribute the concept of *privacy visualizations* to $\mathbf{RQ_{AW}}$. We implemented two prototypes, on a handheld, mobile device and on a handsfree, head-mounted display. In various sample scenarios, including visits of foreign and known smart homes, *PriView* successfully increased users' awareness of potential privacy intrusions, enabling them to avoid these, if necessary.

$\mathbf{RQ_{CO}}$: How can users be empowered to execute privacy and security **control**?

To empower *inhabitants* as well as *visitors* to execute control over their privacy and security ($\mathbf{RQ_{CO}}$), this thesis suggests two means. Firstly, including nudges in device setup procedures led device owners to employ more secure and privacy-preserving settings (Chapter 6), which ultimately protects their smart home systems. Secondly, the *PriKey* concept and prototype (Chapter 7) empowered (co-)inhabitants as well as visitors (in both, known and foreign smart homes) to take control over their privacy by allowing them to deactivate sensors in their vicinity.

$\mathbf{RQ_{AU}}$: How can **authentication** be designed to be usable as well as secure?

In this thesis, we shed light on designing usable authentication ($\mathbf{RQ_{AU}}$) from different angels. Firstly, we focused on (co-)inhabitants and derived design considerations from interviews with end-users and a focus group with security experts (Chapter 8). Secondly, we focused on visitors and opportunities for them to authenticate. We explored the design challenges that arise from various visitor types, and tested one concrete idea: security questions based on shared knowledge (Chapter 9).

11.2 Open Challenges & Future Research Directions

This thesis paves the way to reclaim the notion of a secure and privacy-preserving home, with a particular focus on *(co-)inhabitants* and *guests*. However, further stakeholders frame the scenarios of future smart homes, opening new challenges to the design of privacy and security mechanisms that are inclusive and usable. Moreover, further privacy and security mechanisms are an interesting direction for future research. Lastly, the findings of this thesis can serve research in other application areas beyond the home. We discuss these in the following.

11.2.1 Further Stakeholders

This thesis particularly targets primary device users (*inhabitants*) and *guests*. However, looking at the complex scenario of multi-user households and smart devices, many other stakeholders, from within and outside the actual home, come into play.

(Passive) Co-Inhabitants

Contrary to visitors, co-inhabitants do permanently live in the same environment as the smart device(s). Hence, they are affected by the devices – and respective data recording and/or functionality – while not actively using them. As such, awareness, control, and potentially authentication need to be enabled for them as well.

Awareness *PriView*, as an awareness mechanism, is open for co-inhabitants to use. However, given their permanent stay within the environment, a frequent use of such mechanisms can easily become annoying and burdensome. Instead, an awareness mechanism for this target group could be more active and notify co-inhabitants on change, e.g., on their personal devices.

Control Similarly, a control mechanism such as *PriKey* is available to co-inhabitants, but frequent use is not feasible within the own environment. As such, a control mechanism for co-inhabitants could act more like a personal assistant (cf. PPA, Section 3.2.1) and, e.g., adapt settings of new devices in their home environment proactively.

Authentication As for authentication, care needs to be taken as to which functionality should be opened to whom (cf. Section 10.1.3). Future research should look into how to design authentication mechanisms that are accessible to co-inhabitants, especially if they cannot or do not want to actively interact with devices, might not have access to companion interfaces, but still need access to functionality if necessary (e.g., adjusting critical settings of the smart home system while the primary user is away).

Landlords & Property Owners

Landlords are another interesting target group as they are not living in the home, but still have the power to install devices [78]. As such, it is not (only) their own privacy and security that might be affected, but that of their tenants.

There might be cases in which smart devices fulfill an urgent need (e.g., monitoring humidity after a water leakage) and are, thus, necessarily set up by the landlord or property management, potentially even without inhabitants' consent. Other smart devices, such as, e.g., smart electricity meters, can even be set up by other instances

to serve organizational as well as environmental purposes. However, devices installed by these parties completely take away the tenants' control and awareness, especially if they are not actively informed about the installation. The devices' purposes, as well as access to associated data, need to be considered. For instance, tenants might accept their landlord accessing energy and water consumption, but not the video feed of a camera placed indoors. Future research should look into how this can be ensured (or, if necessary: enforced), and how conflicts between landlords and tenants can be mitigated.

Awareness As the privacy of both, owners and inhabitants of smart home properties, can be affected, awareness should be insured in both directions. Inhabitants should be informed in cases other parties install and have access to devices in the property they (permanently or temporarily) live in. Vice versa, landlords might want to be informed in case inhabitants install devices that are in any way intrusive towards their property or person such as, e.g., surveillance devices or devices that are firmly attached to walls or furniture.

Control Likewise, the ability to control can raise conflicts between property owners and inhabitants. For instance, prior work suggested disabling remote access to devices for Airbnb hosts in case guests are currently living in their property [135]. In line with these findings, landlords should not be able to access personal data of their inhabitants, nor to change critical settings of the smart home system. At the same time, inhabitants should not have the power to turn off devices that have been placed for maintenance, security, and sustainability of the property such as, e.g., smart electricity meters or humidity measures. Instead, they could be enabled to, e.g., anonymize or filter collected data according to their privacy preferences.

Authentication Authentication could help to limit access to certain functionality, while at the same time protecting the smart home system from threats. For instance, personal data about inhabitants (e.g., indoor camera feeds) should not be accessible to landlords. However, data that is critical for maintenance of the property could be made accessible to them upon authentication.

Manufacturers & Developers

Manufacturers typically focus on device features rather than privacy and security [12, 232]. Prior research also showed that developers rarely prioritizes on security, unless actively prompted to do so [150, 151], indicating a need to also support developers in privacy and security matters [68, 69, 82]. At the same time, the consequences of developers not ensuring privacy and security are way more broad and unpredictable as compared to a single user employing workarounds (such as, e.g., writing down a password). While we argue to provide end-users with means to protect their privacy and security, it is still an open question if devices could not

implement privacy and security features by default. This includes, but is not limited to, being transparent about data collection and processing policies, as well as providing means to actively consent or otherwise opt out. Future research should look into how to create awareness and understanding among providers and developers of smart home devices and services, and make them implement suitable privacy and security mechanisms, to ultimately empower and protect end-users.

Awareness Device providers tend to focus on functionality and features, while privacy and security are of lower priority [33, 34, 232]. Hence, their awareness of privacy and security implications needs to be increased, to shift their focus towards considering privacy and security at an early development stage.

Control End-users should be enabled to take control over privacy and security settings. As such, manufacturers should provide suitable interfaces that are accessible, easy to use, and enable meaningful control. Moreover, providing secure and privacy-preserving defaults from the manufacturers' side can help protect smart home systems and consumers' privacy.

Authentication Manufacturers should be encouraged to consider the design of suitable mechanisms for the device(s) and purpose at early development stages, rather than post-hoc transferring legacy mechanisms and conventional metaphors (e.g., password entry via unsuitable input modalities).

11.2.2 Further Privacy & Security Mechanisms

Further mechanisms might become necessary to effectively protect users' homes against attacks and threats. These include, but are not limited to, defining access for various roles, and (automatically) detecting potential intrusions.

Access Control

Given the dynamic and complex role system within smart home scenarios (cf. Sections 10.2 and 11.2.1), defining permissions for individuals is challenging. Security experts of our focus group (Section 8.3) suggested approval of sensitive actions by the device owner (e.g, approving food orders on a smart fridge). As a consequence, other stakeholders such as visitors could, e.g., put items in the shopping basket, but not trigger a financial transaction. This thesis also questioned responsibility, and who should be allowed to access which device(s) and functionality in a smart home. In particular, owners should have full control over their smart home system, while other individuals such as guests should only access certain functionality, and potentially only upon authentication (cf. Section 9.2.2).

Interesting questions for future work include investigating the permissions that can and should be associated with the various roles, considering that roles might also change over time (e.g., children growing up, room-mates moving out). Moreover, it will be interesting to look into how these could be employed (or: enforced), especially when it comes to accessing personal data, services associated with devices, and critical device functionalities.

Intrusion Detection

Rather than (or in addition to) forming a "barrier" for legitimate users, the (automatic) detection of attackers can help to further protect users' homes. For instance, a smart home that is, by its sensors, aware of anyone who is currently present, could detect strangers within its own environment. Attackers who try to access the smart home from outside via the network could likewise be detected by the system. As a consequence, the smart home could temporarily shut down sensitive functionality, and inform its owner (especially when they are currently remote) and/or other trusted parties. Future work should look into how intrusion detection can be realized for smart homes, and what the consequences of a detected intrusion are.

11.2.3 Further Application Areas

As technology advances at a rapidly accelerating pace, not only within users' homes, privacy and security becomes relevant in almost all aspects of their daily lives. This includes, but is not limited to, their cars and workplaces, but also semi-public to public spaces like restaurants, train stations, shops, museums or the streets they are walking on their daily way to work. With an increasing number of users working from home during the pandemic [198], work and home environments even blend, opening new challenges for privacy and security. For instance, users are in their home environment that might or might not be protected, while accessing data and systems of their employer. At the same time, it is usually the employers' responsibility to support secure and privacy-preserving behavior among their employees, and enable secure routines [181]. This, however, becomes more challenging with employees being in their personal environments that is beyond the control of a company's security infrastructure. Novel online technologies, from social networks to *Metaverse*, are other examples in which privacy and security are at risk.

While the mechanisms presented in this thesis specifically target – foreign and known, lived-in and visited – smart homes, the general mitigation strategies can be applied in other scenarios as well. For instance, *PriView* can create awareness beyond the home to, e.g., detect surveillance cameras in foreign train stations. This enables users to again take control and, e.g. avoid areas being covered by cameras completely (cf. Section 5.2.2). The *PriKey* could also be carried in many scenarios to communicate users' preferences to devices in their vicinity or to websites to adjust

privacy and security settings online. Novel authentication mechanisms for ubiquitous devices will also increasingly become necessary. The considerations presented in this thesis can serve future research in this direction.

11.3 Closing Remarks

This thesis aims at reclaiming the notion of the home being a place that can be considered secure as well as private. While home devices become more and more sophisticated with valuable functionalities and features, privacy and security are usually not at their focus. As such, these devices make our homes vulnerable to attacks and threats. We investigated how these threats can be mitigated and argued for three essential means: increasing users' awareness, enabling them to take control over privacy and security, and employing usable authentication in daily use. However, these are only first steps towards fully secure and privacy-preserving smart environments, within and beyond the home. Data collection is increasingly ubiquitous and affects an increasing number of stakeholders. This calls for continuous research around usable privacy and security mechanisms, in various contexts, and for the variety of target groups.

VI

Appendix

A

Understanding Privacy Mental Models of Smart Home Inhabitants & Visitors

A.1 Devices for Drawing Exercise

Table A.1 shows the categories and respective devices that we provided for the drawing exercise. Each participant was asked to choose (at least) one of each category to ensure that they consider a whole smart home ecosystem. The participants were allowed to add further entities if they wished so. The table also shows how many participants of each target group (residents, visitors) in our study choose the respective device to explain their understanding of the data flow in a smart home ecosystem.

		Residents	Visitors	Sum
Entertainment Communication	smartphone	8	7	15
	smart assistant	5	3	8
	smart hub	1	0	1
	smart speaker	0	0	0
	smart TV	1	5	6
Energy Management	smart lights	8	7	15
	smart heating	4	3	7
	smart plugs	3	4	7
	smart water meter	0	1	1
	smart electricity meter	0	0	0
Security Safety	smart smoke detector	5	5	10
	smart surveillance	4	3	7
	smart doorbell	2	4	6
	smart lock	2	3	5
	smart window sensor	2	0	2
Health	smart watch	8	12	20
	smart brush	4	1	5
	smart matress	0	2	2
	smart blood pressure	1	0	1
	smart sleep sensor	2	0	2
Home Automation	smart vacuum	6	2	8
	smart jalousie	3	4	7
	smart fridge	3	4	7
	smart thermostat	3	3	6
	smart coffee machine	0	2	2

Table A.1: Overview of Devices: Participants chose one device per category for their mental model drawing.

A.2 Mental Models of the Smart Home Ecosystem

ID	Target Group	Employment Status	Living Situation	Mental Model	ATI	IUIPC Scales Control	Awareness	Collection
PU1	Resident	student	with partner	advanced understanding	5.78	6.33	6.33	4.25
PU2	Resident	student	family	basic understanding	3.67	4.66	3.33	5.50
PU3	Resident	student	with partner	advanced understanding	3.56	6.33	5.33	4.00
PU4	Resident	student	family	basic understanding	4.00	6.66	6.33	5.75
PU5	Resident	student	family	advanced understanding	3.44	6.66	6.33	5.5
PU6	Resident	other	in a flat share	advanced understanding	4.56	6.00	7.00	3.50
PU7	Resident	student	in a flat share	high-level understanding	5.11	5.66	6.00	4.75
PU8	Resident	self-employed	alone	basic understanding	2.00	6.66	6.66	6.00
PU9	Resident	self-employed	alone	basic understanding	2.89	5.66	6.33	5.75
PU10	Resident	student	family	high-level understanding	5.00	6.66	6.66	5.50
PU11	Resident	self-employed	with partner	high-level understanding	4.67	6.33	7.00	5.50
PU12	Resident	employed, self-employed	with partner	high-level understanding	4.67	6.66	5.66	4.75
PU13	Resident	student	in a flat share	schematic simplification	2.56	6.66	7.00	7.00
PU14	Resident	employed	alone	advanced understanding	4.33	6.66	7.00	6.75
PU15	Resident	self-employed	family	schematic simplification	4.67	4.66	6.00	6.75
PB1	Visitor	employed full time	with partner	advanced understanding	4.78	6.00	5.66	5.25
PB2	Visitor	employed full time	alone	advanced understanding	4.11	6.00	7.00	6.25
PB3	Visitor	student	with partner	advanced understanding	4.67	5.33	4.66	4.25
PB4	Visitor	student	with partner	schematic simplification	2.78	6.33	6.33	6.00
PB5	Visitor	student	in a flat share	advanced understanding	3.56	6.00	3.66	4.50
PB6	Visitor	student	with partner	basic understanding	4.56	5.00	4.66	2.50
PB7	Visitor	student	family	advanced understanding	5.56	7.00	6.33	6.50
PB8	Visitor	student	family	schematic simplification	4.33	5.00	6.00	5.75
PB9	Visitor	student	family	basic understanding	5.00	7.00	7.00	6.25
PB10	Visitor	employed full time	with partner	high-level understanding	4.22	7.00	7.00	6.75
PB11	Visitor	student	alone	schematic simplification	4.33	7.00	7.00	6.25
PB12	Visitor	student	family	schematic simplification	3.67	4.00	6.00	3.50
PB13	Visitor	student	family	schematic simplification	4.56	5.33	6.66	4.00
PB14	Visitor	other	alone	basic understanding	4.11	7.00	5.00	6.50
PB15	Visitor	student	in a flat share	advanced understanding	4.67	6.00	7.00	5.75

Table A.2: Distribution of mental models about the smart home ecosystem, ATI scale and IUIPC scales among participants of both target groups, including their employment status and living situation.

A.3 IUIPC

Detailed values for all 10 IUIPC items [134] and all participants of both target groups, residents and visitors.

