

Enhancing User Awareness of Privacy Practices during interaction with IoT devices in Mixed Reality

Camilla Becker Bessa Mendes

Participating faculties:

FACULTY OF ENGINEERING

FACULTY OF FINE ARTS

FACULTY OF SCIENCES

FACULTY OF ECONOMICS

FACULTY OF ARTS AND HUMANITIES



Master's in Multimedia - Specialization in Interactive Technologies and Digital Games

Supervisor: Prof. Dr. Maria Van Zeller

Second Supervisor: Prof. Dr. Simon Mayer

June 30, 2025

Enhancing User Awareness of Privacy Practices during interaction with IoT devices in Mixed Reality

Camilla Becker Bessa Mendes

Master's in Multimedia - Specialization in Interactive Technologies and Digital Games

June 30, 2025

Abstract

The growing presence of Internet-of-Things (IoT) devices raises significant privacy concerns, as users often struggle to understand how their personal data is collected and processed. Traditional privacy policies, typically presented as lengthy textual documents, have proven ineffective in promoting user awareness. In response, various visualization approaches, such as privacy labels and icons, have been explored to simplify privacy information. However, these methods lack standardization and widespread adoption.

This thesis investigates the potential of mixed reality (MR) as a novel medium for enhancing privacy awareness in IoT environments. While prior work in extended reality (XR) has shown that augmented reality (AR) can improve privacy comprehension through interactive visualizations, no existing solution aligns with regulatory frameworks, such as the General Data Protection Regulation (GDPR) and the European Union (EU) Data Act, and provides intuitive privacy controls for IoT users.

To address this gap, the study adopted a Design-Based Research (DBR) approach, supported by interdisciplinary collaboration. It presents the design and implementation of an MR-based privacy interface, informed by an online user survey and evaluated through in-person testing. Findings show that participants found the interface useful and reported increased response efficacy when facing privacy risks, suggesting its potential to support privacy awareness.

This research contributes to the field of Human-Computer Interaction (HCI) both methodologically and conceptually. It demonstrates how DBR, combined with user research and expert input, can inform the design of privacy-enhancing technologies. It also explores the feasibility of MR as a medium for privacy management in smart environments.

Keywords: Smart Environments, Smart Devices, IoT, Privacy, MR, Visualisation, Interaction, Usability, HCI

Resumo

O crescimento da presença de dispositivos da Internet das Coisas (IoT) levanta preocupações significativas em relação à privacidade, uma vez que os utilizadores frequentemente têm dificuldade em compreender como os seus dados pessoais são recolhidos e processados. As políticas de privacidade tradicionais, geralmente apresentadas como documentos longos e textuais, têm-se mostrado ineficazes na promoção da consciencialização do utilizador. Como alternativa, diversas abordagens de visualização, como rótulos e ícones de privacidade, têm sido exploradas para simplificar as informações sobre privacidade. No entanto, estes métodos carecem de normalização e ampla adoção.

Esta tese investiga o potencial da realidade mista (MR) como um novo meio para aumentar a consciencialização sobre privacidade em ambientes com dispositivos IoT. Embora estudos anteriores em realidade estendida (XR) tenham demonstrado que a realidade aumentada (AR) pode melhorar a compreensão da privacidade através de visualizações interativas, ainda não existem soluções que alinhem os requisitos regulatórios, como o Regulamento Geral sobre a Proteção de Dados (GDPR) e o Regulamento de Dados da União Europeia, com o fornecimento de controlos de privacidade intuitivos para utilizadores de IoT.

Para abordar esta lacuna, o estudo adotou uma abordagem de Investigação Baseada em Design (DBR), com o apoio de uma colaboração interdisciplinar. Apresenta o design e a implementação de uma interface de privacidade em MR, fundamentada por um inquérito online com utilizadores e avaliada através de testes presenciais. Os resultados indicam que os participantes consideraram a interface útil e relataram um aumento na eficácia de resposta perante riscos à privacidade, sugerindo o seu potencial para apoiar a consciencialização sobre privacidade.

Esta investigação contribui para o campo da Interação Humano-Computador (HCI) tanto metodológica como conceptualmente. Demonstra como a abordagem DBR, combinada com investigação com utilizadores e contribuições interdisciplinares, pode orientar o design de tecnologias voltadas para a proteção da privacidade. Também explora a viabilidade da MR como meio para a gestão da privacidade em ambientes inteligentes.

Palavras-chave: Ambientes Inteligentes, Dispositivos Inteligentes, IoT, Privacidade, MR, Visualização, Interação, Usabilidade, Interação Humano-Computador

Acknowledgements

I would like to express my gratitude to all who have helped me throughout the development of this thesis, both directly and indirectly.

I would like to thank the Interactions Research Group at the University of St. Gallen, where I had the chance to conduct this research. I am especially grateful to prof. Dr. Simon Mayer for trusting me with this opportunity, and Dr. Kimberly Garcia and Jannis Strecker for their support, feedback, and inspiring discussions.

I am deeply thankful to my supervisor, prof. Dr. Maria van Zeller, for the continuous guidance, constructive feedback, and encouragement throughout the entire research process.

Special thanks go to all participants who took the time to complete the survey and take part in the user testing sessions. Their input was essential to the development and evaluation of the prototype.

I would like to dedicate this work to my paternal side of the family, who have recently been through unimaginable loss. They continue to inspire me every day with their strength. Lastly, I would like to thank my partner for being my rock through it all.

Camilla Becker Bessa Mendes

Contents

1	Introduction	1
1.1	Context	1
1.2	Motivation	2
1.3	Objectives and Research Question	2
1.4	Dissertation Outline	3
2	State of the Art	5
2.1	Privacy Notices	5
2.2	Threats to User Privacy in IoT Contexts	9
2.3	Legal Frameworks	10
2.4	Privacy Visualizations	11
2.5	Other Privacy Solutions	14
2.6	Using Extended Reality for Privacy	16
2.7	Privacy perceptions and behaviours	17
2.8	Discussion	19
3	Methodology	21
3.1	Design-Based Research	21
3.2	Literature Review	23
3.3	Consultation with Legal Scholar	24
3.4	Data Collection and Analysis	25
4	Requirements and Design	27
4.1	Privacy Personas	27
4.2	Design tools and challenges	32
4.3	Design of Mockups and the Prototype	35
4.4	Interaction Design Decisions	37
4.5	Visual Identity	41
5	Online Survey	45
5.1	Results	50
5.2	Discussion	59
5.3	Limitations	61
6	User Test with the HoloLens	63
6.1	Results	69
6.2	Baseline Condition	71
6.3	Experimental Condition	72
6.4	Discussion	75

CONTENTS

6.5	Limitations	76
7	Conclusion	77
7.1	Discussion	77
7.2	Limitations	78
7.3	Conclusion	78
7.4	Future Work	79
	Appendix A - User Journey	93
	Appendix B: Earlier version of the user flow chart	94
	Appendix C: Legal Designs	95
	Appendix D: Abandoned Exploratory Analysis	98
	Appendix E: Consent Forms	101
	Appendix F: Online Survey Questions	103
	Appendix G: Questions used in the in-person User Test	113
	Appendix H: Mock "AirBnB"-inspired listing	116
	Appendix I: Experiment Procedure for the in-person User Test (for participants)	118