		Residents		Visitors	
		Mean	SD	Mean	SD
Control	Consumer online privacy is the consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.	6.33	0.72	6.00	1.20
	Consumer control of personal information lies at the heart of consumer privacy.	6.33	0.62	5.93	1.16
	I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.	5.8	1.32	6.06	1.10
Awareness	Companies seeking information online should disclose the way the data are collected, processed, and used.	6.07	1.28	6.13	1.19
	A good consumer online privacy policy should have a clear and conspicuous disclosure.	6.46	1.06	6.13	1.06
	It is very important to me that I am aware and knowledgeable about how my personal information will be used.	6.07	1.16	5.73	1.53
Collection	It usually bothers me when online companies ask me for personal information.	4.87	1.4	5.40	1.40
	When online companies ask me for personal information, I sometimes think twice before providing it.	5.8	1.08	5.33	1.45
	It bothers me to give personal information to so many online companies.	5.47	1.19	5.60	1.45
	I'm concerned that online companies are collecting too much personal information about me.	5.53	1.55	5.00	1.60

Table A.3: Participants' IUIPC ratings (10-item version [134]), for residents and visitors.

A.4 Coding Tree

The bullet points represent the categories of our coding tree. The frequency in the two target groups is given in brackets (N_V: visitors, N_R: residents). Data collection and receiving codes follow the structure <IoT device>-<data>.

- **Perceived Control Entities**
  - Central component mentioned (N_V: 9; N_R: 11)
  - Central component not mentioned (N_V: 4; N_R: 4)
  - Central component (if mentioned, multiple codes per participant possible):
    - Server (N_V: 4; N_R: 4)
    - Cloud (N_V: 2; N_R: 1)
    - Smartphone (N_V: 2; N_R: 5)
    - Smart Watch (N_V: 1; N_R: 0)
    - Tablet (N_V: 1; N_R: 1)
    - Generic / unspecified control device (N_V: 2; N_R: 2)
    - Router (N_V: 1; N_R: 3)
    - User (N_V: 0; N_R: 2)
    - local network (N_V: 0; N_R: 1)
    - smart assistant (N_V: 0; N_R: 1)
- **Perceived Data Collection**
  - No interaction with the device
    - camera-video (N_V: 1; N_R: 0)
    - camera-audio (N_V: 1; N_R: 0)
    - smartphone-data (N_V: 3; N_R: 1)
    - smartphone-video (N_V: 1; N_R: 1)
    - smartphone-audio (N_V: 1; N_R: 1)
    - smartphone-location (N_V: 0; N_R: 1)
    - smartwatch-audio (N_V: 2; N_R: 0)
    - smartwatch-data (N_V: 0; N_R: 4)
    - blood pressure sensor-blood pressure (N_V: 0; N_R: 1)
    - mattress-usage (N_V: 0; N_R: 1)
    - lights-usage (N_V: 0; N_R: 2)
    - doorlock-usage (N_V: 0; N_R: 1)
    - tv-audio (N_V: 2; N_R: 0)
    - fridge-audio (N_V: 2; N_R: 1)
    - fridge-temperature (N_V: 0; N_R: 1)
    - jalousie-data (N_V: 0; N_R: 1)
    - window-data (N_V: 0; N_R: 1)
    - smart assistant-audio (N_V: 2; N_R: 3)
    - thermostat-body temperature (N_V: 1; N_R: 0)
    - thermostat-temperature (N_V: 1; N_R: 3)
    - surveillance system-video (N_V: 2; N_R: 3)
    - smoke detector-status (N_V: 0; N_R: 2)
    - vacuum cleaner-data (N_V: 0; N_R: 2)
    - plug-usage (N_V: 0; N_R: 1)
  - By interaction with the device
    - mattress-data (N_V: 2; N_R: 0)
    - fridge-video (N_V: 2; N_R: 1)
    - fridge-order (N_V: 0; N_R: 1)
    - doorlock-data (N_V: 2; N_R: 1)
    - doorbell-video (N_V: 3; N_R: 1)
    - tv-data (N_V: 5; N_R: 0)
    - smart assistant-audio (N_V: 3; N_R: 3)
    - smartphone-data (N_V: 0; N_R: 3)
    - smartwatch-data (N_V: 5; N_R: 1)
    - vacuum cleaner (N_V: 1; N_R: 0)
    - light-usage (N_V: 3; N_R: 0)
    - plug-data (N_V: 1; N_R: 0)

        - brush-usage (N_V: 0; N_R: 2)
    - Via interaction with other devices
        - light-motion (N_V: 1; N_R: 0)
        - smart meter-energy consumption (N_V: 1; N_R: 0)

- **Perceived Data Receiving**
    - No interaction with the device
        - camera-video (N_V: 1; N_R: 0)
        - camera-audio (N_V: 1; N_R: 0)
        - smartphone-video (N_V: 2; N_R: 0)
        - smartphone-audio (N_V: 2; N_R: 1)
        - smartphone-messages (N_V: 0; N_R: 1)
        - smartwatch-audio (N_V: 1; N_R: 0)
        - smartwatch-messages (N_V: 0; N_R: 1)
        - smartwatch-data (N_V: 0; N_R: 1)
        - fridge-data (N_V: 0; N_R: 1)
        - heater-body temperature (N_V: 1; N_R: 0)
        - heater-temperature (N_V: 0; N_R: 1)
        - smart assistant-audio (N_V: 2; N_R: 0)
        - surveillance system-video (N_V: 3; N_R: 1)
        - thermostat-body temperature (N_V: 1; N_R: 0)
        - vacuum cleaner-data (N_V: 0; N_R: 3)
    - By interaction with the device
        - vacuum cleaner-data (N_V: 1; N_R: 1)
        - smartphone-data (N_V: 0; N_R: 1)
        - smartwatch-audio (N_V: 6; N_R: 0)
        - smartwatch-location (N_V: 0; N_R: 1)
        - mattress-body data (N_V: 2; N_R: 0)
        - fridge-video (N_V: 2; N_R: 0)
        - doorbell-video (N_V: 4; N_R: 0)
        - tv-data (N_V: 3; N_R: 0)
        - smart assistant-audio (N_V: 3; N_R: 2)
        - light-usage (N_V: 2; N_R: 4)
        - thermostat-usage (N_V: 1; N_R: 0)
        - doorbell-video (N_V: 1; N_R: 0)
        - plug-data (N_V: 1; N_R: 0)
        - smoke detector-smoke (N_V: 1; N_R: 0)
        - jalousie-data (N_V: 0; N_R: 1)
        - window-data (N_V: 0; N_R: 1)
    - Via interaction with other devices
        - light-motion (N_V: 1; N_R: 0)
        - smart meter-energy consumption (N_V: 1; N_R: 0)

- **Perceived Storage Location**
    - Local server / Internal Storage (N_V: 4; N_R:4)
    - (External) Cloud (N_V: 3; N_R: 3)
    - Internet / Server (N_V: 0; N_R: 3)
    - IoT Devices (N_V: 5; N_R: 0)
    - Smartphone (N_V: 1; N_R: 1)
    - Provider (N_V: 8; N_R: 7)
    - Apps (N_V: 2; N_R: 0)
    - User (N_V: 1; N_R: 0)
    - Hackers (N_V: 1; N_R: 0)
    - Marketing Companies (N_V:0; N_R: 1)
    - No idea (N_V: 1; N_R: 0)
    - Not mentioned (N_V: 0; N_R: 3)

B

PriView – Exploring Visualizations to Support Users' Privacy Awareness

B.1 Study Part I: Smart Device State Detection using *PriView*

B.1.1 Questionnaire

Intermediate Questions after every search task (i.e., after every visualization) on a 5-point Likert scale:

- I felt comfortable using this visualization.
- This visualization was easy to learn.
- This visualization was understandable.
- Finding the devices was fast.
- I would use this application frequently (if I had access to a thermal camera).

B.1.2 Interview Guide

Interview after the first part of the study:

- How was your experience?
- Would an application like this one be useful for you?
- Where would you use such an application? [e.g., Friend's house, Parent's House, Airbnb, Other]
- How frequently would you use this application? [E.g. every time you visit a place, first time visiting a place, when suspecting a place, . . .]
- Why would you use such an application? For which purpose?
- Which representation did you like most? Why?
- Would you like a combination of representations? Why?
- How much Information would you like to see? Might this be different per device? Further factors?
- Did the application assist you in finding the devices or did you find them yourself?
- Do you think the application would find devices you wouldn't?
- Does having access to such an application make you feel safer?
- Does it support you to protect your privacy?
- How did you feel using this application?
- How would you feel if someone around you is using this application (e.g., at your place)?
- What did you (not) like about the application?
- What suggestions or options could be added to the future?
- Do you have any further insights to share?

B.2 Study Part II: *PriView* in VR

B.2.1 Scenarios

S1: Train Station Imagine you are on vacation and this is a train station that you have never been to before in a foreign, far away country. This place tends to be crowded, so many other people might be present as well.

S2: Museum Imagine you are in this museum that you have never been to before. Other visitors might be present as well. There might be interactive exhibits that include some form of sensors.

S3: Rental apartment (bedroom) Imagine you are on vacation and this is an apartment that you rented via AirBnB or any other platform. You have never been here before. You rented the whole apartment for you and whomever is travelling with you. You do not know the host.

S4: A friend's place (living room) Imagine this is the place of a good friend of yours. You visit this place frequently and thus know it very well. This friend recently bought smart home devices.

S5: A shared/office kitchen Imagine this is the kitchen in your office. You spent valuable coffee or tea time here during long work days. You know all people that come here as they are your colleagues. This includes your boss.

S6: Way to work (a public place and/or road) Imagine this is your daily way to work, so you know this place very well. It is a public road, so other (foreign) people, cars, bikes might be present as well.

B.2.2 Questionnaire

Intermediate Questions Intermediate Questions after every scene:

- Overall, I felt comfortable using this application. [5-point Likert scale]
- I would use this application frequently in this scenario (if I had access to AR glasses). [5-point Likert scale]
- Which visualization did you like best in this scenario? Please rank all visualizations (use drag and drop) according to your preference in this scene, from most preferred (1) to least preferred (5).

Final Questions At the end of the session, for every visualization (we provided screenshots for recap):

- This visualization was easy to learn. [5-point Likert scale]
- This visualization was understandable. [5-point Likert scale]

B.2.3 Interview Guide

Interview after the first part of the study:

- How was your experience?
- Would an application like this one be useful for you?
- Where would you use such an application? [e.g., Friend's house, Parent's House, Airbnb, Other]
- For which purpose would you use such an application?
- How frequently would you use this application? [E.g. every time you visit a place, first time visiting a place, when suspecting a place, . . .]
- When would you like to see the visualizations? e.g., on demand, permanently (like now), only on change, only when you are close to a source of tracking, . . .
- How much Information would you like to see? Might this be different per device? Might this be different depending on the location? Further factors?
- Which representation did you like most overall? If there is an overall, otherwise maybe specifically? Why?
- Would you like to rather have a combination of visualizations?
- What else could you imagine?
- Does having access to such an application make you feel safer?
- Does it support you to protect your privacy?
- How did you feel using this application?
- How would you feel if someone around you is using this application (e.g., at your place) ?
- What did you (not) like about the application?
- What suggestions or options could be added to the future?
- Comparing the mobile application and the VR / glasses version, which one would you prefer (think about integrated prototypes)? Why?
- Any further insights to share?

B.3 Code Book

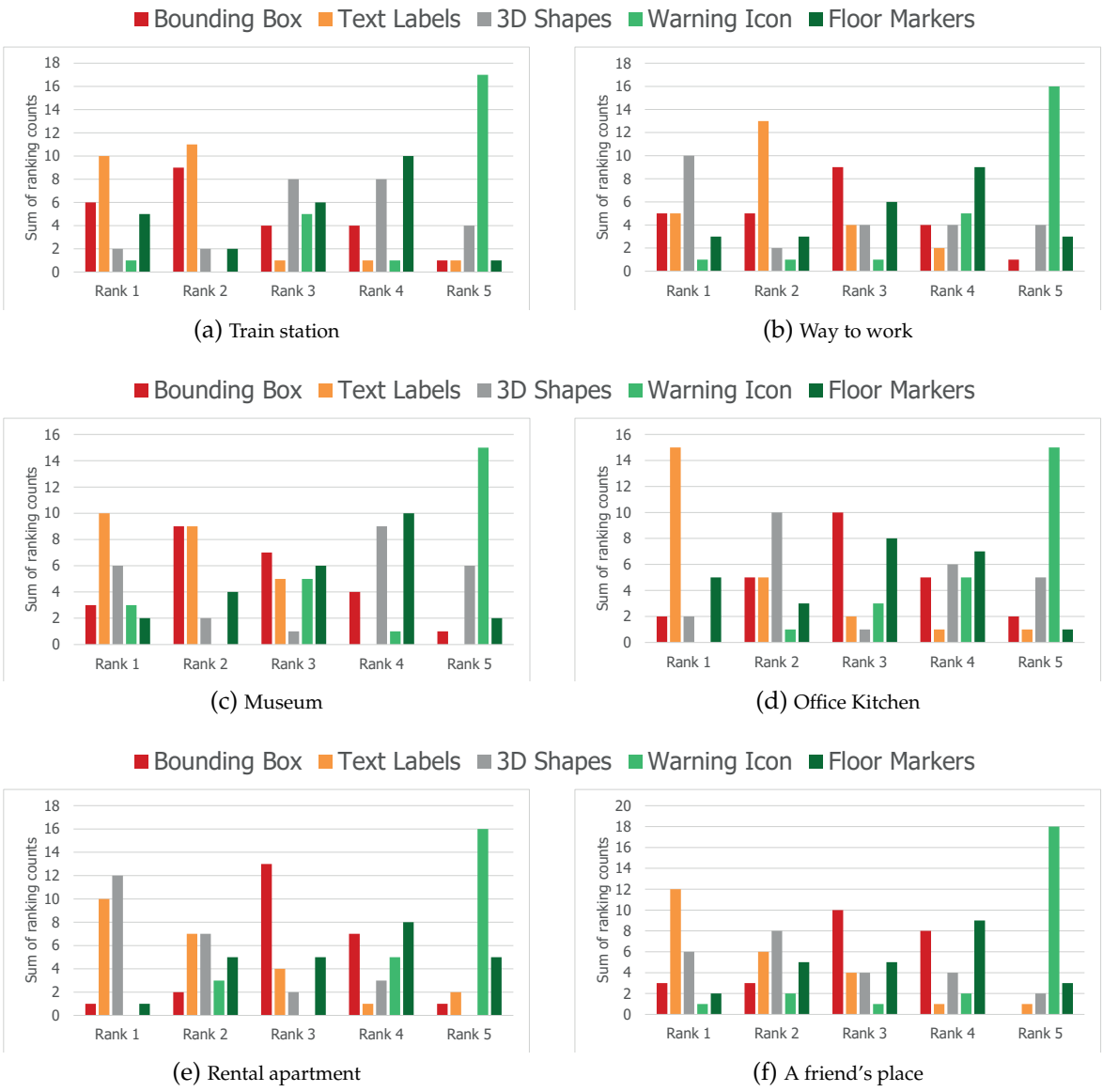
Final coding tree for the thematic analysis:

- Found Devices – Baseline
- Found Devices – Mobile Application
- General Feedback
    - Mobile Application
        - Positive
        - Negative
        - Suggestion for Improvement
    - Head-Mounted Display
        - Positive
        - Negative
        - Suggestion for Improvement
- Usefulness
    - Frequency (of visited place)
        - Once
        - Every time
    - Overtime (e.g., learnability or redundancy)
        - Floor Markers
            - Understood
            - Not understood
        - Bounding Boxes
            - Understood
            - Not understood
        - Warning Icon

        - Understood
        - Not understood
    - Text Labels
        - Understood
        - Not understood
    - 3D Shapes
        - Understood
        - Not understood
- Usage
    - Potential Use Cases
        - Finding Devices
        - Awareness
    - Location
        - Familiarity
        - Space (i.e., private vs public)
        - Trusted
    - Context
        - Redundancy
- Privacy
    - Self
    - Other
        - Comfort
        - Acceptance
        - Social Trust

- Preference
    - Interaction Modality
        - Activation Methods
            - Notification for Updates
            - Always on
            - Button
            - Nested
    - Form Factor
        - Why
    - Visualization
        - Why
            - Distraction
            - Quick Overview
            - Easy to Understand
            - Information Level (level of detail)
              More information | Less information
        - Suggestion for Improvement
        - Context
        - Location

B.4 Ranking of Visualizations per Scenario



(a) Train station

(b) Way to work

(c) Museum

(d) Office Kitchen

(e) Rental apartment

(f) A friend's place

Figure B.1: Study Part II (using *PriView* in an HMD in various scenes): Detailed ranking of visualizations per scene, i.e. sum of count of rank positions per scene.

C

PriKey – Enabling Privacy Control for Visitors

C.1 Smart Home Scenarios

Inhabitants Group Please imagine that you live with a friend in a shared flat.

1) Primary User: You recently bought 12 new SH devices. Today, you installed them in all rooms of your home. Now, you just finished. You are currently alone at home.

2) Co-Inhabitant: Imagine that your friend recently bought 12 SH devices. Your friend just installed them in all rooms of your shared home. You were not involved in the decision-making process, but you are allowed to use the devices if you want to. Your friend is there with you.

Visitors Group

3) Visitor in familiar environment: Please imagine you are visiting a friend in their home. This friend recently installed 12 SH devices in all rooms. You are just arriving at your friend's flat. Your friend is there with you.

4) Visitor in unfamiliar environment: Please imagine you rented an apartment for a weekend-trip. You just arrived and noticed that it has 12 SH devices installed in all rooms. You are alone in the apartment.

Tasks/Rooms Alternatives for scenario the *visitor in a familiar environment* are included in parentheses.

Living Room: Imagine you enter the living room to sit down and call a good friend on your phone (talk with your friend). You just want to get up to date with each other's lives.

Bathroom: Imagine you have to use the bathroom now. So you finish your phone-call (conversation) and go to the bathroom.

Kitchen: Imagine that you are getting hungry. You go to the kitchen (with your friend), prepare dinner (together) and have it there.

Bedroom: Imagine that, while talking with your friend, you remembered a dear memory. You want to look at some photos of this occasion on the PC, which is situated in your (friend's) bedroom.

C.2 Participants' Demographics

ID	age	gender	occupation	living situation	owned device	knows owner	used device	IUIPC control	IUIPC collection	IUIPC awareness
1	23	female	student	parents / siblings	no	yes	no	6,00	5.33	3.00
2	21	male	student	parents / siblings	yes	no	yes	6,33	7.00	6.50
3	21	male	student	alone	yes	yes	yes	6,33	3.67	5.25
4	20	male	student	parents / siblings	no	yes	yes	7,00	4.33	2.00
5	22	male	student	shared flat	yes	yes	yes	6.33	6.33	5.50
6	23	male	student	parents / siblings	yes	yes	yes	5.67	6.33	2.50
7	26	female	student	alone	yes	yes	yes	6.00	6.00	7.00
8	66	male	retired	partner / children	yes	yes	yes	7.00	7.00	7.00
9	20	male	student	parents / siblings	no	yes	yes	5.33	6.33	6.25
10	28	female	student	shared flat	no	yes	yes	7.00	6.67	5.25
11	20	female	student	shared flat	no	no	no	7.00	7.00	6.75
12	22	female	student	partner / children	no	yes	yes	6.00	7.00	7.00
13	62	female	retired	partner / children	no	no	no	4.33	7.00	7.00
14	57	female	employed	partner / children	no	no	no	5.67	6.67	6.50
15	55	female	employed	alone	yes	yes	yes	6.00	7.00	5.25
16	45	male	self-employed	partner / children	no	yes	no	7.00	7.00	7.00

Table C.1: Participants of our Exploratory User Study: demographics, previous experiences with smart homes and detailed results for control, collection and awareness using the IUIPC scale [134].

C.3 Codebook

Participants' Previous Experiences and Knowledge:

Category	Code	Description	count
Knowledge on Smart Homes	knowledge_remote_control	remote control of SH devices	7
	knowledge_assistance	SH assist their users	5
	knowledge_intelligence_automation	SH are intelligent/automated	4
	knowledge_control	allows to control devices	14
	knowledge_smartphone_app	done via app	12
	knowledge_smart_speaker	involves a smart speaker	11
	knowledge_entertainment	knows entertainment device	5
	knowledge_energy_automation	knows energy/automation devices (e.g., plug, thermostats, light)	11
	knowledge_surveillance	knows surveillance devices (e.g., camera)	5
	knowledge_health_care	knows health care devices (e.g., scale)	1
Experience with Devices	prior_used_no_device	never used a SH device	8
	prior_used_device	used SH devices before	11
	prior_owns_device	owns SH devices	9
Privacy in Smart Homes	privacy_concern	is concerned about own privacy in SHs	13
	privacy_disclosure_lack	perceived lack of disclosure on privacy invasion	4
	privacy_feels_observed	feels observed in SHs	8
	privacy_personality_dependent	perceived importance of privacy depends on personality	7
	privacy_unauthorized_access	stored data could be accessed by an unauthorized party	4
	privacy_mistrust_provider	mistrust in provider of SH	4
	privacy_not_purchased_removed	did not buy a SH device or removed one because of privacy	6

$RQ_{CO}2.a$ – Adoption:

Category	Code	Description	count
Adoption	adoption_inhabitant_no_use	would not use *PriKey* as a inhabitant	4
	adoption_inhabitant_use	would use *PriKey* as a inhabitant or at least try it out	13
	adoption_visitor_use	would use *PriKey* as a visitor or at least try it out	15
Feedback on Concept	concept_privacy_choice_important	important to enable persons to enforce privacy choices	14
	concept_visitor_benefit	especially visitors benefit from *PriKey*	8
	concept_intuitive	is easy to use / intuitive	5
	concept_fast	is fast to use	3
	concept_proactive	provides information/control proactively	3
	concept_increases_awareness	increases awareness/provides information	7
	concept_provides_control	enables control on privacy choices	9
	concept_potential_conflicts	cause conflicts between multiple users choices/needs	6
	concept_device_centric_control	mentioned/expected device centric aproach	8
	concept_threat_prikey	unauthorized access to *PriKey* could impose a threat	4
	concept_presence_location	confuses presence with location	10
	concept_social_mitigation	would first communicate choices to primary owner	2
Trustworthiness	preference_prikey_trust	*PriKey* is more trusted	2
	concept_mistrust_prikey	expressed some mistrust in correct operation	4
Use Cases	usecase_work	workplace as further use case	3
	usecase_doctor	usecase at the physician/doctor	2
	usecase_hotel	usecase in a hotel	4
	usecase_public	public spaces as further use case	7
	usecase_increase_awareness	increasing awareness everywhere	1
	usecase_limited_control	control everywhere would be limited	7
	usecase_everywhere	would want to use it everywhere	4
	targetgroup_older_adults	could be useful for older adults	1
	usecase_future	use case is in the future	6
	targetgroup_high_risk	persons exposed to greater risks	1
	usecase_privacy	protecting ones privacy in different scenarios	10
	usecase_foreign	visiting a foreign household	3

RQ_{CO}2.b – Individuals Needs:

Category	Code	Description	count
Privacy Choices	on_convenience	devices on due to convenience	3
	on_needed	on as device might be needed	9
	on_anyway_shared	on as data is collected anyway	3
	on_concern_lack	left on as user is not concerned	9
	off_privacy	off to preserve privacy	15
	off_not_needed	off as device is not needed	6
	all_off_convenience	all off button as it is convenient	3
Sensor Dependent	consideration_sensor_video_concern	especially concerned about video footage	12
	consideration_sensor_audio_concern	especially concerned about audio recordings	8
	consideration_sensor_presence_no_concern	not/very little concerned about presence sensing	4
Device Dependent	consideration_device_utility	mentioned/asked about utility of device	10
	consideration_device_functionality	mentioned/asked about basic functionalities (e.g., light)	8
	consideration_device_smart_speaker	especially concerned about smart speakers	6
Role Dependent	consideration_primary_user_access	only primary user of the device can access the data	6
	consideration_primary_user_functionality_important	correct functionality is most important for primary user	2
	consideration_primary_user_trust	depends on trust towards the SH primary_user	8
	consideration_primary_user_configuration	primary users can configure their choices beforehands	4
	consideration_primary_user_consent	primary user consented by purchasing / installing	3
Room/Task Dependent	consideration_bath_no_video	would not install/want a camera in the bathroom	11
	consideration_bath_no_audio	would not install/want a microphone in the bathroom	4
	consideration_bath_intimate	bathroom is perceived as an intimate environment	5
	consideration_bed_no_video	would not install/want a camera in the bedroom	2
	consideration_bed_role_dependent	no devices another person installed in the bedroom	2
	consideration_bed_intimate	bedroom is perceived as an intimate environment	4
	consideration_kitchen_not_intimate	tasks in kitchen perceived as not sensitive	6
	consideration_living_eavesdrop	conversation in living room could be recorded	10
	consideration_bed_task	depends on task of bedroom	6
	consideration_bed_photos	considers protecting photos visible on screen	3
Comparison to App	preference_app	prefers app	8
	preference_prikey	prefers *PriKey*	5
	preference_test_both	would try both app and key and then decide	3
	preference_prikey_direct	*PriKey* is more direct/ready-to-hand compared to an app	4
	preference_prikey_reminds	*PriKey* reminds user to think about privacy	1
	preference_app_no_extra_device	no extra device necessary for smartphone app	8
	preference_app_near	smartphone is always nearby	6

D

Design Considerations for Usable Authentication in Smart Homes

D.1 User Interviews: Story Completion Guide

Tim and Lara are a couple, recently having moved together in a common house. Lately, they saw many advertisements on, e.g., Amazon Alexa, electronic door locks, smart cameras, Internet-connected fridges, app-controlled washing machines, smart lights, Internet-connected audio systems, smart TVs, Internet-connected alarm clocks, sensor-equipped microwaves, hoover robots, and many more. Tim and Lara know, that any device exists with many interaction modalities and features.

Please imagine a future scenario in which any imaginable device exists.

A. Appliances and Reasons After both did some research on smart devices, Tim and Lara are now interested in getting one for their new home. However, they are not quite sure which type of device(s) to choose, as many – e.g., security or entertainment devices – promise benefits for daily life. They decide to no longer delay the purchase. What happens next? Please describe the scenario. Include Tim's and Lara's reasons for their choice, and what they expect from the device. Consider that they will probably use the device regularly.

Note: following parts of the story were based on the <*smart device*> that was chosen.

B. Functionality, Setup & Interaction A few days later, the <*smart device*> arrives and Tim and Lara want to try out all functionality. What happens next? How is the device's setup process and what functionality does <*smart device*> provide? How can both interact with the <*smart device*>?

C. Authentication Mechanisms Tim and Lara are aware that smart devices collect and store personal information. Thus, they want to make sure that illegitimate users to not have access to their account. The <*smart device*> can meet this requirement. How could an authentication mechanism look like, that is more than a one-time login, but does not require user input on each and every device use?

D. Problems & Concerns of Shared Use

D.1. Couple After a few weeks, Tim and Lara realize that shared use of a smart device can lead to problems. Which problems could that be, and how could future solutions look like?

D.2. Children Lara's sister is visiting every month, together with her children (3 and 5 years old). As they see the <*smart device*>, they want to play around with it. While Lara is busy talking with her sister, Tim is concerned as he is not sure about consequences of using the <*smart device*> for the children.

Please describe (potentially harmful) consequences in this scenario and include potential countermeasures.

D.3. Worried Guest Tim and Lara have a worried guest. This guest is convinced, that any Internet-connected device is used for surveillance by, e.g., secret service or marketing companies.

How can Tim and Lara convince their guest to feel more safe, i.e., that their home is still a safe place? What requirements would the <*smart device*> need to fulfil (e.g., an option to turn off the microphone)?

D.2 Expert Focus Group: Protocol

1. **Threats in Smart Homes**
   - **a)** Think about 5 threats and rank them in order of priority.
   - **b)** How can this threat be automatically recognized?
2. **Data Tracking, Transparency and Management**
   - **a)** From a scale from 1-7 (1=not at all) how much do you agree with this phrase?
     "It is not tracked when I put the smart device in the freezer." [provided on a paper sheet]
   - **b)** How can we increase awareness of what is tracked when and how (e.g., by means of a visualization)?
     Think about 3 solutions.
   - **c)** From a scale from 1-7 (1=not at all) how much do you agree with this phrase?
     "When guests enter my smart home, they loose the right to their data." [provided on a paper sheet]
   - **d)** How can we share data that is tracked from guests with them?

3. Privacy and Societal Goals

a) Which of the following smart devices are more *privacy intrusive*? Think about, e.g., which data these devices can access. Rank them on a scale from 1 to 4, 1=least intrusive.

- smart hoover
- smart fridge
- smart light
- smart voice assistant

I do not think it is possible to rank them. Why?

b) Which *factors* would you consider when designing an authentication mechanism for smart devices? Think about 5 factors.
e.g., one central authentication system vs. individual ones for each smart device? e.g., consider context?

4. Authentication Mechanisms
There are three user groups (owner, adult household members, children, guests) and three smart devices (smart fridge, smart voice assistant, smart coffee machine). Let us think about one authentication method for each smart device that can be shared with each group.

D.3 Codes for Qualitative Analysis

A Appliances and Reasons

- Appliances
  - Household
    - vacuum cleaner robot (7)
    - fridge (5)
    - washing machine (4)
    - light (2)
    - heater (1)
    - coffee machine (1)
    - dishwasher (1)
  - Entertainment
    - Alexa (6)
    - TV (1)
  - Control
    - smart hub (3)
  - Security
    - camera (1)
    - door lock (1)
- Factors of Influence
  - comfort
  - chores
  - internet access
  - central control
  - automation
  - showing off
  - easy installation
  - safe energy

B Functionality, Setup & Interaction

- Features
  - Device Features
    - It is always on
    - photo album
    - self programming what it can do
    - efficient
    - scanner checks content
  - Use Cases
    - mange shopping / orders / delivery
    - automation
    - (vacuum) clean
    - change lights
    - lawnmower
    - play music
    - waterproof
    - indoor and outdoor use
    - create and change profiles
    - personal settings / individual programming
    - play music
    - <not mentioned>
- Setup
  - Establish connection

        - connect with other devices
        - connect to Wi-Fi
        - connect
        - enter Wi-Fi Password
        - internet connection
        - connect with all accounts
    - Authentication
        - automatic authentication depending on other devices
        - two-factor authentication
        - enter login data
    - start the device / first steps
        - plug in
        - unpack
        - turn on
        - download companion app
        - device training time
        - employ light bulb
    - try out / learn device
        - try it out
        - read manual
        - learning by doing
        - watch a video
        - plug and play
    - others
        - sensors
- Interaction Modalities
    - app / smartphone
    - voice commands
    - touch
    - via voice assistant / Alexa
    - 3rd person/friend
    - remote control
    - high importance/dependence
    - via a display
    - none (completely automated)
    - indirect
    - directly with the coffee machine
    - fingerprint
    - face recognition

C Authentication Mechanisms

- fingerprint (11)
- face recognition/scan (6)
- voice commands / recognition (6)
- login via smartphone / companion app (3)
- PIN (3)
- two-factor authentication over mobile phone (1)
- camera (1)
- connection to Wi-Fi (1)
- door handle (1)
- password (1)
- location dependent authentication with mobile phone (1)
- locks device from being accessed (fridge) for a few min (1)
- only authenticate once upon installation (1)
- token / proximity based (1)

D Problems & Concerns of Shared Use

- Shared Devices
    - (varying) preferences
    - interfering commands
    - voice recognition failures within family
    - responsibility
    - children
        - children may get hurt
        - device may be damaged
        - other/miscellaneous problems
    - Visitors
        - dislike
        - disagree
- other/miscellaneous problems
- Data
    - data leakage to co-living partners
    - knowing when the device is on/off or saving data
- Technology / Device related

E

Exploring Usable Authentication for Smart Home Visitors

E.1 Exploratory Study Results

E.1.1 Results

(a) When did you first meet the smart home owner?