List of Figures

2.1	Example of a typical cookie and data processing notice on the web. The "Accept all" button is more prominent than other potentially more privacy-preserving options, hidden under "Settings".	6
2.2	An example of a privacy-threatening dark pattern. There is no clear option to deny the use of personal data for marketing purposes.	7
2.3	Colette R. Brunschwig, Visualization of Article 1 Section 1 of the Swiss Code of Obligations.	12
2.4	Two instances of privacy labeling: the label on the right, by Kelley et al., (2009), the one on the left developed by Emami-Naeini et al., (2020).	13
2.5	Icons and corresponding "essential information" statements from Annex 1 to Article 13a of the European Parliament legislative resolution on the GDPR (COM(2012)0011). Adapted from Pettersson (2015).	15
2.6	The interface designs of privacy apps: on the left, the smart home app by Zeng et al., (2019); in the centre, the work by He et al., (2020); on the right, the mobility app by Thakkar et al., (2022).	16
2.7	Two examples of cases related to the topic of this thesis: PARA (Fernandez et al., 2021), and privacy visualizations created for a head-mounted display (Prange et al., 2021).	17
3.1	Diagram of the overall thesis process.	22
3.2	Diagram of the literature review process.	23
3.3	Decision tree by Windl et al. to decide on the best privacy preserving mechanism in the physical world based on the constraints of a situation (Windl et al., 2023).	25
4.1	Amateur persona adapted from descriptions provided by Dupree et al.	29
4.2	Lazy Expert persona adapted from descriptions provided by Dupree et al.	30
4.3	Technician persona adapted from descriptions provided by Dupree et al.	30
4.4	Fundamentalist persona adapted from descriptions provided by Dupree et al.	31
4.5	Marginally Concerned persona adapted from descriptions provided by Dupree et al.	31
4.6	Final version of the user flowchart that informed the creation of the prototype.	33
4.7	Alce et al. (2017) design of a floating menu.	34
4.8	Our screen displays to the user the devices found in the room. The number of devices would be scalable by adding navigation arrows and a pagination indicator, similar to 4.7.	35
4.9	Figma screenshot showing a part of the workflow for designing the mockups.	36
4.10	Figma screenshot displaying part of the workflow for designing the prototype.	37
4.11	The menu included in the prototype.	38

LIST OF FIGURES

4.12	The optimal zone for hologram placement as recommended by Microsoft. Image by Microsoft.	39
4.13	Unity screenshot showing a part of the workflow for designing and implementing the prototype.	39
4.14	HoloLens 2, image provided by Microsoft.	40
4.15	Colours used in the design of the MR app.	42
4.16	Typography used in the design of the MR app.	42
4.17	Icons depicting a vacuum cleaner, a TV, a dehumidifier, lights, and a speaker, all used in the final prototype of the app.	42
4.18	Results of the contrast check between text and background colours used in the interface. The tool confirmed that accessibility standards were met for legibility. .	43
5.1	"UI1": "Turn off all devices" Screen – Designed for Technicians, who were hypothesized to prefer direct control over all IoT devices.	46
5.2	"UI2": "Parameters" Screen – Designed for Fundamentalists, who were hypothesized to aim for detailed customization of privacy settings.	46
5.3	"UI3": "Scan" Screen – Designed for Lazy Experts, who were hypothesized to want a quick overview of connected devices with minimal effort.	47
5.4	"UI4": "Protect" Screen – Designed for Amateurs, who were hypothesized to require guidance and simple privacy options. The Marginally Concerned persona was not assigned a specific UI, as this group is characterized by a lack of motivation to engage with privacy-related tools. It is hypothesized that individuals who identify with this persona would not actively use such a system.	47
5.5	Example of a question of the online user survey.	48
5.6	Average UI rating per persona group, showing that the initial hypothesis was incorrect.	57
5.7	Participant answers to the question "Would an application like this be useful for you?"	57
5.8	Participant answers to the question "Would having access to such an application make you feel safer?"	58
5.9	Participant answers to the question "How frequently would you use this application?"	58
6.1	The "Living Lab" of the Institute of Behavioural Sciences at the University of St. Gallen in St. Gallen, Switzerland.	64
6.2	A smart vacuum cleaner, one of the objects used in the in-person user test.	65
6.3	Smart lights interface, where users can adjust their privacy preferences by disconnecting the device from Wi-Fi, or disabling its presence detection capabilities. . .	66
6.4	Smart dehumidifier interface, where users can adjust their privacy preferences by disconnecting the device from Wi-Fi, or disabling its voice control or presence detection capabilities.	66
6.5	Smart speaker interface, where users can adjust their privacy preferences by disconnecting the device from Wi-Fi, or adjusting the microphone level. Note that a help button was also included in case users did not understand the meaning of "microphone level" and how it impacts privacy. If clicked, a help screen would open with a simple explanation.	67
6.6	Smart vacuum cleaner interface, where users can adjust their privacy preferences by disconnecting the device from Wi-Fi, or disabling its camera capture.	67

LIST OF FIGURES

6.7	Smart TV interface, where users can adjust their privacy preferences by disconnecting the device from Wi-Fi, or adjusting the microphone level. Note that a help button was also included in case users did not understand the meaning of "microphone level" and how it impacts privacy. If clicked, a help screen would open with a simple explanation.	68
1	User journey mapping the process of encountering privacy-threatening smart devices in rental homes.	93
2	Early version of the user flowchart representing the steps of VISTA.	94
3	This screen lets users know that it is not possible to influence the data collection of a smart device (here, a camera) due to legitimate interest. The user can then choose to learn more about legitimate interest, click a button to "see options", or exit. "See options" would make the system suggest alternative measures, such as switching off a router.	95
4	Screen warning users that it is not possible to influence the data collection of a particular device. This could be due to contractual necessity, for instance. In this case, the system would suggest alternative solutions found in the environment, such as switching off the router, as shown above.	96
5	This screen explains to a user the meaning of the term "legitimate interest". . . .	97
6	Consent form used in the online user survey.	101
7	Consent form used in the in-person user test.	102
8	Mock "AirBnB"-inspired listing used in the in-person user test.	116
9	Experiment procedure outlining to participants the steps of the experiment. . . .	118

LIST OF FIGURES

List of Tables

5.1	Familiarity with AR, VR, and Smart Devices, and Device Ownership	51
5.2	Spearman's Rank Correlation Between Familiarity with AR and VR, and User-Centered or Object-Centered UI preference.	51
5.3	Spearman's Rank Correlation Between Familiarity with AR, VR, and IoT, and UI Ratings.	52
5.4	Mann-Whitney U Test Comparing UI Ratings by IoT Ownership.	52
5.5	Average IUIPC scores, standard deviations, and coefficients of variation.	53
5.6	Average IUIPC Statement Scores by Persona.	53
5.7	Kruskal-Wallis Test Results, followed by Dunn's test with Bonferroni correction for IUIPC Statements by Persona.	54
5.8	Participant Self-Identification with Privacy Personas.	54
5.9	Participant Preference of Mascot and Icons.	55
5.10	Comparison of General Preference Between User-Centered and Object-Centered UIs.	55
5.11	Average Satisfaction Scores and Significant Differences (Bonferroni-adjusted). .	56
5.12	Results of the free-text question ("Why would you use such an application? For which purpose?") included in the online survey. This analysis was done using the Braun & Clarke method (Braun&Clarke, 2006).	60
6.1	Familiarity with AR, VR, and Smart Devices, and Device Ownership	69
6.2	Average IUIPC scores and standard deviations by category	70
6.3	Participant Self-Identification with Privacy Personas	70
6.4	Semi-structured interview after the baseline condition: codes, definition, participant quotes, and count. This analysis was done using the Braun&Clarke method (Braun&Clarke, 2006).	71
6.5	Scores for Self-efficacy and Response efficacy after the baseline condition. . . .	72
6.6	Semi-structured interview after the experimental condition: codes, definition, participant quotes, and count. This analysis was done using the Braun&Clarke method (Braun&Clarke, 2006). (Part 1)	73
6.7	Semi-structured interview after the experimental condition: codes, definition, participant quotes, and count. This analysis was done using the Braun&Clarke method (Braun&Clarke, 2006). (Part 2)	74
6.8	Scores for Self-efficacy and Response efficacy after the experimental condition. .	74
6.9	SUS results.	75
6.10	Paired t-test results comparing Baseline and Tech conditions (n = 20).	75
1	Persona assignments across three survey formats in the exploratory pilot (Top and 2nd result)	100

LIST OF TABLES

Abbreviations

AR	Augmented Reality
GDPR	General Data Protection Regulation
HCI	Human-Computer Interaction
IoT	Internet of Things
MR	Mixed Reality
MRTK3	Mixed Reality Toolkit 3
SHPPB	Smart Home Privacy-Protective Behaviors
UI	User Interface
UX	User Experience
VR	Virtual Reality
XR	Extended Reality

Chapter 1

Introduction

1.1 Context

Today, humans are being tracked more than ever. As digital information becomes an increasingly central and valuable resource, new ways of monitoring human activity appear in our surroundings through sensors. Internet of Things (IoT) devices are common carriers of these sensors. By the end of 2024, the number of IoT devices was expected to reach 18.8 billion. While the data tracked might facilitate and personalize different tasks and services, it poses significant risks to privacy. For example, sensitive information might be inferred, or identities might be disclosed.

Privacy is “the ability of an individual to control the terms under which their personal information is acquired and used” (Culnan, 2000). Privacy is a fundamental human right, as stated in the Universal Declaration of Human Rights. The protection of this right is covered in the European Union by the General Data Protection Regulation (GDPR), one of the world’s strictest sets of privacy laws. Additionally, the Data Act, set to become applicable in September 2025, reinforces the need for businesses to handle user data privately and fairly. Taking into account these provisions, promoting privacy in digital services is more important than ever.

In order to inform users and facilitate the protection of one’s privacy, this project aims to find suitable design solutions for those interacting with IoT devices. Extended reality (XR) serves as the medium through which this goal is pursued. XR is an umbrella term that covers Augmented Reality (AR), Mixed Reality (MR), and Virtual Reality (VR). This thesis explores the use of MR to mediate the interaction between humans and IoT devices.

An MR environment is one in which the physical world and virtual world objects and stimuli are presented together within a single percept (Skarbez et al., 2021). This means that when a user simultaneously perceives physical and virtual content, potentially across different senses, they are experiencing mixed reality. This thesis considers that using MR to simplify the finding and managing of IoT devices in the context of privacy presents a meaningful opportunity for research.

Recent advances in XR technology show its potential for assisting individuals in diverse daily life activities, such as getting directions while walking or receiving reminders while shopping.

This hands-free, context-aware support could also help protect privacy by making users more aware of when and how their personal data is being collected.

This work was conducted in collaboration with the University of St. Gallen's Interactions Research Group in St. Gallen, Switzerland, where the author stayed for several months to complete the work done for this thesis.

1.2 Motivation

Mark Weiser envisioned in his 1991 “The Computer for the 21st Century” essay that computers will eventually be so embedded in everyday life that they will hardly be noticeable anymore (Weiser, 1991). This idea of *ubiquity* denotes the seamless incorporation of computation into objects and environments in a way that users hardly perceive the presence of the technology. The notion of ubiquity and the rise in the number of IoT devices lead to a substantial increase in privacy risks (Bellotti & Sellen, 1993). Users might be unaware of the presence of these devices in environments such as smart offices or smart homes, and not recognize the privacy risks that the devices pose.

Privacy notices pose their own challenges. Users commonly face difficulties in comprehending the privacy practices of products and services, since privacy notices are typically lengthy and use complicated legal jargon (MacLean, 2016). In the case of IoT devices, retrieving these notices may be even more challenging since many devices lack a traditional user interface, and in public or shared spaces, it can be hard to identify which exact product is collecting data and where its notice lives.

Tackling these issues means encouraging a fairer and more user-friendly way of displaying and managing privacy practices. This project aims to achieve just that by focusing on the user scenario of uncovering IoT devices in a rental home (e.g., AirBnB or similar rental home services) and managing one's privacy preferences in that context. In this way, users gain greater awareness of privacy practices and protect their personal data accordingly.

1.3 Objectives and Research Question

The main objectives of this dissertation are to:

- Understand the different user preferences and behaviors related to privacy, especially in the context of the use of IoT devices.
- Explore how privacy notices can be effectively communicated to users in MR settings.
- Identify MR design elements that enhance user awareness of privacy practices during interactions with IoT devices.
- Evaluate the usability and effectiveness of the proposed design solutions through user testing and iterative design.

Introduction

To achieve these goals, this work explores the following research question:

”What are the most effective design elements to enhance user awareness of privacy practices during interaction with IoT devices in MR?”

This dissertation adopts a Design-Based Research (DBR) methodology to create an MR privacy app that empowers users to manage their privacy preferences when interacting with IoT devices. User needs and privacy requirements drove each phase of ideation, prototyping, and evaluation. Moreover, design decisions have been partially informed by regulatory frameworks, specifically the GDPR and the EU Data Act. Finally, the design of the app is also based on an extensive literature review and interactions with fellow researchers, including a legal scholar.

To explore visual methods for presenting privacy information, this research adopted a user-centered approach, drawing on established privacy personas from the literature. Since Rossi and Palmirani indicated that most privacy visualisation methods fall short due to not being user tested (Palmirani & Rossi, 2017), this work prioritized user testing from the start. An online questionnaire was sent to 150 participants to analyse user preferences and inform the design of a mixed reality privacy interface. This survey included mockups, which participants evaluated to provide feedback on design elements. Based on these findings, a prototype was developed and subsequently tested in-person with 20 participants to assess its usability and effectiveness.

The thesis makes a significant contribution to the field of Human-Computer Interaction, and more specifically to the design of privacy interfaces for XR apps. The results found here highlight the potential of MR for assisting users in visualizing privacy risks, as well as increasing one’s sense of efficacy when responding to such threats.

1.4 Dissertation Outline

This thesis is divided into seven chapters. The current Chapter 1 introduces the topic, outlining the research motivation, its objectives, and the research question. Chapter 2 presents the literature review, highlighting research on privacy in the context of emerging technologies. Chapter 3 presents the methodology, namely DBR.

Chapter 4 describes the design process, as well as design challenges encountered during development. Chapter 5 presents the methodology and results of the online user survey. Chapter 6 examines the HoloLens user test, including its experimental procedure and findings. Chapter 7 concludes this research by summarizing and discussing the main contributions, as well as analysing its limitations and suggesting relevant topics for future research.

Introduction

Chapter 2

State of the Art

This section introduces and discusses the state of the art in privacy in the context of emerging technologies, specifically IoT devices. It focuses on user interactions with these devices, both in physical reality and in XR environments. The chapter begins with a detailed overview of the challenges associated with privacy notices and other relevant legal frameworks. This is followed by an introduction to privacy visualizations and the development of privacy labels and icons. An overview of privacy perceptions and behaviours commonly found is additionally included.