(b) In which city did the both of you meet the first time?

(c) Which hobby do you have in common?

(d) What binds you two together?

(e) How many smart home devices do you own together?

(f) What was your first activity together?

(g) Where did you meet last time?

(h) Which restaurant have you visited most together?

(i) What was the furthest place you have been to together?

Figure E.1: Exploratory Study Results: Detailed plots for the Likert items referring to every security question in the categories easy (a-c), medium (d-f), and hard (g-i).

VII

Bibliography

FULL LIST OF CO-AUTHORED PUBLICATIONS

2022

1. Sarah Delgado Rodriguez, **Sarah Prange**, Christina Vergara Ossenberg, Markus Henkel, Florian Alt, and Karola Marky. 2022. *PriKey* – Investigating Tangible Privacy Control for Smart Home Inhabitants and Visitors. In *Nordic Human-Computer Interaction Conference (NordiCHI '22)*. ACM, New York, NY, USA, Article 74, 1–13. https://doi.org/10.1145/3546155.3546640

2. **Sarah Prange**, Niklas Thiem, Michael Fröhlich, and Florian Alt. 2022. "Secure settings are quick and easy!" – Motivating End-Users to Choose Secure Smart Home Configurations. 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/10.1145/3531073.3531089

3. **Sarah Prange**, Sarah Delgado Rodriguez, Timo Döding, and Florian Alt. 2022. "Where did you first meet the owner?" – Exploring Usable Authentication for Smart Home Visitors. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '22 Extended Abstracts), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3491101.3519777

4. Vera Volk, **Sarah Prange**, and Florian Alt. 2022. *PriCheck*– An Online Privacy Assistant for Smart Device Purchases. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '22 Extended Abstracts), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3491101.3519827

2021

5. Rivu Radiah, Ville Mäkelä, **Sarah Prange**, Sarah Delgado Rodriguez, Robin Piening, Yumeng Zhou, Kay Köhle, Ken Pfeuffer, Yomna Abdelrahman, Matthias Hoppe, Albrecht Schmidt, and Florian Alt. 2021. Remote VR Studies: A Framework for Running Virtual Reality Studies Remotely Via Participant-Owned HMDs. In *ACM Trans. Comput.-Hum. Interact.* 28, 6, Article 46 (December 2021), 36 pages. https://doi.org/10.1145/3472617

6. Karola Marky, **Sarah Prange**, Max Mühlhäuser, and Florian Alt. 2021. Roles Matter! Understanding Differences in the Privacy Mental Models of Smart Home Visitors and Residents. In *20th International Conference on Mobile and Ubiquitous Multimedia (MUM 2021), December 5–8, 2021, Leuven, Belgium.* ACM, New York, NY, USA, 15 pages. **Honorable Mention Award.** https://doi.org/10.1145/3490632.3490664

7. **Sarah Prange**, Ceenu George, and Florian Alt. 2021. Design Considerations for Usable Authentication in Smart Homes. In *Mensch und Computer '21, September 05–08, Ingolstadt, Germany.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/1122445.1122456

8. Sarah Delgado Rodriguez, **Sarah Prange**, and Florian Alt. 2021. Take Your Security and Privacy Into Your Own Hands! Why Security and Privacy Assistants Should be Tangible. In: *Wienrich, C., Wintersberger, P. & Weyers, B. (Hrsg.), Mensch und Computer 2021 - Workshopband*. Bonn: Gesellschaft für Informatik e.V.. https://doi.org/10.18420/muc2021-mci-ws09-393

9. **Sarah Prange**, Sven Mayer, Maria-Lena Bittl, Mariam Hassib, and Florian Alt. 2021. Investigating User Perceptions Towards Wearable Mobile Electromyography. In: *Human-Computer Interaction – INTERACT 2021. INTERACT 2021.* Lecture Notes in Computer Science, vol 12935. Springer, Cham. https://doi.org/10.1007/978-3-030-85610-6_20

10. Robin Piening, Ken Pfeuffer, Augusto Esteves, Tim Mittermeier, **Sarah Prange**, Philippe Schröder, and Florian Alt. 2021. Looking for Info: Evaluation of Gaze Based Information Retrieval in Augmented Reality. In: *Human-Computer Interaction – INTERACT 2021. INTERACT 2021.* Lecture Notes in Computer Science, vol 12932. Springer, Cham. https://doi.org/10.1007/978-3-030-85623-6_32

11. **Sarah Prange**, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. 2021. *PriView* – Exploring Visualisations to Support Users' Privacy Awareness. In *CHI Conference on Human Factors in Computing Systems (CHI'21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3411764.3445067

12. Leon Müller, Ken Pfeuffer, Jan Gugenheimer, Bastian Pfleging, **Sarah Prange**, and Florian Alt. 2021. SpatialProto: Exploring Real-World Motion Captures for Rapid Prototyping of Interactive Mixed Reality. In *CHI Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3411764.3445560

13. Sarah Delgado Rodriguez, **Sarah Prange**, Lukas Mecke, and Florian Alt. 2021. ActPad– A Smart Desk Platform to Enable User Interaction with IoT Devices.

In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '21 Extended Abstracts), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3411763.3451825

14. **Sarah Prange**, Karola Marky, and Florian Alt. 2021. Usable Authentication in Multi-Device Ecosystems. In *CHI 2021 Workshop on User Experience for Multi-Device Ecosystems: Challenges and Opportunities*. ACM, New York, NY, USA, 3 pages. https://www.unibw.de/usable-security-and-privacy/publikationen/pdf/prange2021ux4mde.pdf

2020

15. Karola Marky, **Sarah Prange**, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You just can't know about everything": Privacy Perceptions of Smart Home Visitors. In *19th International Conference on Mobile and Ubiquitous Multimedia (MUM 2020), November 22–25, 2020, Essen, Germany.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3428361.3428464

16. **Sarah Prange**, Lukas Mecke, Alice Nguyen, Mohamed Khamis, and Florian Alt. 2020. Don't Use Fingerprint, it's Raining! How People Use and Perceive Context-Aware Selection of Mobile Authentication. In *International Conference on Advanced Visual Interfaces (AVI '20), September 28-October 2, 2020, Salerno, Italy.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3399715.3399823

17. **Sarah Prange** and Florian Alt. 2020. I Wish You Were Smart(er): Investigating Users' Desires and Needs Towards Home Appliances. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (*CHI EA '20*). Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/3334480.3382910

18. **Sarah Prange** and Florian Alt. 2020. Interact2Authenticate: Towards Usable Authentication in Smart Environments. In *Proceedings of the 1st CHI Workshop on Authentication Beyond Desktops and Smartphones (WABDS '20)*. https://www.unibw.de/usable-security-and-privacy/publikationen/pdf/prange2020wabds.pdf

19. Yasmeen Abdrabou, **Sarah Prange**, Lukas Mecke, Ken Pfeuffer, and Florian Alt. 2020. VolumePatterns: Using Hardware Buttons beyond Volume Control on Mobile Devices. In *Proceedings of the 1st CHI Workshop on Authentication Beyond Desktops and Smartphones (WABDS '20)*. https://www.unibw.de/usable-security-and-privacy/publikationen/pdf/abdrabou2020wabds.pdf

2019

20. **Sarah Prange**, Lukas Mecke, Michael Stadler, Maximilian Balluff, Mohamed Khamis, and Florian Alt. 2019. Securing Personal Items in Public Space: Stories of Attacks and Threats. In *Proceedings of the 18th International Conference on Mobile and Ubiquitous Multimedia* (*MUM '19*). Association for Computing Machinery, New York, NY, USA, Article 27, 1–8. https://doi.org/10.1145/3365610.3365628

21. Lukas Mecke, Sarah Delgado Rodriguez, Daniel Buschek, **Sarah Prange**, and Florian Alt. 2019. Communicating Device Confidence Level and Upcoming Re-authentications in Continuous Authentication Systems on Mobile Devices. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (*SOUPS '19*). USENIX Association, USA, 289–301. https://www.usenix.org/system/files/soups2019-mecke_confidence.pdf

22. Lukas Mecke, Daniel Buschek, Mathias Kiermeier, **Sarah Prange**, and Florian Alt. 2019. Exploring Intentional Behaviour Modifications for Password Typing on Mobile Touchscreen Devices. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (*SOUPS '19*). USENIX Association, USA, 303–318. https://www.usenix.org/system/files/soups2019-mecke_behaviour.pdf

23. **Sarah Prange**, Yasmeen Abdrabou, Lukas Mecke and Florian Alt. 2019. Hidden in Plain Sight: Using Lockscreen Content for Authentication on Mobile Devices. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (*SOUPS '19*). USENIX Association, USA. https://www.unibw.de/usable-security-and-privacy-en/team/usablesecurity-and-privacy/publikationen/pdf/prange2019soupsadj.pdf

24. Ken Pfeuffer, Matthias J. Geiger, **Sarah Prange**, Lukas Mecke, Daniel Buschek, and Florian Alt. 2019. Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (*CHI '19*). Association for Computing Machinery, New York, NY, USA, Paper 110, 1–12. https://doi.org/10.1145/3290605.3300340

25. **Sarah Prange**, Christian Tiefenau, Emanuel von Zezschwitz, and Florian Alt. 2019. Towards Understanding User Interaction in Future Smart Homes. In *Proceedings of CHI '19 Workshop on New Directions for the IoT: Automate, Share, Build, and Care (Glasgow, UK) (CHI '19 Workshop)*. ACM, New York, NY, USA, 5 pages. https://www.unibw.de/usable-security-and-privacy/publikationen/pdf/prange2019iot.pdf

26. **Sarah Prange**, Daniel Buschek, Ken Pfeuffer, Lukas Mecke, Peter Ehrich, Jens Le, and Florian Alt. 2019. Go for GOLD: Investigating User Behaviour in Goal-Oriented Tasks. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (*CHI EA '19*). Association for Computing Machinery, New York, NY, USA, Paper LBW0256, 1–6. https://doi.org/10.1145/3290607.3312949

2018

27. **Sarah Prange**, Daniel Buschek, and Florian Alt. 2018. An Exploratory Study on Correlations of Hand Size and Mobile Touch Interactions. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia* (*MUM 2018*). Association for Computing Machinery, New York, NY, USA, 279–283. https://doi.org/10.1145/3282894.3282924

28. Ludwig Trotter, **Sarah Prange**, Mohamed Khamis, Nigel Davies, and Florian Alt. 2018. Design Considerations for Secure and Usable Authentication on Situated Displays. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia* (*MUM 2018*). Association for Computing Machinery, New York, NY, USA, 483–490. https://doi.org/10.1145/3282894.3289743

29. Lukas Mecke, **Sarah Prange**, Daniel Buschek, Mohamed Khamis, Mariam Hassib, and Florian Alt. 2018. "Outsourcing Security": Supporting People to Support Older Adults. In *Proceedings of the Mobile HCI '18 Workshop on Mobile Privacy and Security for an Aging Population*. https://www.unibw.de/usable-security-and-privacy/publikationen/pdf/mecke2018mobilehciadj.pdf

30. Daniel Buschek, Sarah Völkel, Clemens Stachl, Lukas Mecke, **Sarah Prange**, and Ken Pfeuffer. 2018. Experience Sampling as Information Transmission: Perspective and Implications. In *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers* (*UbiComp '18*). Association for Computing Machinery, New York, NY, USA, 606–611. https://doi.org/10.1145/3267305.3267543

31. Lukas Mecke, Ken Pfeuffer, **Sarah Prange**, and Florian Alt. 2018. Open Sesame! User Perception of Physical, Biometric, and Behavioural Authentication Concepts to Open Doors. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia* (*MUM 2018*). Association for Computing Machinery, New York, NY, USA, 153–159. https://doi.org/10.1145/3282894.3282923

32. Lukas Mecke, **Sarah Prange**, Daniel Buschek, and Florian Alt. 2018. A Design Space for Security Indicators for Behavioural Biometrics on Mobile Touchscreen Devices. In *Extended Abstracts of the 2018 CHI Con-*

ference on Human Factors in Computing Systems (*CHI EA '18*). Association for Computing Machinery, New York, NY, USA, Paper LBW003, 1–6. https://doi.org/10.1145/3170427.3188633

2017

33. **Sarah Prange**, Victoria Müller, Daniel Buschek, and Florian Alt. 2017. QuakeQuiz - A Case Study on Deploying a Playful Display Application in a Museum Context. In *Proceedings of the 16th International Conference on Mobile and Ubiquitous Multimedia* (*MUM '17*). Association for Computing Machinery, New York, NY, USA, 49–56. https://doi.org/10.1145/3152832.3152841

REFERENCES

[1] 2008. *Central Limit Theorem*. Springer New York, New York, NY, 66–68. DOI: http://dx.doi.org/10.1007/978-0-387-32833-1_50

[2] Yomna Abdelrahman, Paweł W. Woźniak, Pascal Knierim, Dominik Weber, Ken Pfeuffer, Niels Henze, Albrecht Schmidt, and Florian Alt. 2019. Exploring the Domestication of Thermal Imaging. In *Proceedings of the 18th International Conference on Mobile and Ubiquitous Multimedia (MUM '19)*. Presented in Pisa, Italy. Association for Computing Machinery, New York, NY, USA, Article 9, 7 pages. DOI:http://dx.doi.org/10.1145/3365610.3365648

[3] Noura Abdi, Kopo M. Ramokapane, and Jose M. Such. 2019. More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS '19)*. USENIX Association, Berkeley, CA, USA, 1–16.

[4] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Comput. Surv.* 50, 3, Article 44 (aug 2017), 41 pages. DOI:http://dx.doi.org/10.1145/3054926

[5] Anne Adams. 2000. Multimedia Information Changes the Whole Privacy Ballgame. In *Proceedings of the Tenth Conference on Computers, Freedom and Privacy: Challenging the Assumptions (CFP '00)*. Presented in Toronto, Ontario, Canada. Association for Computing Machinery, New York, NY, USA, 25–32. DOI: http://dx.doi.org/10.1145/332186.332199

[6] Anne Adams and Martina Angela Sasse. 1999. Users Are Not the Enemy. *Commun. ACM* 42, 12 (dec 1999), 40–46. DOI:http://dx.doi.org/10.1145/322796.322806

[7] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2020. Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW2, Article 116 (Oct. 2020), 28 pages. DOI: http://dx.doi.org/10.1145/3415187

[8] Ameena Saad al sumaiti, Mohammed Hassan Ahmed, and Magdy M. A. Salama. 2014. Smart Home Activities: A Literature Review. *Electric Power Components and Systems* 42, 3-4 (2014), 294–305. DOI:http://dx.doi.org/10.1080/15325008.2013.832439

[9] Mussab Alaa, A.A. Zaidan, B.B. Zaidan, Mohammed Talal, and M.L.M. Kiah. 2017. A review of smart home applications based on Internet of Things. *Journal of Network and Computer Applications* 97 (2017), 48–65. DOI:http://dx.doi.org/https://doi.org/10.1016/j.jnca.2017.08.017

[10] Frances K. Aldrich. 2003. *Smart Homes: Past, Present and Future*. Springer London, London, 17–39. DOI:http://dx.doi.org/10.1007/1-85233-854-7_2

[11] Bako Ali and Ali Ismail Awad. 2018. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors* 18, 3 (2018). DOI:http://dx.doi.org/10.3390/s18030817

[12] Florian Alt and Emanuel von Zezschwitz. 2019. Special Issue: Emerging Trends in Usable Security and Privacy. *Journal of Interactive Media (icom)* 18, 3 (dec 2019), 1–13. DOI:http://dx.doi.org/10.1515/icom-2019-0019

[13] Malik Nadeem Anwar, Mohammad Nazir, and Khurram Mustafa. 2017. Security threats taxonomy: Smart-home perspective. In *2017 3rd International Conference on Advances in Computing,Communication Automation (ICACCA) (Fall)*. 1–4. DOI:http://dx.doi.org/10.1109/ICACCAF.2017.8344666

[14] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 2 (2018), 59. DOI:http://dx.doi.org/10.1145/3214262

[15] Luigi Atzori, Antonio Iera, and Giacomo Morabito. 2017. Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks* 56 (2017), 122–140. DOI:http://dx.doi.org/https://doi.org/10.1016/j.adhoc.2016.12.004

[16] Anitra Babic, Huijun Xiong, Danfeng Yao, and Liviu Iftode. 2009. Building Robust Authentication Systems with Activity-Based Personal Questions. In *Proceedings of the 2nd ACM Workshop on Assurable and Usable Security Configuration (SafeConfig '09)*. Presented in Chicago, Illinois, USA. Association for Computing Machinery, New York, NY, USA, 19–24. DOI:http://dx.doi.org/10.1145/1655062.1655067

[17] Costin Badica, Marius Brezovan, and Amelia Badica. 2013. An Overview of Smart Home Environments: Architectures, Technologies and Applications. In

Proceedings of the Sixth Balkan Conference in Informatics. Presented in Thessaloniki, Greece. Citeseer. http://ceur-ws.org/Vol-1036/p78-Badica.pdf

[18] Aaron Bangor, Philip Kortum, and James Miller. 2009. Determining what individual SUS scores mean: Adding an adjective rating scale. *Journal of usability studies* 4, 3 (2009), 114–123.