The immersive nature of XR technology also introduces unique privacy challenges (Hadan et al., 2024). XR headsets have sensors such as cameras, microphones, or eye trackers that might have a negative impact on the privacy of a user. For example, VR headsets with cameras can record personal spaces, microphones can record private conversations, and eye-tracking technology can track eye movements (Fineman & Lewis, 2018). While these biometric data might enhance personalisation and thus user experience, they can also be privacy-invasive.

However, the challenges related to privacy in the context of XR fall outside the scope of this thesis. In the scenario chosen for this analysis, namely the rental home scenario (to be described in more detail in Chapter 4), the mixed reality glasses are considered to be trusted by their user. In this way, the main focus of this project is rather on the interaction with smart devices and how these can be privacy-threatening. The XR technology serves merely as a medium through which this interaction happens.

2.1 Privacy Notices

A privacy notice is a statement provided to data subjects that explains how an organization collects, uses, retains, and discloses their personal information. Often called a privacy statement, fair processing statement, or a privacy policy ¹, privacy notices are mandated by numerous privacy and data protection laws around the world (International Association of Privacy Professionals, n.d.). In

¹A privacy policy is an internal statement that outlines how an organization manages personal information. It guides employees and decision-makers on proper procedures for collecting, using, storing, and disposing of data, and details the rights afforded to data subjects. Note that “privacy policy” and “privacy notice” are sometimes used interchangeably.

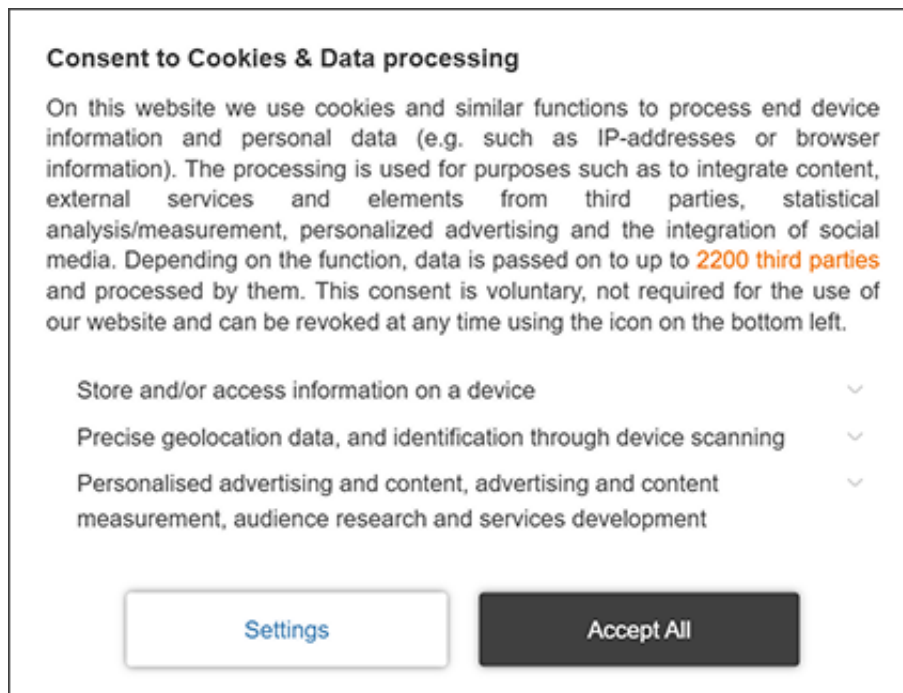


Figure 2.1: Example of a typical cookie and data processing notice on the web. The "Accept all" button is more prominent than other potentially more privacy-preserving options, hidden under "Settings".

digital contexts, privacy notices often appear as lengthy on-screen text blocks or pop-up dialogs, often along a cookie notice, and terms of use.

"Cookies" refer to text files that websites store on a user's device during their visit. These files typically contain information such as a unique identifier, which enables websites to recognize returning users and tailor their experiences accordingly (ICO, n.d.). Cookie notices typically require users to click "Accept All," "Reject All," or "Manage Preferences," leading them into a preference menu where they can toggle categories like "Analytics" or "Marketing." Similarly, terms of use agreements may present clickable check boxes or "I Agree" buttons. Figure 2.1 is an example of a pop-up notice typically found on the web.

Privacy notices are frequently ignored by online users. "I accept the terms of use" has been cited as "the biggest lie on the Internet" (Obar & Oeldorf-Hirsch, 2020) or as a "legal fiction" (MacLean, 2016). The reasons why people do not read privacy notices vary, but their extensive length, difficult language, and the presence of dark patterns might help explain this phenomenon. In 2008, it was found that if every American internet user took the time to read all the privacy notices they encountered daily, the total value of the time spent doing so would amount to approximately 781 billion dollars. This estimate is based on the idea that time spent reading these notices could have been used for other productive activities, such as work (McDonald et al., 2008).

The Privacy Project, an initiative by The New York Times, compared the readability of classic literature to that of privacy notices (Litman-Navarro, 2019). They found that Facebook's privacy notice was one of the most difficult texts analyzed, with only Immanuel Kant's *Critique of Pure*

Reason ranking as harder to read. Google's privacy notice took an average of 30 minutes to read, further exemplifying the excessive time required to go through these documents.

Dark patterns are "user interface design choices that benefit a service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions" (Mathur et al., 2019). Figure 2.2 is an example of a dark pattern. Designers may employ dark patterns to deliberately hinder users from implementing their privacy choices (Waldman, 2020). Some dark patterns associated with privacy include: privacy default settings that expose user data, privacy options that are hard to find, and the use of emotionally charged language to drive users away from making privacy-respecting choices (Mathur et al., 2021).

A Consent Management Platform (CMP) is a tool used by companies to collect and manage user consent required for processing personal data. In an analysis of 680 websites that use CMPs, a study found that in over 88% of them there were pre-ticked boxes, rejecting privacy notices was more difficult than accepting them, and consent was implicit (Nouwens et al., 2020). These dark patterns violate principles outlined by the GDPR.

Since users decide on the spot and on a case-by-case basis whether to agree or disagree with a privacy notice, their choice is influenced by the way the information is presented. Thus, if the information is framed in a way that induces users to agree to it and the "agree" button is visually highlighted, because of inattention, cognitive, and physical laziness, users are likely to comply with the conditions (Bellman et al., 2001).

Essentially, privacy policies were never meant to be a consumer tool (Litman-Navarro, 2019), having been created by lawyers to protect companies, but they are still used as privacy notices. At the same time, they are often the primary way users can learn about their privacy rights concerning specific products or services. Considering that people tend not to read privacy notices, their use is inefficient at best and useless at worst. In the end, users remain uninformed and vulnerable.

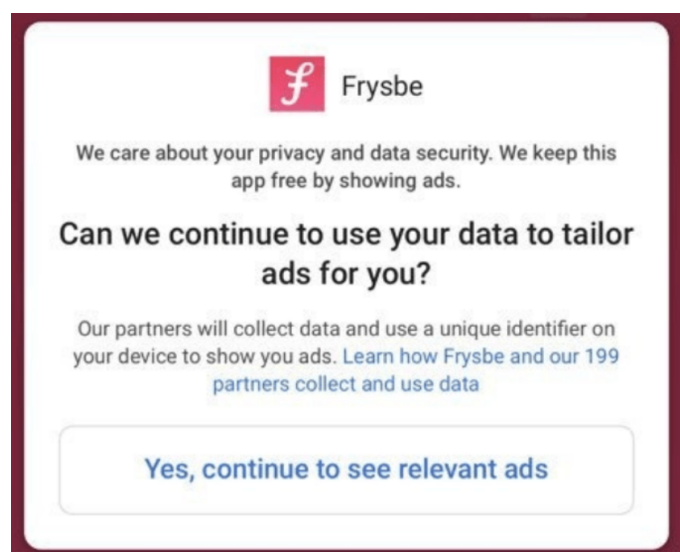


Figure 2.2: An example of a privacy-threatening dark pattern. There is no clear option to deny the use of personal data for marketing purposes.

Privacy notices can take a variety of forms depending on how and when they engage users. Broad, all-in-one notices attempt to cover several data practices up front, but might overwhelm users with length and complexity. Layered notices seek to alleviate this by presenting a concise "primary layer" first, with an optional "second layer" with more detailed sections (Emami-Naeini et al., 2020). Other approaches include icon-based or tabular summaries that use graphics or labels to convey the most important points intuitively.

In the IoT context, where devices may lack a screen or traditional interface, some manufacturers publish their notices exclusively on a companion app or website, while others include minimal notices directly on the device. Each privacy notice format currently available presents its own benefits and challenges for discoverability, comprehension, and transparency. A summary of common privacy notice models is found below.

- **Notice and choice**

Notice and choice is the most common way of presenting privacy information online today (Sloan & Warner, 2014). "Notice" is the privacy notice itself, while "choice" is typically an "I agree" or "I disagree" button that follows. However, this approach might not be ideal for fulfilling the GDPR notion of informed consent. Many online users click "accept" simply to clear their path, ignoring the notice and its intended value (Stewart, 2019).

This behaviour can lead to consent fatigue. Consent fatigue can occur when users are repeatedly asked to agree or disagree to terms, and begin to accept defaults without reflecting on their implications (Schermer et al., 2014). Designing better consent flows means reducing the number of associated steps by providing fair defaults and offering granular controls, so users can change permissions to their desired level rather than being forced into black and white decisions.

- **Opt-in and Opt-out models**

Privacy frameworks typically adopt either opt-in or opt-out models for data collection. An opt-in model requires user action before any personal information is captured or processed. In contrast, an opt-out model presumes consent by default, requiring the user to take action to disable or withdraw data collection. These opt-out controllers are often hidden behind settings or multiple menu layers. Under the GDPR, opt-in is the preferred standard for sensitive data. See the GDPR guidelines on consent for more information ².

- **Just-in-Time notices**

Just-in-Time (JIT) notices deliver privacy-related explanations and permission requests when a feature is about to be used (Schaub et al., 2015). JIT notices pop up contextually, e.g., "This camera is about to record audio. Tap 'Allow' to continue." By tying the request directly to its consequence, JIT notices can improve users' understanding of why data is needed and how it will be used. However, poorly designed JIT prompts might still present

²See "Consent" in <https://gdpr-info.eu/issues/consent/>

issues if they fire too frequently, or confuse users if the timing or wording is unclear. In MR and other XR scenarios, JIT elements may appear as spatial overlays.

- **Modality**

Privacy notices can be presented to users in different modalities, such as visual, auditory, haptic, machine-readable, or combined formats (Feng et al., 2021). As previously described, the current paradigm for privacy notices is a textual, notice-and-choice model. A textual model fits under the visual modality. This thesis mostly explores visual forms of displaying privacy notices, following the current paradigm. However, other modalities have been explored and might perform effectively in other contexts, as well as be more accessible to certain groups of users (e.g., auditory notices, such as warning sounds, might be more accessible to deaf users).

2.2 Threats to User Privacy in IoT Contexts

IoT refers to the concept of connected objects and devices, whether wireless or not, that communicate over the Internet (Tawalbeh et al., 2020). IoT devices are sometimes (including in this thesis document) referred to as "smart devices", as this term might be more accessible to the general public. IoT devices carry privacy risks due to their collection, transmission, and sometimes storage of personal data, often with limited security protections.

Individuals might at times no longer be *users* of IoT devices but are rather *subjects* of these devices (Chow, 2017). This notion, closely related to the idea of "bystanders", means that people might have their data captured by devices that are not their own by simply being present in a smart environment. "Bystanders" might also be unaware of the capture of their data. An example is a scenario in which smart surveillance cameras record individuals walking down the street in smart cities.

Another key issue is that because this technology is fairly new, users have not yet developed accurate mental models of how to protect their privacy and security when interacting with these interfaces (Williams, Nurse & Creese, 2017). Since the user interface of smart devices may be different from interfaces users might be accustomed to (e.g., modern computer interfaces), they might find it more difficult to use and navigate them (Rowland et al., 2015).

The interconnectivity of these devices further aggravates privacy risks, since data collected in one context can be accessed or shared across multiple platforms, increasing the likelihood of privacy breaches and loss of control over personal information (Ziegeldorf, Morchon & Wehrle, 2014). This problem might be exacerbated in smart homes, smart offices, or smart schools, where there is a higher concentration of smart devices. To use and administer privacy preferences across multiple devices in this context proves to be another key challenge.

An online survey showed that users worry more about privacy in scenarios in which multiple smart devices are interconnected. However, the same survey also indicated a lack of understanding or inaccurate mental models of privacy-relevant processes (Windl et al., 2024a). Participants did

not fully grasp which entities handle their data when interacting with IoT devices, for example. This shows that privacy policies are insufficient in informing users about privacy in the context of smart devices (Windl et al., 2024a).

These challenges are not exhaustive, and as the technology evolves, other issues may arise. All of the challenges mentioned above call for privacy solutions that empower users to have more control over their privacy, and for user-friendly interfaces that allow users to learn more about and administer their privacy in the context of smart device use.

2.3 Legal Frameworks

This section outlines two of the most relevant privacy legal frameworks: the GDPR and the EU Data Act. The GDPR is a set of security and privacy laws. It was drafted and passed by the European Union and put into effect in May 2018. The GDPR applies to any organization around the globe that targets or collects data related to people in the EU. Harsh penalties are imposed on those who violate the provisions of the GDPR.

As shown in the previous section, privacy policies and the way they are displayed at times challenge the key principles of the GDPR. Individuals often consent to the use of their data without properly reading these policies. However, the GDPR has strict rules on what constitutes consent from a data subject, such as:

- Consent must be “freely given, specific, informed, and unambiguous.”
- Requests for consent must be “clearly distinguishable from the other matters” and presented in “clear and plain language.”
- Data subjects can withdraw previously given consent whenever they want, and their decision has to be honored.

The GDPR further recognizes a series of privacy rights for data subjects, such as the right to be informed, the right of access, the right to erasure, and the right to object. Complying with the provisions of the GDPR and these rights is important not only for avoiding legal and financial problems, but also for ensuring fairer digital environments. Even though technologies such as IoT devices and extended reality are still relatively new, it is important from now on to consider the legal frameworks surrounding privacy in these contexts, and to respect these provisions.

The Data Act is an initiative that addresses the challenges presented by data in the European Union. These laws entered into force in January 2024, and will become applicable in September 2025. The act establishes rules for accessing and using data, a necessity heightened by the growing prevalence of smart devices (European Commission, 2024).

In practice, the act gives individuals and companies the right to access the data produced during their utilization of IoT devices. Before finalizing contracts for the purchase or lease of connected products, sellers are required to clearly inform users about the type, format, and volume of data

the product will generate, whether it collects data in real-time, and where and for how long the data will be stored.