[19] Debjanee Barua, Judy Kay, and Cécile Paris. 2013. Viewing and Controlling Personal Sensor Data: What Do Users Want?. In *Persuasive Technology*, Shlomo Berkovsky and Jill Freyne (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 15–26.

[20] Carlos Bermejo Fernandez, Lik Hang Lee, Petteri Nurmi, and Pan Hui. 2021. *PARA: Privacy Management and Control in Emerging IoT Ecosystems Using Augmented Reality*. Association for Computing Machinery, New York, NY, USA, 478–486. https://doi.org/10.1145/3462244.3479885

[21] Cristina Bicchieri and Eugen Dimant. 2019. Nudging with care: The risks and benefits of social information. *Public choice* (2019), 1–22. https://doi.org/10.1007/s11127-019-00684-6

[22] Kang Bing, Liu Fu, Yun Zhuo, and Liang Yanlei. 2011. Design of an Internet of Things-Based Smart Home System. *Proc. ICICIP 2011* 2 (2011), 921–924. DOI: http://dx.doi.org/10.1109/ICICIP.2011.6008384

[23] Joseph Bonneau, Elie Bursztein, Ilan Caron, Rob Jackson, and Mike Williamson. 2015. Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google. In *Proceedings of the 24th International Conference on World Wide Web (WWW '15)*. Presented in Florence, Italy. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 141–150. DOI:http://dx.doi.org/10.1145/2736277.2741691

[24] Christine L. Borgman. 1986. The User's Mental Model of an Information Retrieval System: An Experiment on a Prototype Online Catalog. *International Journal of Man-Machine Studies* 24, 1 (1986), 47–64. DOI:http://dx.doi.org/10.1016/S0020-7373(86)80039-6

[25] Scott Boss, Dennis Galletta, Paul Lowry, Gregory Moody, and Peter Polak. 2015. What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly* 39 (12 2015), 837–864. DOI:http://dx.doi.org/10.25300/MISQ/2015/39.4.5

[26] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. DOI:http://dx.doi.org/10.1191/1478088706qp063oa

[27] Virginia Braun and Victoria Clarke. 2012. Thematic analysis. *APA handbook of research methods in psychology. Research designs: Quantitative, qualitative, neuropsychological, and biological* 2 (2012), 57–71.

[28] Bernardo Breve, Giuseppe Desolda, Vincenzo Deufemia, Francesco Greco, and Maristella Matera. 2021. An End-User Development Approach to Secure Smart Environments. In *End-User Development*, Daniela Fogli, Daniel Tetteroo, Barbara Rita Barricelli, Simone Borsci, Panos Markopoulos, and George A. Papadopoulos (Eds.). Springer International Publishing, Cham, 36–52.

[29] John Brooke. 1996. SUS: a "quick and dirty" usability scale. *Usability evaluation in industry* 1 (1996), 189.

[30] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. 2016. On Privacy and Security Challenges in Smart Connected Homes. In *2016 European Intelligence and Security Informatics Conference (EISIC)*. 172–175. DOI:http://dx.doi.org/10.1109/EISIC.2016.044

[31] Ana Caraban, Evangelos Karapanos, Daniel Gonçalves, and Pedro Campos. 2019. *23 Ways to Nudge: A Review of Technology-Mediated Nudging in Human-Computer Interaction*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3290605.3300733

[32] Nico Castelli, Corinna Ogonowski, Timo Jakobi, Martin Stein, Gunnar Stevens, and Volker Wulf. 2017. What Happened in My Home? An End-User Development Approach for Smart Home Data Visualization. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Presented in Denver, Colorado, USA. Association for Computing Machinery, New York, NY, USA, 853–866. DOI:http://dx.doi.org/10.1145/3025453.3025485

[33] George Chalhoub, Ivan Flechais, Norbert Nthala, and Ruba Abu-Salma. 2020b. Innovation Inaction or In Action? The Role of User Experience in the Security and Privacy Design of Smart Home Cameras. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Berkeley, CA, USA, 185–204. https://www.usenix.org/conference/soups2020/presentation/chalhoub

[34] George Chalhoub, Ivan Flechais, Norbert Nthala, Ruba Abu-Salma, and Elie Tom. 2020a. Factoring User Experience into the Security and Privacy Design of Smart Home Devices: A Case Study. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA '20)*. Presented in Honolulu, HI, USA. Association for Computing Machinery, New York, NY, USA, 1–9. DOI:http://dx.doi.org/10.1145/3334480.3382850

[35] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. "It Did Not Give Me an Option to Decline": A Longitudinal Analysis of the

User Experience of Security and Privacy in Smart Home Products. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Presented in Yokohama, Japan. Association for Computing Machinery, New York, NY, USA, Article 555, 16 pages. DOI:http://dx.doi.org/10.1145/3411764.3445691

[36] Marie Chan, Eric Campo, Daniel Estève, and Jean-Yves Fourniols. 2009. Smart homes — Current features and future perspectives. *Maturitas* 64, 2 (2009), 90–97. DOI:http://dx.doi.org/https://doi.org/10.1016/j.maturitas.2009.07.014

[37] Yuxin Chen, Huiying Li, Shan-Yuan Teng, Steven Nagels, Zhijing Li, Pedro Lopes, Ben Y. Zhao, and Haitao Zheng. 2020. Wearable Microphone Jamming. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Presented in Honolulu, HI, USA. Association for Computing Machinery, New York, NY, USA, 1–12. DOI:http://dx.doi.org/10.1145/3313831.3376304

[38] Youngjun Cho, Nadia Bianchi-Berthouze, Nicolai Marquardt, and Simon J. Julier. 2018. Deep Thermal Imaging: Proximate Material Type Recognition in the Wild through Deep Learning of Spatial Surface Temperature Patterns. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. Presented in Montreal QC, Canada. Association for Computing Machinery, New York, NY, USA, 1–13. DOI:http://dx.doi.org/10.1145/3173574.3173576

[39] Richard Chow. 2017. The Last Mile for IoT Privacy. *IEEE Security & Privacy* 15, 6 (2017), 73–76. DOI:http://dx.doi.org/10.1109/MSP.2017.4251118

[40] Richard Chow, Serge Egelman, Raghudeep Kannavara, Hosub Lee, Suyash Misra, and Edward Wang. 2015. HCI in Business: A Collaboration with Academia in IoT Privacy. In *HCI in Business*, Fiona Fui-Hoon Nah and Chuan-Hoo Tan (Eds.). Springer International Publishing, Cham, 679–687.

[41] Hyunji Chung, Michaela Iorga, Jeffrey Voas, and Sangjin Lee. 2017. Alexa, Can I Trust You? *Computer* 50, 9 (2017), 100–104. DOI:http://dx.doi.org/10.1109/MC.2017.3571053

[42] Victoria Clarke, Nikki Hayfield, Naomi Moller, and Irmgard Tischner. 2017. Once Upon A Time…: Story Completion Methods. *Collecting Qualitative Data: A Practical Guide to Textual, Media and Virtual Techniques* 1 (2017), 45–70.

[43] Camille Cobb, Sruti Bhagavatula, Kalil Anderson Garrett, Alison Hoffman, Varun Rao, and Lujo Bauer. 2021. "I would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users. *Proceedings on Privacy Enhancing Technologies* 4 (2021), 54–75.

[44] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. 2020. Informing the Design of a Personalized Privacy Assistant for the Internet of Things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Presented in Honolulu, HI, USA. Association for Computing Machinery, New York, NY, USA, 1–13. DOI:http://dx.doi.org/10.1145/3313831.3376389

[45] Jessica Colnago and Hélio Guardia. 2016. How to Inform Privacy Agents on Preferred Level of User Control?. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct (UbiComp '16)*. Presented in Heidelberg, Germany. Association for Computing Machinery, New York, NY, USA, 1542–1547. DOI:http://dx.doi.org/10.1145/2968219.2968546

[46] Lorrie Cranor, Tal Rabin, Vitaly Shmatikov, Salil Vadhan, and Daniel Weitzner. 2016. Towards a Privacy Research Roadmap for the Computing Community. (2016). DOI:http://dx.doi.org/10.48550/ARXIV.1604.03160

[47] Lorrie Faith Cranor. 2012. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.* 10 (2012), 273. https://fpf.org/wp-content/uploads/2013/07/Cranor_Necessary-But-Not-Sufficient1.pdf

[48] Lorrie Faith Cranor and Simson Garfinkel. 2005. *Security and Usability: Designing Secure Systems That People Can Use*. O'Reilly Media, Inc.

[49] Mary J. Culnan and Pamela K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science* 10, 1 (1999), 104–115. DOI:http://dx.doi.org/10.1287/orsc.10.1.104

[50] Anupam Das, Martin Degeling, Daniel Smullen, and Norman Sadeh. 2018. Personalized Privacy Assistants for the Internet of Things: Providing Users with Notice and Choice. *IEEE Pervasive Computing* 17, 3 (Jul 2018), 35–46. DOI: http://dx.doi.org/10.1109/MPRV.2018.03367733

[51] Sauvik Das, Eiji Hayashi, and Jason I. Hong. 2013. Exploring Capturable Everyday Memory for Autobiographical Authentication. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '13)*. Presented in Zurich, Switzerland. Association for Computing Machinery, New York, NY, USA, 211–220. DOI:http://dx.doi.org/10.1145/2493432.2493453

[52] Alexander De Luca, Bernhard Frauendienst, Max Maurer, and Doris Hausen. 2010. On the Design of a "Moody" Keyboard. In *Proceedings of the 8th ACM*

Conference on Designing Interactive Systems (DIS '10). Presented in Aarhus, Denmark. Association for Computing Machinery, New York, NY, USA, 236–239. DOI:http://dx.doi.org/10.1145/1858171.1858213

[53] Marie Delacre, Christophe Leys, Youri L Mora, and Daniël Lakens. 2019. Taking parametric assumptions seriously: Arguments for the use of Welch's F-test instead of the classical F-test in one-way ANOVA. *International Review of Social Psychology* 32, 1 (2019).

[54] Carole Després. 1991. The Meaning of Home: Literature Review and Directions for Future Research and Theoretical Development. *Journal of Architectural and Planning Research* 8, 2 (1991), 96–115. http://www.jstor.org/stable/43029026

[55] Reyhan Duezguen, Peter Mayer, Benjamin Berens, Christopher Beckmann, Lukas Aldag, Mattia Mossano, Melanie Volkamer, and Thorsten Strufe. 2021. How to Increase Smart Home Security and Privacy Risk Perception. In *20th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 18 - 20 Augus 2021, Shenyang, China*.

[56] Janna Lynn Dupree, Richard Devries, Daniel M. Berry, and Edward Lank. 2016. Privacy Personas: Clustering Users via Attitudes and Behaviors toward Security Practices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. Presented in San Jose, California, USA. Association for Computing Machinery, New York, NY, USA, 5228–5239. DOI:http://dx.doi.org/10.1145/2858036.2858214

[57] Marc Dupuis and Mercy Ebenezer. 2018. Help Wanted: Consumer Privacy Behavior and Smart Home Internet of Things (IoT) Devices. In *Proceedings of the 19th Annual SIG Conference on Information Technology Education*.

[58] Nico Ebert, Kurt Alexander Ackermann, and Björn Scheppler. 2021. Bolder is Better: Raising User Awareness through Salient and Concise Privacy Notices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Presented in Yokohama, Japan. Association for Computing Machinery, New York, NY, USA, Article 67, 12 pages. DOI:http://dx.doi.org/10.1145/3411764.3445516

[59] Zohar Efroni, Jakob Metzger, Lena Mischau, and Marie Schirmbeck. 2019. Privacy Icons:. *European Data Protection Law Review* 5, 3 (2019). DOI:http://dx.doi.org/10.21552/edpl/2019/3/9

[60] Serge Egelman, David Molnar, Nicolas Christin, Alessandro Acquisti, Cormac Herley, and Shriram Krishnamurthi. 2010. Please Continue to Hold: An Empirical Study on User Tolerance of Security Delays. In *9th Annual Workshop*

on the Economics of Information Security, WEIS 2010, Harvard University, Cambridge, MA, USA, June 7-8, 2010. http://weis2010.econinfosec.org/papers/session3/weis2010_egelman.pdf

[61] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the Experts: What Should Be on an IoT Privacy and Security Label?. In *2020 IEEE Symposium on Security and Privacy (SP)*. Presented in San Francisco, CA, USA. IEEE, New York, NY, USA, 447–464. DOI:http://dx.doi.org/10.1109/SP40000.2020.00043

[62] Pardis Emami-Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS '17)*. USENIX Association, Berkeley, CA, USA, 399–412.

[63] Pardis Emami Naeini, Martin Degeling, Lujo Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghighat, and Heather Patterson. 2018. The Influence of Friends and Experts on Privacy Decision Making in IoT Scenarios. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 48 (Nov. 2018), 26 pages. DOI:http://dx.doi.org/10.1145/3274317

[64] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In *Proc. of the CHI Conference on Human Factors in Computing Systems (CHI '19)*. Presented in Glasgow, Scotland Uk. ACM, New York, NY, USA, Article 534, 12 pages. DOI:http://dx.doi.org/10.1145/3290605.3300764

[65] Julian James Faraway. 2002. *Practical regression and ANOVA using R*. Vol. 168. University of Bath Bath.

[66] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Presented in Yokohama, Japan. Association for Computing Machinery, New York, NY, USA, Article 64, 16 pages. DOI:http://dx.doi.org/10.1145/3411764.3445148

[67] Andy Field and Graham Hole. 2002. *How to design and report experiments*. Sage.

[68] Ivan Flechais, Cecilia Mascolo, and M. Angela Sasse. 2007. Integrating security and usability into the requirements and design process. *International Journal of Electronic Security and Digital Forensics* 1, 1 (2007), 12–26. DOI:http://dx.doi.org/10.1504/IJESDF.2007.013589

[69] Ivan Flechais, M. Angela Sasse, and Stephen M. V. Hailes. 2003. Bringing Security Home: A Process for Developing Secure and Usable Systems. In *Proceedings of the 2003 Workshop on New Security Paradigms (NSPW '03)*. Presented in

Ascona, Switzerland. Association for Computing Machinery, New York, NY, USA, 49–57. DOI:http://dx.doi.org/10.1145/986655.986664

[70] Donna L. Floyd, Steven Prentice-Dunn, and Ronald W. Rogers. 2000. A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology* 30, 2 (2000), 407–429. DOI:http://dx.doi.org/https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

[71] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human-Computer Interaction* 35, 6 (2019), 456–467. DOI:http://dx.doi.org/10.1080/10447318.2018.1456150

[72] Batya Friedman, David Hurley, Daniel C. Howe, Edward Felten, and Helen Nissenbaum. 2002. Users' Conceptions of Web Security: A Comparative Study. In *CHI '02 Extended Abstracts on Human Factors in Computing Systems (CHI EA '02)*. Presented in Minneapolis, Minnesota, USA. Association for Computing Machinery, New York, NY, USA, 746–747. DOI:http://dx.doi.org/10.1145/506443.506577

[73] Markus Funk, Robin Boldt, Bastian Pfleging, Max Pfeiffer, Niels Henze, and Albrecht Schmidt. 2014. Representing Indoor Location of Objects on Wearable Computers with Head-Mounted Displays. In *Proceedings of the 5th Augmented Human International Conference (AH '14)*. Presented in Kobe, Japan. Association for Computing Machinery, New York, NY, USA, Article 18, 4 pages. DOI:http://dx.doi.org/10.1145/2582051.2582069

[74] Pranay P. Gaikwad, Jyotsna P. Gabhane, and Snehal S. Golait. 2015. A Survey Based on Smart Homes System Using Internet-of-Things. In *Proceedings of the International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC '15)*. IEEE, Piscataway, NJ, USA, 0330–0335. DOI:http://dx.doi.org/10.1109/ICCPEIC.2015.7259486

[75] Paul A Games and John F Howell. 1976. Pairwise multiple comparison procedures with unequal n's and/or variances: a Monte Carlo study. *Journal of Educational Statistics* 1, 2 (1976), 113–125.

[76] Simson Garfinkel and Heather Richter Lipford. 2014. Usable Security: History, Themes, and Challenges. *Synthesis Lectures on Information Security, Privacy, and Trust* 5, 2 (2014), 1–124. DOI:http://dx.doi.org/10.2200/S00594ED1V01Y201408SPT011

[77] Radhika Garg and Christopher Moreno. 2019. Understanding Motivators, Constraints, and Practices of Sharing Internet of Things. *Proc. ACM Interact.*

Mob. Wearable Ubiquitous Technol. 3, 2, Article 44 (June 2019), 21 pages. DOI: http://dx.doi.org/10.1145/3328915

[78] Christine Geeng and Franziska Roesner. 2019. Who's In Control? Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Presented in Glasgow, Scotland Uk. ACM, New York, NY, USA, Article Paper 268, 13 pages. DOI: http://dx.doi.org/10.1145/3290605.3300498

[79] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security* 77 (2018), 226–261. DOI:http://dx.doi.org/https://doi.org/10.1016/j.cose.2018.04.002

[80] Nina Gerber, Benjamin Reinheimer, and Melanie Volkamer. 2019. Investigating People's Privacy Risk Perception. *Proceedings on privacy enhancing technologies* 2019, 3 (2019), 267–288. DOI:http://dx.doi.org/10.2478/popets-2019-0047

[81] Kirsten Gram-Hanssen and Sarah J. Darby. 2018. "Home is where the smart is"? Evaluating smart home research and approaches against the concept of home. *Energy Research & Social Science* 37 (2018), 94–101. DOI:http://dx.doi.org/https://doi.org/10.1016/j.erss.2017.09.037

[82] Matthew Green and Matthew Smith. 2016. Developers are Not the Enemy!: The Need for Usable Security APIs. *IEEE Security & Privacy* 14, 5 (2016), 40–46. DOI:http://dx.doi.org/10.1109/MSP.2016.111

[83] Rebecca Grier. 2015. How high is high? A metanalysis of NASA TLX global workload scores. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 59 (10 2015). DOI:http://dx.doi.org/10.1177/1541931215591373

[84] Siddharth Gulati, Sonia Sousa, and David Lamas. 2018. Modelling trust in human-like technologies. In *Proceedings of the 9th Indian conference on human computer interaction*. 1–10.

[85] Siddharth Gulati, Sonia Sousa, and David Lamas. 2019. Design, development and evaluation of a human-computer trust scale. *Behaviour & Information Technology* 38, 10 (2019), 1004–1015. DOI:http://dx.doi.org/10.1080/0144929X.2019.1656779

[86] Alina Hang, Alexander De Luca, and Heinrich Hussmann. 2015. I Know What You Did Last Week! Do You? Dynamic Security Questions for Fallback Authentication on Smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. Presented in Seoul, Republic of Korea. Association for Computing Machinery, New York, NY, USA, 1383–1392. DOI:http://dx.doi.org/10.1145/2702123.2702131

[87] Marian Harbach, Markus Hettig, Susanne Weber, and Matthew Smith. 2014. Using Personal Examples to Improve Risk Communication for Security & Privacy Decisions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. Presented in Toronto, Ontario, Canada. Association for Computing Machinery, New York, NY, USA, 2647–2656. DOI: http://dx.doi.org/10.1145/2556288.2556978

[88] Hamza Harkous, Kassem Fawaz, Rémi Lebret, Florian Schaub, Kang G. Shin, and Karl Aberer. 2018. Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning. In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, Baltimore, MD, 531–548. https://www.usenix.org/conference/usenixsecurity18/presentation/harkous

[89] Hamza Harkous, Kassem Fawaz, Kang G. Shin, and Karl Aberer. 2016. PriBots: Conversational Privacy with Chatbots. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 6. https://www.usenix.org/conference/soups2016/workshop-program/wfpn/presentation/harkous

[90] Sandra G. Hart. 2006. Nasa-Task Load Index (NASA-TLX); 20 Years Later. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 50, 9 (Oct. 2006), 904–908. DOI:http://dx.doi.org/10.1177/154193120605000909

[91] Sandra G. Hart and Lowell E. Staveland. 1988. Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research. In *Advances in Psychology*, Peter A. Hancock and Najmedin Meshkati (Eds.). Advances in Psychology, Vol. 52. North-Holland, Oxford, England, 139–183. DOI:http://dx.doi.org/https://doi.org/10.1016/S0166-4115(08)62386-9

[92] Katrin Hartwig and Christian Reuter. 2021. Nudge or Restraint: How Do People Assess Nudging in Cybersecurity - A Representative Study in Germany. In *European Symposium on Usable Security 2021 (EuroUSEC '21)*. Presented in Karlsruhe, Germany. Association for Computing Machinery, New York, NY, USA, 141–150. DOI:http://dx.doi.org/10.1145/3481357.3481514

[93] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. 2018. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, Baltimore, MD, 255–272. https://www.usenix.org/conference/usenixsecurity18/presentation/he

[94] Yangyang He. 2019. Recommending Privacy Settings for IoT. In *Proceedings of the 24th International Conference on Intelligent User Interfaces: Companion (IUI*

'19). Presented in Marina del Ray, California. Association for Computing Machinery, New York, NY, USA, 157–158. DOI:http://dx.doi.org/10.1145/3308557.3308732

[95] Ryan Heartfield, George Loukas, Sanja Budimir, Anatolij Bezemskij, Johnny R.J. Fontaine, Avgoustinos Filippoupolitis, and Etienne Roesch. 2018. A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security* 78 (2018), 398–428. DOI:http://dx.doi.org/https://doi.org/10.1016/j.cose.2018.07.011

[96] Almut Herzog and Nahid Shahmehri. 2007. User Help Techniques for Usable Security. In *Proceedings of the 2007 Symposium on Computer Human Interaction for the Management of Information Technology (CHIMIT '07)*. Presented in Cambridge, Massachusetts. Association for Computing Machinery, New York, NY, USA, 11–es. DOI:http://dx.doi.org/10.1145/1234772.1234787

[97] Yue Huang, Borke Obada-Obieh, and Konstantin (Kosta) Beznosov. 2020. Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Presented in Honolulu, HI, USA. Association for Computing Machinery, New York, NY, USA, 1–13. DOI:http://dx.doi.org/10.1145/3313831.3376529

[98] Martin J Kraemer, Ivan Flechais, and Helena Webb. 2019. Exploring Communal Technology Use in the Home. In *Proceedings of the Halfway to the Future Symposium 2019 (HTTF 2019)*. Presented in Nottingham, United Kingdom. Association for Computing Machinery, New York, NY, USA, Article Article 5, 8 pages. DOI:http://dx.doi.org/10.1145/3363384.3363389

[99] Timo Jakobi, Corinna Ogonowski, Nico Castelli, Gunnar Stevens, and Volker Wulf. 2017. The Catch(Es) with Smart Home: Experiences of a Living Lab Field Study. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '17)*. Presented in Denver, Colorado, USA. ACM, New York, NY, USA, 1620–1633. DOI:http://dx.doi.org/10.1145/3025453.3025799

[100] William Jang, Adil Chhabra, and Aarathi Prasad. 2017. Enabling Multi-User Controls in Smart Home Devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy (IoTS&P '17)*. Presented in Dallas, Texas, USA. Association for Computing Machinery, New York, NY, USA, 49–54. DOI:http://dx.doi.org/10.1145/3139937.3139941

[101] Li Jiang, Da-You Liu, and Bo Yang. 2004. Smart home research. In *Proceedings of 2004 International Conference on Machine Learning and Cybernetics (IEEE Cat. No.04EX826)*, Vol. 2. 659–663 vol.2. DOI:http://dx.doi.org/10.1109/ICMLC.2004.1382266

[102] Haojian Jin, Boyuan Guo, Rituparna Roychoudhury, Yaxing Yao, Swarun Kumar, Yuvraj Agarwal, and Jason I. Hong. 2022. Exploring the Needs of Users for Supporting Privacy-Protective Behaviors in Smart Homes. In *CHI Conference on Human Factors in Computing Systems (CHI '22)*. Presented in New Orleans, LA, USA. Association for Computing Machinery, New York, NY, USA, Article 449, 19 pages. DOI:http://dx.doi.org/10.1145/3491102.3517602

[103] Matthew Johnson and Frank Stajano. 2009. Usability of Security Management:Defining the Permissions of Guests. In *Security Protocols*, Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 276–283.

[104] Philip N. Johnson-Laird. 1983. *Mental Models: Towards a Cognitive Science of Language, Inference, and Consciousness*. Number 6. Harvard University Press, Cambridge, MA, USA.

[105] Mike Just. 2005. Designing authentication systems with challenge questions. *Security and usability: Designing Secure Systems That People Can Use* (2005), 143–155.

[106] Mike Just and David Aspinall. 2009. Personal Choice and Challenge Questions: A Security and Usability Assessment. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09)*. Presented in Mountain View, California, USA. Association for Computing Machinery, New York, NY, USA, Article 8, 11 pages. DOI:http://dx.doi.org/10.1145/1572532.1572543

[107] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS '15)*. USENIX Association, Berkeley, CA, USA, 39–52.

[108] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "Nutrition Label" for Privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09)*. Presented in Mountain View, California, USA. Association for Computing Machinery, New York, NY, USA, Article 4, 12 pages. DOI:http://dx.doi.org/10.1145/1572532.1572538

[109] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as Part of the App Decision-Making Process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. Presented in Paris, France. Association for Computing Machinery, New York, NY, USA, 3393–3402. DOI:http://dx.doi.org/10.1145/2470654.2466466

[110] Hassan Khan, Urs Hengartner, and Daniel Vogel. 2018. Augmented Reality-Based Mimicry Attacks on Behaviour-Based Smartphone Authentication. In

Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '18). Presented in Munich, Germany. Association for Computing Machinery, New York, NY, USA, 41–53. DOI:http://dx.doi.org/10.1145/3210240.3210317

[111] Cory D. Kidd, Robert Orr, Gregory D. Abowd, Christopher G. Atkeson, Irfan A. Essa, Blair MacIntyre, Elizabeth Mynatt, Thad E. Starner, and Wendy Newstetter. 1999. The Aware Home: A Living Laboratory for Ubiquitous Computing Research. In *Cooperative Buildings. Integrating Information, Organizations, and Architecture*, Norbert A. Streitz, Jane Siegel, Volker Hartkopf, and Shin'ichi Konomi (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 191–198.

[112] Agnieszka Kitkowska, Mark Warner, Yefim Shulman, Erik Wästlund, and Leonardo A. Martucci. 2020. Enhancing Privacy through the Visual Design of Privacy Notices: Exploring the Interplay of Curiosity, Control and Affect. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Berkeley, CA, USA, 437–456. https://www.usenix.org/conference/soups2020/presentation/kitkowska

[113] Predrag Klasnja, Sunny Consolvo, Tanzeem Choudhury, Richard Beckwith, and Jeffrey Hightower. 2009. Exploring Privacy Concerns about Personal Sensing. In *Pervasive Computing*, Hideyuki Tokuda, Michael Beigl, Adrian Friday, A. J. Bernheim Brush, and Yoshito Tobe (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 176–183.

[114] Marion Koelle, Katrin Wolf, and Susanne Boll. 2018. Beyond LED Status Lights - Design Requirements of Privacy Notices for Body-Worn Cameras. In *Proceedings of the Twelfth International Conference on Tangible, Embedded, and Embodied Interaction (TEI '18)*. Presented in Stockholm, Sweden. Association for Computing Machinery, New York, NY, USA, 177–187. DOI:http://dx.doi.org/10.1145/3173225.3173234

[115] Vinay Koshy, Joon Sung Sung Park, Ti-Chung Cheng, and Karrie Karahalios. 2021. "We Just Use What They Give Us": Understanding Passenger User Perspectives in Smart Homes. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Presented in Yokohama, Japan. Association for Computing Machinery, New York, NY, USA, Article 41, 14 pages. DOI:http://dx.doi.org/10.1145/3411764.3445598

[116] Tobias Kowatsch and Wolfgang Maass. 2012. Privacy Concerns and Acceptance of IoT Services. In *The Internet of Things 2012 : New Horizons*. IERC - Internet of Things European Research Cluster, Halifax, UK, 176–187. https://www.alexandria.unisg.ch/212316/

[117] Andraž Krašovec, Daniel Pellarini, Dimitrios Geneiatakis, Gianmarco Baldini, and Veljko Pejović. 2020. Not Quite Yourself Today: Behaviour-Based

Continuous Authentication in IoT Environments. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 4, 4, Article 136 (dec 2020), 29 pages. DOI:http://dx.doi.org/10.1145/3432206

[118] Tobias Kroll, Ute Paukstadt, Kseniya Kreidermann, and Milad Mirbabaie. 2019. Nudging People to Save Energy in Smart Homes with Social Norms and Self-Commitment. In *Proceedings of the 27th European Conference on Information System*.

[119] Todd Kulesza, Simone Stumpf, Margaret Burnett, Sherry Yang, Irwin Kwan, and Weng-Keen Wong. 2013. Too Much, Too Little, or Just Right? Ways Explanations Impact End Users' Mental Models. In *Proceedings of the IEEE Symposium on Visual Languages and Human Centric Computing (VL/HCC '13)*. IEEE, Piscataway, NJ, USA, 3–10. DOI:http://dx.doi.org/10.1109/VLHCC.2013.6645235

[120] Albrecht Kurze, Andreas Bischof, Sören Totzauer, Michael Storz, Maximilian Eibl, Margot Brereton, and Arne Berger. 2020. *Guess the Data: Data Work to Understand How People Make Sense of and Use Simple Sensor Data from Homes*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376273

[121] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-Seeking Behaviors With Smart Speakers. *Proceedings of the ACM Conference on Human-Computer Interaction* 2, CSCW, Article 102 (Nov. 2018), 31 pages. DOI:http://dx.doi.org/10.1145/3274371

[122] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2017. *Research methods in human computer interaction* (2nd edition ed.). Morgan Kaufmann, Cambridge, MA.