Additionally, sellers must specify the methods for accessing, retrieving, or erasing the data, along with the technical means and terms of use. This approach aims to ensure transparency, user control over personal data, and alignment with the principles set forth in the GDPR. Similarly to the GDPR, the Data Act emphasizes transparency, ensuring user participation and understanding of how their data is handled.

2.4 Privacy Visualizations

Privacy visualizations, such as tables or icons, emerge as an alternative to traditional textual privacy policies. They are an attempt to solve the issues surrounding privacy notices as described earlier. Additionally, visualizations can be used to make users more aware of the presence of IoT devices in their surroundings and gain a better understanding of the privacy risks of these devices. The idea of using privacy visualizations is central to this thesis. In the following paragraphs, the new field of legal design is explored, as well as common design strategies that tackle this issue.

Legal design is a relatively new interdisciplinary field that brings concepts of user-centered design to law (Hagan, 2020). One key aspect of legal design concerns language. As analysed earlier, the language used in legal texts (such as privacy notices) is often difficult for the general public to comprehend (Mellinkoff, 2004). To simplify this process and make it more user-friendly, some authors have proposed ways of visualizing legal texts, in the form of comics (Brunschwig, 2019), icons (Efroni et al., 2019), or simply colour-coding and highlighting certain areas of the text (Passera, 2012; Passera & Haapio, 2013). Figure 2.3 is an illustration created by Brunschwig of an article of the Swiss Code of Obligations.

The GDPR reinforces the notion that information related to data processing must be presented in a concise and transparent manner in Article 12 (1). These laws go even further by suggesting visualizations. Article 12 (7) is the first instance in the history of the European Union in which the potential of icons to enhance individuals' understanding of data practices and their decision-making is acknowledged (Rossi et al., 2017). Overall, there seems to be a general trend toward visual legal communication (Brunschwig, 2014).

Considering privacy notices only, there is evidence that visualizations lead to higher privacy awareness levels than conventional textual policies, especially when icons are included (Soumelidou & Tsohou, 2020). Another approach to visualizing privacy notices is through labels. Inspired by nutrition, warning, and energy labeling, in 2009, Kelley et al. developed a privacy label for the web that presented to users how organizations collected, used, and shared personal data. This was an attempt to represent privacy notices in a visual, more engaging way (Kelley et al., 2009).

Other attempts to create privacy labels followed, including the work of Emami-Naeini et al., which was academically and politically well-received (Windl et al., 2024b) by the community. This label was created specifically for IoT products and is meant to be included in physical product

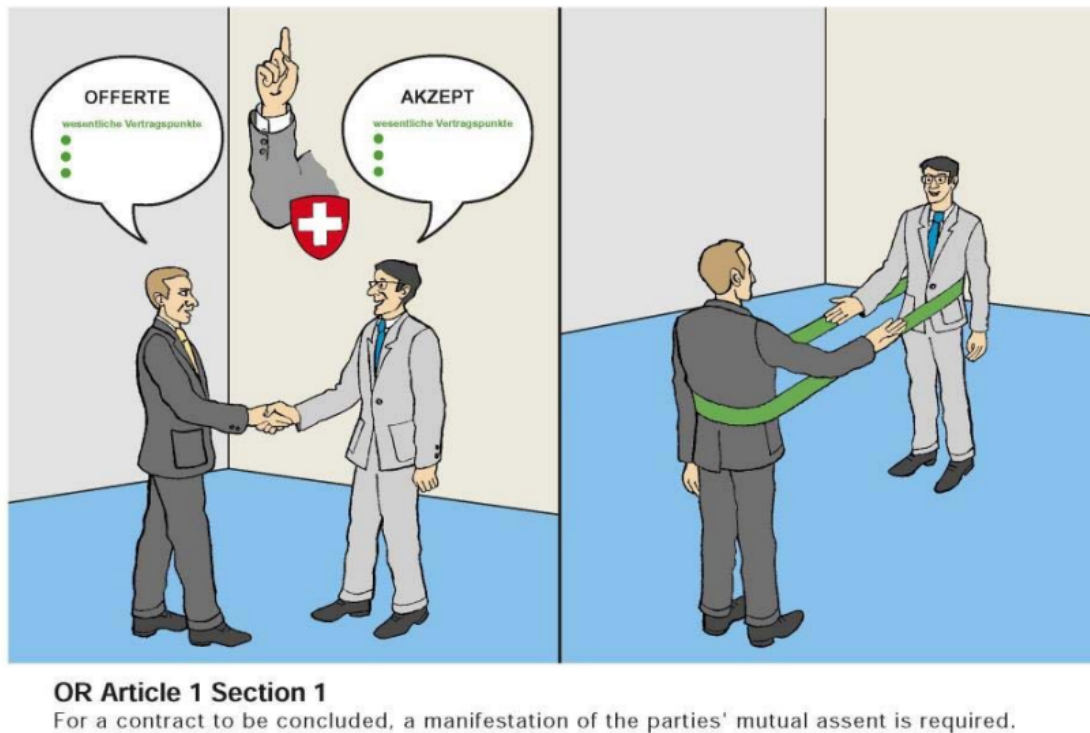


Figure 2.3: Colette R. Brunschwig, Visualization of Article 1 Section 1 of the Swiss Code of Obligations.

packaging (Emami-Naeini et al., 2020). It "set the scene" for privacy-related communication of IoT features (Windl et al., 2024b).

Another related instance is a privacy label tailored to dog-related smart devices that informs consumers about privacy concerns that might affect individuals, since through animal data, one might be able to infer human data (McParlan & Van Der Linden, 2021). For example, data collected from a smart dog leash might be able to reveal patterns about an owner's location, routines, and lifestyle, thereby posing indirect privacy risks. Figure 2.4 shows two influential privacy labels, one created by Kelley et al. and the other one by Emami-Naeini et al.

Labeling allows for the creation of primary and secondary layers. The primary layer includes the most important information concerning privacy, while an optional secondary layer provides users with more context or clarity in case they feel the need to know more. A secondary layer might be accessible through a QR code or a website, for example. These layers accommodate the needs of different user profiles, since they offer the essential information to users who might be satisfied with the basics, while also responding to the preferences of users who might have more concerns.

Barth et al. designed a colour-coded label with ratings from A to G to empower users to become more knowledgeable and aware of online privacy (Barth et al., 2021). Twelve categories were identified by experts and separated into four main groups (collection, sharing, control, and security). User research focused on usability, perceived usefulness, and effects on trust showed

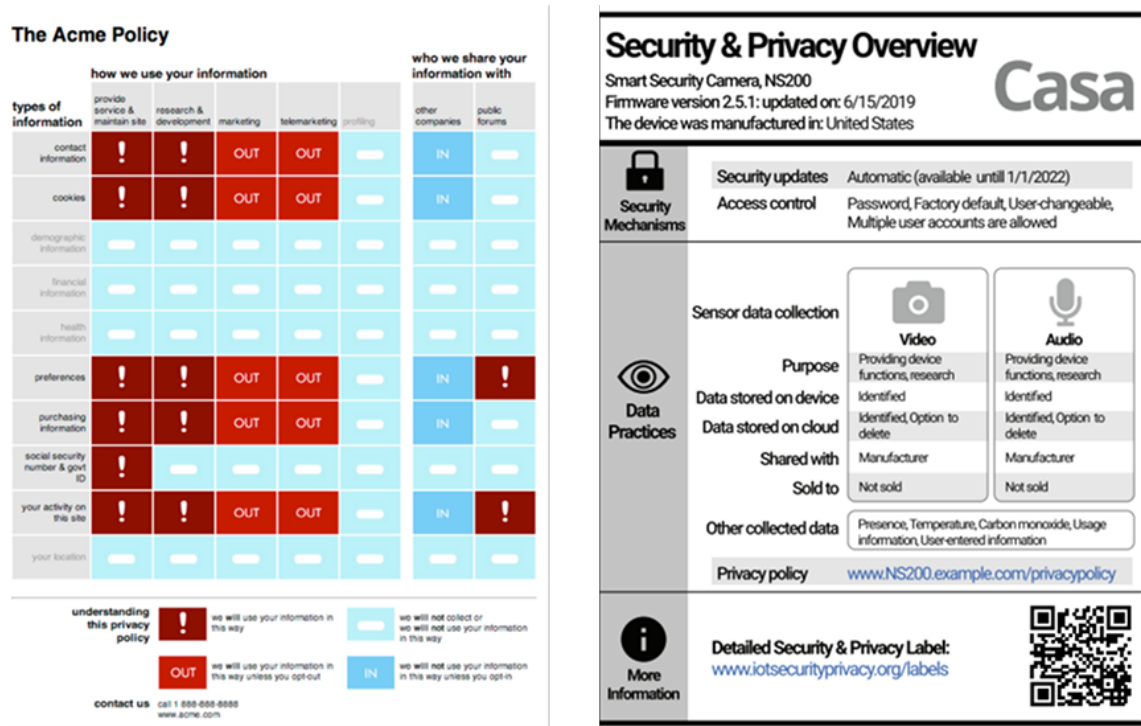


Figure 2.4: Two instances of privacy labeling: the label on the right, by Kelley et al., (2009), the one on the left developed by Emami-Naeini et al., (2020).

that users would like this type of visualization to become an established standard (Barth et al., 2021).

Providing a way for users to compare device configurations (e.g., numerical grades or a star system) in the context of privacy might be useful. However, using rankings or measurable metrics like Barth et al.'s A-to-G rating proves to be challenging because, to date, there is no independent third-party analysing these metrics and no established way to visualize this data (Windl et al., 2024b).

More recently, attempts to create digital interactive versions of these labels followed, such as Windl's label for IoT devices (Windl et al., 2024b). This label is intended to provide users with information about more advanced device configuration options, such as sensor states and device connectivity. These authors found that most participants successfully used the label and retrieved sensor information efficiently and correctly, showing the potential for this type of labeling. Making the label interactive, however, implicates that more attention is required to accessibility (Windl et al., 2024b).

Outside of academia, other initiatives attempted to create IoT ranking, certificates, or labeling. For more information on other initiatives, see ³. Despite academic and private efforts, these labels

³A non-exhaustive list of organizations that have created IoT labels or certificates includes: UL solutions (<https://www.ul.com/services/ul-verified-iot-device-security-rating>); Your Things (<https://yourthings.info/scorecards/>); Mozilla's Privacy Not Included (<https://foundation.mozilla.org/en/privacynotincluded/>).

have not been widely adopted or standardized by public entities. Recently, the Biden administration announced the U.S. Cyber Trust Mark program, an initiative that aims to equip smart devices that meet government security standards with a label. While the initiative has been announced, it has not yet been launched, and it is unclear when this will take place in the Trump administration (Federal Communications Commission, 2025).

Privacy icons can be understood as standardized, intuitive pictograms that illustrate data processing risks, ideally enhancing user understanding and informing decisions (Efroni et al., 2019). In 2013, a document from the European Parliament included six icons designed to convey privacy policy elements to users. However, these icons were not well-received, and a study showed that participants demonstrated difficulties in interpreting them and associating them with privacy (Pettersson et al., 2015). Some of these icons are included in Figure 2.5.

Other authors attempted to create sets of icons for indicating privacy preferences and achieved mixed results among participants (Ianella & Finden, 2010). With the implementation of the GDPR in 2018, no standard for privacy icons followed. It is still unclear which set of icons might be able to realize the visualization suggestion of the GDPR (Rossi & Lenzini, 2017).

Any set of proposed icons so far lacks widespread adoption. A reason for this rejection might be fear of misunderstandings or misrepresentations of the nuances of legal concepts that are normally showcased in natural language (Rossi & Palmirani, 2017). Nevertheless, there are benefits to adopting icons. Icons can express meanings independently of literacy or language barriers (Efroni, 2019). Furthermore, standardized privacy icons would allow for comparison between entities, which could lead to more user awareness (Efroni, 2019).

With the benefits in mind, it is still relevant to consider the challenges associated with the use of icons. Icons are not necessarily universally understood and might be culture-dependent (Nielsen, 2003). Besides, frequent and widespread exposure to icons could result in user habituation (Efroni, 2019) and diminish the perception of privacy risks.

It is generally understood that privacy icons would not substitute privacy notices (Holtz et al., 2011), but rather complement them. When designing such icons, the legibility of the elements of the graphical symbol, the familiarity with the corresponding concept, and the learnability of the graphical language need to be considered (Rossi & Lenzini, 2017).

2.5 Other Privacy Solutions

Not particularly focused on visualizations, other solutions have been explored to convey privacy practices. The next few paragraphs outline some of them. PriKey, a tangible user interface in the shape of a key, allows users to control and configure sensor settings (Delgado Rodriguez et al., 2022); PriBot, a bot that delivers privacy notice and choice through a dialogue between a user and a computer agent (Harkous et al., 2016); and several prototypes for mobile apps have been created.

Some of these apps include: a smart home app with features such as location-based access controls, supervisory permissions, and activity notifications (Zeng et al., 2019); an app in which users manually adjust their privacy settings across various IoT devices (He et al., 2020); an app

ICON	ESSENTIAL INFORMATION
	No personal data are collected beyond the minimum necessary for each specific purpose of the processing
	No personal data are retained beyond the minimum necessary for each specific purpose of the processing
	No personal data are processed for purposes other than the purposes for which they were collected

Figure 2.5: Icons and corresponding “essential information” statements from Annex 1 to Article 13a of the European Parliament legislative resolution on the GDPR (COM(2012)0011). Adapted from Pettersson (2015).

that helps users discover nearby IoT devices and generates privacy notices (Das et al., 2018). Mohammadi created interface design patterns for mobile apps with the goal of giving users a chance to select their privacy preferences in an intuitive way (Mohammadi et al., 2019). The interfaces of three of these apps are included in Figure 2.6.