[123] Scott Lederer, Anind K. Dey, and Jennifer Mankoff. 2002. *A Conceptual Model and a Metaphor of Everyday Privacy in Ubiquitous*. Technical Report. University of California at Berkeley, USA.

[124] Scott Lederer, Jennifer Mankoff, and Anind K. Dey. 2003. Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing. In *CHI '03 Extended Abstracts on Human Factors in Computing Systems (CHI EA '03)*. Presented in Ft. Lauderdale, Florida, USA. Association for Computing Machinery, New York, NY, USA, 724–725. DOI:http://dx.doi.org/10.1145/765891.765952

[125] H. Lee and A. Kobsa. 2016. Understanding user privacy in Internet of Things environments. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*. Presented in Reston, VA, USA. IEEE, New York, NY, USA, 407–412.

[126] H. Lee and A. Kobsa. 2017. Privacy preference modeling and prediction in a simulated campuswide IoT environment. In *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. Presented in Kona, HI, USA. IEEE, New York, NY, USA, 276–285.

[127] Thomas C Leonard. 2008. Richard H. Thaler, Cass R. Sunstein, Nudge: Improving decisions about health, wealth, and happiness. (2008).

[128] Howard Levene. 1961. Robust tests for equality of variances. *Contributions to probability and statistics. Essays in honor of Harold Hotelling* (1961), 279–292.

[129] Xiaopeng Li, Fengyao Yan, Fei Zuo, Qiang Zeng, and Lannan Luo. 2019. Touch Well Before Use: Intuitive and Secure Authentication for IoT Devices. In *The 25th Annual International Conference on Mobile Computing and Networking*. Association for Computing Machinery, New York, NY, USA, Article 33, 17 pages. https://doi.org/10.1145/3300061.3345434

[130] Huichen Lin and Neil W. Bergmann. 2016. IoT Privacy and Security Challenges for Smart Home Environments. *Information* 7, 3 (2016). DOI:http://dx.doi.org/10.3390/info7030044

[131] Hao-xiang Lin and Chun Chang. 2021. Factors associated with the quitting intention among Chinese adults: Application of protection motivation theory. *Current Psychology* (2021).

[132] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun Zhang, Norman Sadeh, Alessandro Acquisti, and Yuvraj Agarwal. 2016. Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions. In *Proceedings of the Twelfth Symposium on Usable Privacy and Security*.

[133] Karen MacDonell, Xinguang Chen, Yaqiong Yan, Fang Li, Jie Gong, Huiling Sun, Xiaoming Li, and Bonita Stanton. 2013. A Protection Motivation Theory-Based Scale for Tobacco Research among Chinese Youth. *Journal of addiction research & therapy* 4 (2013), 154.

[134] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15, 4 (2004), 336–355. DOI:http://dx.doi.org/10.1287/isre.1040.0032

[135] Shrirang Mare, Logan Girvin, Franziska Roesner, and Tadayoshi Kohno. 2019. Consumer Smart Homes: Where We Are and Where We Need to Go. In *Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications (HotMobile '19)*. Presented in Santa Cruz, CA, USA. Association for Computing Machinery, New York, NY, USA, 117–122. DOI:http://dx.doi.org/10.1145/3301293.3302371

[136] Shrirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (2020), 436–458. DOI: http://dx.doi.org/https://doi.org/10.2478/popets-2020-0035

[137] Davit Marikyan, Savvas Papagiannidis, and Eleftherios Alamanos. 2019. A Systematic Review of the Smart Home Literature: A User Perspective. *Technological Forecasting and Social Change* 138 (2019), 139–154. DOI:http://dx.doi.org/10.1016/j.techfore.2018.08.015

[138] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020a. "You Just Can't Know about Everything": Privacy Perceptions of Smart Home Visitors. In *19th International Conference on Mobile and Ubiquitous Multimedia*. Association for Computing Machinery, New York, NY, USA, 83–95. https://doi.org/10.1145/3428361.3428464

[139] Karola Marky, Alexandra Voit, Alina Stöver, Kai Kunze, Svenja Schröder, and Max Mühlhäuser. 2020b. "I Don't Know How to Protect Myself": Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society (NordiCHI '20)*. Presented in Tallinn, Estonia. Association for Computing Machinery, New York, NY, USA, Article 4, 11 pages. DOI:http://dx.doi.org/10.1145/3419249.3420164

[140] Simon Mayer, Yassin N. Hassan, and Gábor Sörös. 2014. A Magic Lens for Revealing Device Interactions in Smart Environments. In *SIGGRAPH Asia 2014 Mobile Graphics and Interactive Applications (SA '14)*. Presented in Shenzhen, China. Association for Computing Machinery, New York, NY, USA, Article 9, 6 pages. DOI:http://dx.doi.org/10.1145/2669062.2669077

[141] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. of the ACM on Human-Computer Interaction (HCI)* 3, CSCW, Article 72 (Nov. 2019), 23 pages. DOI:http://dx.doi.org/10.1145/3359174

[142] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys That Listen: A Study of Parents, Children, and Internet-Connected Toys. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Presented in Denver, Colorado, USA. ACM, New York, NY, USA, 5197–5207. DOI:http://dx.doi.org/10.1145/3025453.3025735

[143] Lukas Mecke, Ken Pfeuffer, Sarah Prange, and Florian Alt. 2018. Open Sesame!: User Perception of Physical, Biometric, and Behavioural Authenti-

cation Concepts to Open Doors. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia (MUM'18)*. Presented in Cairo, Egypt. ACM, New York, NY, USA, 153–159. DOI:http://dx.doi.org/10.1145/3282894.3282923

[144] Vikram Mehta. 2019. Tangible Interactions for Privacy Management *(TEI '19)*. Presented in Tempe, Arizona, USA. Association for Computing Machinery, New York, NY, USA, 723–726. DOI:http://dx.doi.org/10.1145/3294109.3302934

[145] Vikram Mehta, Arosha K. Bandara, Blaine A. Price, and Bashar Nuseibeh. 2016. Privacy Itch and Scratch: On Body Privacy Warnings and Controls. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. Presented in San Jose, California, USA. Association for Computing Machinery, New York, NY, USA, 2417–2424. DOI:http://dx.doi.org/10.1145/2851581.2892475

[146] Vikram Mehta, Arosha K. Bandara, Blaine A. Price, Bashar Nuseibeh, and Daniel Gooch. 2021a. Up Close & Personal: Exploring User-Preferred Image Schemas for Intuitive Privacy Awareness and Control. In *Proceedings of the Fifteenth International Conference on Tangible, Embedded, and Embodied Interaction (TEI '21)*. Presented in Salzburg, Austria. Association for Computing Machinery, New York, NY, USA, Article 7, 13 pages. DOI:http://dx.doi.org/10.1145/3430524.3440626

[147] Vikram Mehta, Daniel Gooch, Arosha Bandara, Blaine Price, and Bashar Nuseibeh. 2021b. Privacy Care: A Tangible Interaction Framework for Privacy Management. *ACM Trans. Internet Technol.* 21, 1, Article 25 (Feb. 2021), 32 pages. DOI:http://dx.doi.org/10.1145/3430506

[148] Mateusz Mikusz, Steven Houben, Nigel Davies, Klaus Moessner, and Marc Langheinrich. 2018. Raising Awareness of IoT Sensor Deployments. In *Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT*. IET, London, UK, 8. DOI:http://dx.doi.org/10.1049/cp.2018.0009

[149] M Granger Morgan, Baruch Fischhoff, Ann Bostrom, Cynthia J Atman, and others. 2002. *Risk communication: A mental models approach*. Cambridge University Press, Cambridge, United Kingdom.

[150] Alena Naiakshina, Anastasia Danilova, Eva Gerlitz, Emanuel von Zezschwitz, and Matthew Smith. 2019. "If You Want, I Can Store the Encrypted Password": A Password-Storage Field Study with Freelance Developers. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Presented in Glasgow, Scotland Uk. Association for Computing Machinery, New York, NY, USA, 1–12. DOI:http://dx.doi.org/10.1145/3290605.3300370

[151] Alena Naiakshina, Anastasia Danilova, Christian Tiefenau, Marco Herzog, Sergej Dechand, and Matthew Smith. 2017. Why Do Developers Get Password Storage Wrong? A Qualitative Usability Study. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)*. Presented in Dallas, Texas, USA. Association for Computing Machinery, New York, NY, USA, 311–328. DOI:http://dx.doi.org/10.1145/3133956.3134082

[152] Daniela Napoli, Sebastian Navas Chaparro, Sonia Chiasson, and Elizabeth Stobert. 2020. Something Doesn't Feel Right: Using Thermal Warnings to Improve User Security Awareness. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association. https://www.usenix.org/system/files/soups2020_poster_napoli.pdf

[153] David H. Nguyen, Alfred Kobsa, and Gillian R. Hayes. 2008. An Empirical Investigation of Concerns of Everyday Tracking and Recording Technologies. In *Proceedings of the International Conference on Ubiquitous Computing (UbiComp '08)*. Presented in Seoul, Korea. Association for Computing Machinery, New York, NY, USA, 182–191. DOI:http://dx.doi.org/10.1145/1409635.1409661

[154] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[155] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, Stanford, CA, USA.

[156] Donald A. Norman. 2014. Some Observations on Mental Models. In *Mental Models*. Psychology Press, 15–22.

[157] Briony J. Oates. 2005. *Researching Information Systems and Computing*. Sage.

[158] L. O'Gorman. 2003. Comparing passwords, tokens, and biometrics for user authentication. *Proc. IEEE* 91, 12 (Dec 2003), 2021–2040. DOI:http://dx.doi.org/10.1109/JPROC.2003.819611

[159] Aafaf Ouaddah, Hajar Mousannif, Anas Abou Elkalam, and Abdellah Ait Ouahman. 2017. Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks* 112 (2017), 237–262. DOI:http://dx.doi.org/https://doi.org/10.1016/j.comnet.2016.11.007

[160] Stefan Palan and Christian Schitter. 2018. Prolific.ac – A subject pool for online experiments. *Journal of Behavioral and Experimental Finance* 17 (2018), 22–27.

[161] Sarah Pidcock, Rob Smits, Urs Hengartner, and Ian Goldberg. 2011. Notisense: An Urban Sensing Notification System to Improve Bystander Privacy. In *Proceedings of the International Workshop Sensing Applications on Mobile Phones (PhoneSense '11)*. 1–5.

[162] Alexander Ponticello, Matthias Fassl, and Katharina Krombholz. 2021. Exploring Authentication for Security-Sensitive Tasks on Smart Home Voice Assistants, In Seventeenth Symposium on Usable Privacy and Security. *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)* (August 2021). https://publications.cispa.saarland/3433/

[163] Rebecca S. Portnoff, Linda N. Lee, Serge Egelman, Pratyush Mishra, Derek Leung, and David Wagner. 2015. Somebody's Watching Me? Assessing the Effectiveness of Webcam Indicator Lights. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. Presented in Seoul, Republic of Korea. Association for Computing Machinery, New York, NY, USA, 1649–1658. DOI:http://dx.doi.org/10.1145/2702123.2702164

[164] LEXICO powered by Oxford. 2022. smart home. https://www.lexico.com/definition/smart_home. (2022). Last accessed April 22, 2022.

[165] Sarah Prange and Florian Alt. 2020. I Wish You Were Smart(er): Investigating Users' Desires and Needs Towards Home Appliances. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Presented in Honolulu, HI, US. Association for Computing Machinery, New York, NY, USA, Article Paper LBW1338, 8 pages. DOI:http://dx.doi.org/10.1145/3334480.3382910

[166] Sarah Prange, Victoria Müller, Daniel Buschek, and Florian Alt. 2017. QuakeQuiz - A Case Study on Deploying a Playful Display Application in a Museum Context. In *Proceedings of the 16th International Conference on Mobile and Ubiquitous Multimedia (MUM '17)*. Presented in Stuttgart, Germany. ACM, New York, NY, USA. DOI:http://dx.doi.org/10.1145/3152832.3152841

[167] Sarah Prange, Christian Tiefenau, Emanuel von Zezschwitz, and Florian Alt. 2019. Towards Understanding User Interaction in Future Smart Homes. In *Proceedings of CHI '19 Workshop on New Directions for the IoT: Automate, Share, Build, and Care (CHI '19 Workshop)*. Presented in Glasgow, UK. ACM, New York, NY, USA, 5. https://www.unibw.de/usable-security-and-privacy/publikationen/pdf/prange2019iot.pdf

[168] S. Prange, E. von Zezschwitz, and F. Alt. 2019. Vision: Exploring Challenges and Opportunities for Usable Authentication in the Smart Home. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. 154–158. DOI:http://dx.doi.org/10.1109/EuroSPW.2019.00024

[169] I. Psychoula, D. Singh, L. Chen, F. Chen, A. Holzinger, and H. Ning. 2018. Users' Privacy Concerns in IoT Based Applications. In *2018 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City*

Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). Presented in Guangzhou, China. IEEE, New York, NY, USA, 1887–1894.

[170] B. Qolomany, A. Al-Fuqaha, A. Gupta, D. Benhaddou, S. Alwajidi, J. Qadir, and A. C. Fong. 2019. Leveraging Machine Learning and Big Data for Smart Buildings: A Comprehensive Survey. *IEEE Access* 7 (2019), 90316–90356. DOI: http://dx.doi.org/10.1109/ACCESS.2019.2926642

[171] Ariel Rabkin. 2008. Personal Knowledge Questions for Fallback Authentication: Security Questions in the Era of Facebook. In *Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS '08)*. Presented in Pittsburgh, Pennsylvania, USA. Association for Computing Machinery, New York, NY, USA, 13–23. DOI:http://dx.doi.org/10.1145/1408664.1408667

[172] Joseph Redmon and Ali Farhadi. 2018. YOLOv3: An Incremental Improvement. (2018).

[173] Jun Rekimoto. 2002. SmartSkin: An Infrastructure for Freehand Manipulation on Interactive Surfaces. In *Proc. SIGCHI Conference on Human Factors in Computing Systems (CHI '02)*. ACM, 113–120.

[174] Biljana L. Risteska Stojkoska and Kire V. Trivodaliev. 2017. A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production* 140 (2017), 1454–1464. DOI:http://dx.doi.org/https://doi.org/10.1016/j.jclepro.2016.10.006

[175] Ronald W. Rogers. 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology* 91, 1 (1975), 93–114. DOI: http://dx.doi.org/10.1080/00223980.1975.9915803 PMID: 28136248.

[176] Ronald W. Rogers, John Cacioppo, and Richard Petty. 1983. *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation*. 153–177.

[177] Graeme D. Ruxton and Guy Beauchamp. 2008. Time for some a priori thinking about post hoc testing. *Behavioral Ecology* 19, 3 (02 2008), 690–693. DOI:http://dx.doi.org/10.1093/beheco/arn020

[178] Jerome H. Saltzer and Michael D. Schroeder. 1975. The protection of information in computer systems. *Proc. IEEE* 63, 9 (1975), 1278–1308. DOI: http://dx.doi.org/10.1109/PROC.1975.9939

[179] Sriram Sami, Sean Rui Xiang Tan, Bangjie Sun, and Jun Han. 2021. LAPD: Hidden Spy Camera Detection Using Smartphone Time-of-Flight Sensors. In *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*

(SenSys '21). Presented in Coimbra, Portugal. Association for Computing Machinery, New York, NY, USA, 288–301. DOI:http://dx.doi.org/10.1145/3485730.3485941

[180] S. Sujin Issac Samuel. 2016. A Review of Connectivity Challenges in IoT-Smart Home. In *Proceedings of the MEC International Conference on Big Data and Smart City (ICBDSC '16)*. IEEE, Piscataway, NJ, USA, 1–4. DOI:http://dx.doi.org/10.1109/ICBDSC.2016.7460395

[181] Angela Sasse, Jonas Hielscher, Jennifer Friedauer, Maximilian Peiffer, and Uta Menges. 2022. Warum IT-Sicherheit in Organisationen einen Neustart braucht. In *18. Deutscher IT-Sicherheitskongress*. BSI.

[182] M. A. Sasse, S. Brostoff, and D. Weirich. 2001. Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal* 19, 3 (jul 2001), 122–131. DOI:http://dx.doi.org/10.1023/A:1011902718709

[183] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A Design Space for Effective Privacy Notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 1–17. https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub

[184] Stuart Schechter, A.J. Bernheim Brush, and Serge Egelman. 2009. It's No Secret. Measuring the Security and Reliability of Authentication via "Secret" Questions. In *2009 30th IEEE Symposium on Security and Privacy*. 375–390. DOI:http://dx.doi.org/10.1109/SP.2009.11

[185] Michael Schiefer. 2015. Smart Home Definition and Security Threats. In *2015 Ninth International Conference on IT Security Incident Management IT Forensics*. 114–118. DOI:http://dx.doi.org/10.1109/IMF.2015.17

[186] Paul M Schwartz and Daniel Solove. 2009. Notice and choice: Implications for digital marketing to youth. In *The Second NPLAN/BMSG Meeting on Digital Media and Marketing to Children*. 1–6.

[187] William Seymour, Martin J. Kraemer, Reuben Binns, and Max Van Kleek. 2020. Informing the Design of Privacy-Empowering Tools for the Connected Home. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Presented in Honolulu, HI, USA. Association for Computing Machinery, New York, NY, USA, 1–14. DOI:http://dx.doi.org/10.1145/3313831.3376264

[188] Syed W. Shah and Salil S. Kanhere. 2019. Recent Trends in User Authentication – A Survey. *IEEE Access* 7 (2019), 112505–112519. DOI:http://dx.doi.org/10.1109/ACCESS.2019.2932400

[189] Joseph Shams, N. A. Arachchilage, and J. Such. 2020. Vision: Why Johnny Can't Configure Smart Home? A Behavioural Framework for Smart Home Privacy Configuration. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (2020), 184–189.

[190] Cong Shi, Jian Liu, Hongbo Liu, and Yingying Chen. 2017. Smart User Authentication through Actuation of Daily Activities Leveraging WiFi-Enabled IoT. In *Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing (Mobihoc '17)*. Presented in Chennai, India. Association for Computing Machinery, New York, NY, USA, Article 5, 10 pages. DOI: http://dx.doi.org/10.1145/3084041.3084061

[191] Zaied Shouran, Ahmad Ashari, and Tri Priyambodo. 2019. Internet of things (IoT) of smart home: privacy and security. *International Journal of Computer Applications* 182, 39 (2019), 3–8.

[192] Manuel Silverio-Fernández, Suresh Renukappa, and Subashini Suresh. 2018. What is a smart device? - a conceptualisation within the paradigm of the internet of things. *Visualization in Engineering* 6, 1 (5 2018), 1–10. DOI:http://dx.doi.org/10.1186/s40327-018-0063-8

[193] Robert H Sloan and Richard Warner. 2014. Beyond notice and choice: Privacy, norms, and consent. *J. High Tech. L.* 14 (2014), 370.

[194] Yunpeng Song, Yun Huang, Zhongmin Cai, and Jason I. Hong. 2020. I'm All Eyes and Ears: Exploring Effective Locators for Privacy Awareness in IoT Scenarios. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Presented in Honolulu, HI, USA. Association for Computing Machinery, New York, NY, USA, 1–13. DOI:http://dx.doi.org/10.1145/3313831.3376585

[195] Statista. 2019. Smart Home Worldwide. (2019). https://www.statista.com/outlook/279/100/smart-home/worldwide last accessed November 17, 2021.

[196] Statista. 2020. Smart Home Report 2020. (2020). https://de.statista.com/statistik/studie/id/41155/dokument/smart-home-report/ last accessed April 15, 2021.

[197] Statista. 2021. Forecast market size of the global smart home market from 2016 to 2022. (2021). https://www.statista.com/statistics/682204/global-smart-home-market-size/ last accessed June 03, 2022.

[198] Statista. 2022a. Anteil der im Homeoffice arbeitenden Beschäftigten in Deutschland vor und während der Corona-Pandemie 2020 und 2021. (2022). https://de.statista.com/statistik/daten/studie/1204173/umfrage/befragung-zur-homeoffice-nutzung-in-der-corona-pandemie/ last accessed June 15, 2022.

[199] Statista. 2022b. Smart home devices unit shipments worldwide from 2018 to 2025. (2022). https://www.statista.com/statistics/920679/smart-home-device-shipments-worldwide-by-category/ last accessed June 03, 2022.

[200] Elizabeth Stobert and Robert Biddle. 2013. Authentication in the Home. In *Workshop on Home Usable Privacy and Security (HUPS)*, Vol. 29. HUPS 2013, Newcastle, UK, 209–218. https://cups.cs.cmu.edu/soups/2013/HUPS/HUPS13-ElizabethStobert.pdf

[201] Peter Story, Daniel Smullen, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. From Intent to Action: Nudging Users Towards Secure Mobile Payments. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, 379–415. https://www.usenix.org/conference/soups2020/presentation/story

[202] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2021. Awareness, Adoption, and Misconceptions of Web Privacy Tools. *Proceedings on Privacy Enhancing Technologies* 2021, 3 (2021), 308–333. DOI:http://dx.doi.org/doi:10.2478/popets-2021-0049

[203] Madiha Tabassum, Tomasz Kosiński, and Heather Richter Lipford. 2019. "I don't own the data": End User Perceptions of Smart Home Device Data Practices and Risks. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security (SOUPS'19)*. Presented in Santa Clara, CA, USA. USENIX Association, Berkeley, CA, USA, 435–450.

[204] Marc Teyssier, Marion Koelle, Paul Strohmeier, Bruno Fruchard, and Jürgen Steimle. 2021. Eyecam: Revealing Relations between Humans and Sensing Devices through an Anthropomorphic Webcam. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Presented in Yokohama, Japan. Association for Computing Machinery, New York, NY, USA, Article 622, 13 pages. DOI:http://dx.doi.org/10.1145/3411764.3445491

[205] Parth Kirankumar Thakkar, Shijing He, Shiyu Xu, Danny Yuxing Huang, and Yaxing Yao. 2022. "It Would Probably Turn into a Social Faux-Pas": Users' and Bystanders' Preferences of Privacy Awareness Mechanisms in Smart Homes. In *CHI Conference on Human Factors in Computing Systems (CHI '22)*. Presented in New Orleans, LA, USA. Association for Computing Machinery, New York, NY, USA, Article 404, 13 pages. DOI:http://dx.doi.org/10.1145/3491102.3502137

[206] Christian Tiefenau, Maximilian Häring, Eva Gerlitz, and Emanuel von Zezschwitz. 2019. Making Privacy Graspable: Can we Nudge Users to use Privacy Enhancing Techniques? (2019). https://arxiv.org/abs/1911.07701

[207] Michael Toomim, Xianhang Zhang, James Fogarty, and James A. Landay. 2008. Access Control by Testing for Shared Knowledge. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '08)*. Presented in Florence, Italy. Association for Computing Machinery, New York, NY, USA, 193–196. DOI:http://dx.doi.org/10.1145/1357054.1357086

[208] Joe Tullio, Anind K. Dey, Jason Chalecki, and James Fogarty. 2007. How It Works: A Field Study of Non-Technical Users Interacting with an Intelligent System. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '07)*. Presented in San Jose, California, USA. Association for Computing Machinery, New York, NY, USA, 31–40. DOI:http://dx.doi.org/10.1145/1240624.1240630

[209] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2013. The current state of access control for smart devices in homes. In *Workshop on Home Usable Privacy and Security (HUPS)*, Vol. 29. HUPS 2013, Newcastle, UK, 209–218.

[210] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2014. Intruders Versus Intrusiveness: Teens' and Parents' Perspectives on Home-entryway Surveillance. In *Proceedings of the International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '14)*. Presented in Seattle, Washington. ACM, New York, NY, USA, 129–139. DOI:http://dx.doi.org/10.1145/2632048.2632107

[211] R. Van Bavel and N. Rodriguez Priego. 2016. Nudging Online Security Behaviour with Warning Messages: Results from an online experiment. *Publications Office of the European Union,* (2016). DOI:http://dx.doi.org/10.2791/2476

[212] René Van Bavel, Nuria Rodríguez-Priego, José Vila, and Pam Briggs. 2019. Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies* 123 (2019), 29–39.

[213] Elise van den Hoven, Evelien van de Garde-Perik, Serge Offermans, Koen van Boerdonk, and Kars-Michiel H. Lenssen. 2013. Moving Tangible Interaction Systems to the Next Level. *Computer* 46, 8 (2013), 70–76. DOI:http://dx.doi.org/10.1109/MC.2012.360

[214] Alexandra Voit, Sven Mayer, Valentin Schwind, and Niels Henze. 2019. *Online, VR, AR, Lab, and In-Situ: Comparison of Research Methods to Evaluate Smart Artifacts*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300737

[215] T. Franklin Waddell, Joshua R. Auriemma, and S. Shyam Sundar. 2016. Make It Simple, or Force Users to Read? Paraphrased Design Improves Comprehension of End User License Agreements. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. Presented in San Jose,

California, USA. Association for Computing Machinery, New York, NY, USA, 5252–5256. DOI:http://dx.doi.org/10.1145/2858036.2858149

[216] Mark Weiser. 1999. The Computer for the 21st Century. *SIGMOBILE Mob. Comput. Commun. Rev.* 3, 3 (July 1999), 3–11. DOI:http://dx.doi.org/10.1145/329124.329126

[217] M. Weiser, R. Gold, and J. S. Brown. 1999. The origins of ubiquitous computing research at PARC in the late 1980s. *IBM Systems Journal* 38, 4 (1999), 693–696.

[218] Daniel Wessel, Moreen Heine, Christiane Attig, and Thomas Franke. 2020. Affinity for Technology Interaction and Fields of Study: Implications for Human-Centered Design of Applications for Public Administration. In *Proceedings of the Conference on Mensch Und Computer (MuC '20)*. Presented in Magdeburg, Germany. Association for Computing Machinery, New York, NY, USA, 383–386. DOI:http://dx.doi.org/10.1145/3404983.3410020

[219] Gary White, Christian Cabrera, Andrei Palade, and Siobhán Clarke. 2019. Augmented Reality in IoT. In *Service-Oriented Computing – ICSOC 2018 Workshops*, Xiao Liu, Michael Mrissa, Liang Zhang, Djamal Benslimane, Aditya Ghose, Zhongjie Wang, Antonio Bucchiarone, Wei Zhang, Ying Zou, and Qi Yu (Eds.). Springer International Publishing, Cham, 149–160.

[220] EJ Williams. 1949. Experimental designs balanced for the estimation of residual effects of treatments. *Australian Journal of Chemistry* 2, 2 (1949), 149–168.

[221] Jacob O. Wobbrock and Julie A. Kientz. 2016. Research Contributions in Human-Computer Interaction. *Interactions* 23, 3 (apr 2016), 38–44. DOI:http://dx.doi.org/10.1145/2907069

[222] Irene Woon, Gek-Woo Tan, and R Low. 2005. A protection motivation theory approach to home wireless security. (2005).

[223] Roman V. Yampolskiy and Venu Govindaraju. 2008. Behavioural Biometrics: A Survey and Classification. *Int. J. Biometrics* 1, 1 (June 2008), 81–113. DOI:http://dx.doi.org/10.1504/IJBM.2008.018665

[224] Yaxing Yao. 2019. Designing for Better Privacy Awareness in Smart Homes. In *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing (CSCW '19)*. Presented in Austin, TX, USA. Association for Computing Machinery, New York, NY, USA, 98–101. DOI:http://dx.doi.org/10.1145/3311957.3361863

[225] Yaxing Yao, Justin Reed Basdeo, Smirity Kaushik, and Yang Wang. 2019a. Defending My Castle: A Co-Design Study of Privacy Mechanisms for Smart

Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Presented in Glasgow, Scotland Uk. ACM, New York, NY, USA, Article Paper 198, 12 pages. DOI:http://dx.doi.org/10.1145/3290605.3300428

[226] Yaxing Yao, Justin Reed Basdeo, Oriana Rosata Mcdonough, and Yang Wang. 2019b. Privacy Perceptions and Designs of Bystanders in Smart Homes. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW, Article 59 (Nov. 2019), 24 pages. DOI:http://dx.doi.org/10.1145/3359161

[227] Lihua Yin, Binxing Fang, Yunchuan Guo, Zhe Sun, and Zhihong Tian. 2020. Hierarchically defining Internet of Things security: From CIA to CACA. *International Journal of Distributed Sensor Networks* 16, 1 (2020), 1550147719899374. DOI:http://dx.doi.org/10.1177/1550147719899374

[228] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security & Privacy Concerns with Smart Homes. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS '17)*. USENIX Association, Berkeley, CA, USA, 65–80.

[229] Eric Zeng and Franziska Roesner. 2019. Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA, 159–176. https://www.usenix.org/conference/usenixsecurity19/presentation/zeng

[230] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, and Shiuhpyng Shieh. 2014. IoT Security: Ongoing Challenges and Research Opportunities. In *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*. 230–234. DOI:http://dx.doi.org/10.1109/SOCA.2014.58

[231] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User Perceptions of Smart Home IoT Privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW, Article 200 (Nov. 2018), 20 pages. DOI:http://dx.doi.org/10.1145/3274469

[232] Wei Zhou, Yan Jia, Anni Peng, Yuqing Zhang, and Peng Liu. 2019. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet of Things Journal* 6, 2 (2019), 1606–1616. DOI:http://dx.doi.org/10.1109/JIOT.2018.2847733

[233] Verena Zimmermann, Merve Bennighof, Miriam Edel, Oliver Hofmann, Judith Jung, and Melina von Wick. 2018. 'Home, Smart Home'–Exploring End Users' Mental Models of Smart Homes. In *Mensch und Computer 2018-Workshopband*. Gesellschaft für Informatik e.V., Bonn, Germany, 407–417.

[234] Verena Zimmermann, Paul Gerber, Karola Marky, Leon Böck, and Florian Kirchbuchner. 2019. Assessing Users' Privacy and Security Concerns of Smart Home Technologies. *i-com* 18, 3 (2019), 197–216. DOI:http://dx.doi.org/10.1515/icom-2019-0015

[235] Verena Zimmermann and Karen Renaud. 2021. The Nudge Puzzle: Matching Nudge Interventions to Cybersecurity Decisions. *ACM Trans. Comput.-Hum. Interact.* 28, 1, Article 7 (Jan. 2021), 45 pages. DOI:http://dx.doi.org/10.1145/3429888

[236] Mary Ellen Zurko and Richard T. Simon. 1996. User-Centered Security. In *Proceedings of the 1996 Workshop on New Security Paradigms (NSPW '96)*. Presented in Lake Arrowhead, California, USA. Association for Computing Machinery, New York, NY, USA, 27–33. DOI:http://dx.doi.org/10.1145/304851.304859

Eidesstattliche Versicherung

(Siehe Promotionsordnung vom 12.07.11, § 8, Abs. 2 Pkt. 5)

Hiermit erkläre ich an Eidesstatt, dass die Dissertation von mir selbstständig und ohne unerlaubte Beihilfe angefertigt wurde.

München, den 24. Juni 2022

Sarah Maribel Prange