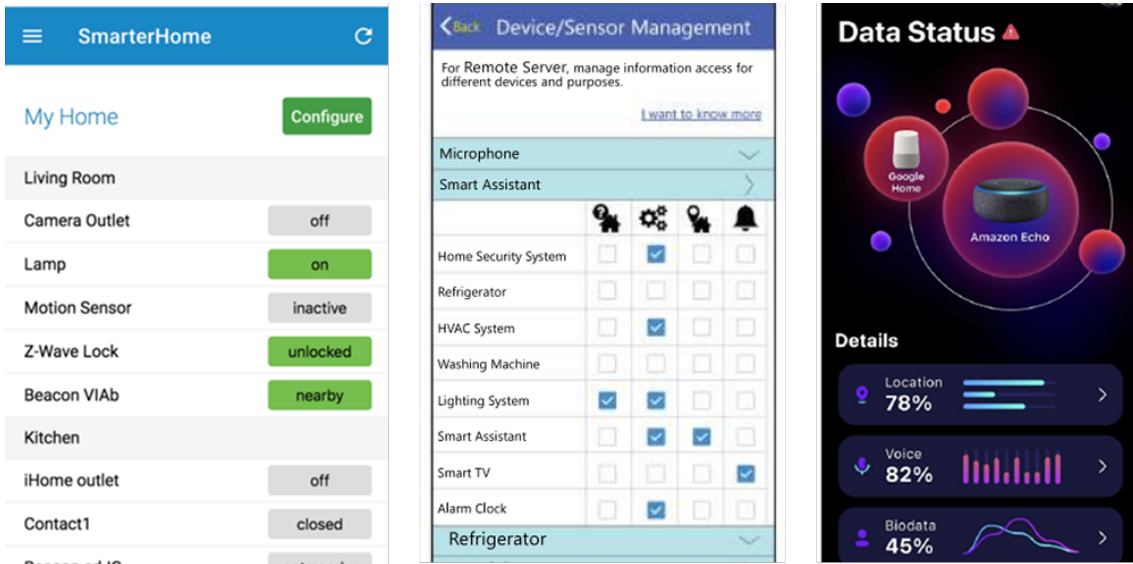


Figure 2.6: The interface designs of privacy apps: on the left, the smart home app by Zeng et al., (2019); in the centre, the work by He et al., (2020); on the right, the mobility app by Thakkar et al., (2022).

Another study explored ways to inform users and bystanders about data collection practices. It evaluated four different solutions: a data dashboard, a mobility app for push notifications, ambient lighting for subtle visual cues, and a privacy speaker for audio alerts. Similar to existing mobile apps that offer privacy controls, notifications, and device discovery, these mechanisms aim to enhance transparency and user autonomy. The mobility app was the most preferred, but integrating multiple approaches may provide a more effective privacy solution (Thakkar et al., 2022).

2.6 Using Extended Reality for Privacy

This section explores cases related to the topic of this thesis. In these cases, XR was used to display visualizations concerning privacy. As a reminder, this thesis hypothesizes that the use of MR is effective in presenting privacy practices to users. Because of the lack of research in MR for this purpose, in this section, the broader umbrella of XR is considered.

Knutzen explored how privacy icons (designed by the authors) displayed by an AR head-mounted display and co-located with smart home devices affect users' privacy awareness. The authors found that participants reported increased privacy awareness, learning benefits, and felt more in control after experiencing these AR icons (Knutzen et al., 2021).

PriView helps users in locating and understanding sensors by providing them with AR visualizations in a mobile application or a head-mounted display (HMD). Participants generally had

a positive perception of PriView, agreeing that it increased their privacy awareness (Prange et al., 2021). PARA is an AR system that detects IoT devices and allows users to use filters to conceal their identity and prevent their personal data from being captured (Fernandez et al., 2021). 2.7 displays the work of Prange et al. and Fernandez et al..

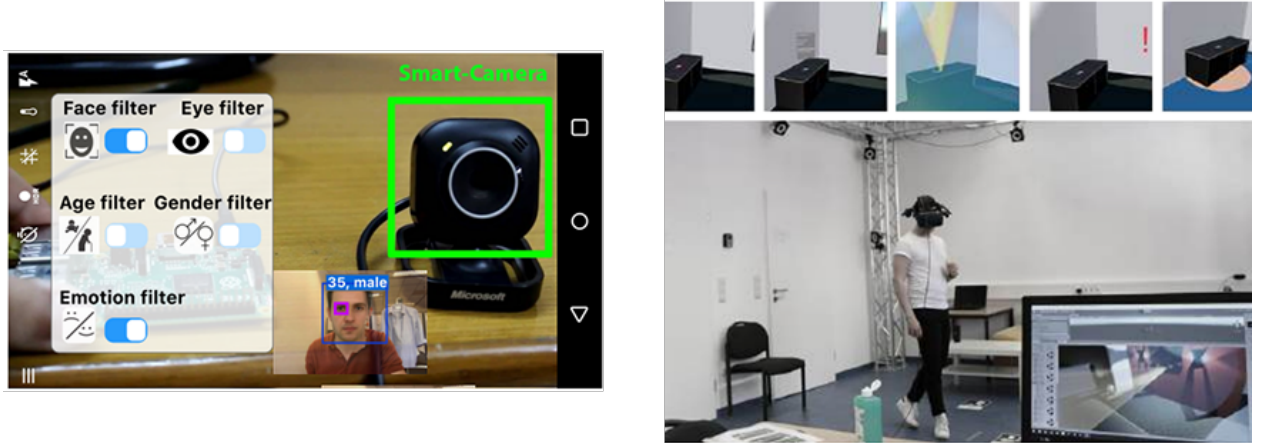


Figure 2.7: Two examples of cases related to the topic of this thesis: PARA (Fernandez et al., 2021), and privacy visualizations created for a head-mounted display (Prange et al., 2021).

Abraham proposed that AR headsets could use fine-grained permissions to enable applications to capture only necessary data (Abraham et al., 2024), giving users more options besides the usual binary permissions. Alce et al's work does not mention privacy, but its comparison of 3 AR interaction models (icons, floating menu with icons, world-in-miniature) to manage IoT devices using the HoloLens (Alce et al., 2017) could also be applied to privacy visualizations. Their results showed that preferences varied across participants, with some preferring the floating icons while others preferred the floating menu models. This suggests that a combination of the models might be ideal for future AR IoT systems.

2.7 Privacy perceptions and behaviours

When designing a user-centered app focused on privacy, it is important to recognize that people's privacy perceptions and behaviours vary. Some individuals may be comfortable sharing personal information, while others may prioritize its protection. These differences make it more difficult to create an app that resonates with a broader audience. Still, they are essential to make such an app useful for different user groups.

To overcome this challenge, it is important to identify patterns in behaviour and perception, especially those that may have a negative impact on privacy, as described below. Note that other behavioural patterns have been identified (Draper et al., 2024), such as privacy cynicism (Hoffmann et al., 2016), privacy apathy (Hargittai & Marwick, 2016), and privacy helplessness (Cho, 2022). For the purposes of this thesis, we focus on the following three:

- **Paradox**

The term privacy paradox was first introduced by Brown (Brown, 2001). It is a phenomenon identified by numerous researchers in which individuals claim to find protecting their privacy important, but act in a way that contradicts that claim (Williams et al., 2017). The privacy paradox might be more prevalent among IoT owners, and the widespread use of these devices might exacerbate the privacy paradox (Williams et al., 2017).

This paradox might prevent people from protecting their privacy as they wish. To address the privacy paradox, there are two main approaches: either align people's behaviour with their attitudes, or adjust their attitudes to match their behaviour, the second one being more privacy-preserving (Pötzsch, 2009).

There is an indication that the presence of dark patterns might intensify the privacy paradox (Waldman, 2020). If this is correct, it could mean that creating user-friendly interfaces might limit the effects of this issue. In general, implementing tools that support users in protecting their privacy might assist them in matching their actions to their values. Privacy awareness is considered by some to be the solution to the privacy paradox (Soumelidou & Tsohou, 2021).

- **Resignation**

Some individuals claim to have given up on having control over their privacy. This phenomenon is called privacy resignation, and similarly to the privacy paradox, it has been identified in the literature in several instances. Privacy resignation can be understood as a reaction to threats and a belief that one cannot protect oneself against these threats (Wirth et al., 2018).

There are 3 different types of resignation: strong resignation, indicating negative expectations towards data collection and technology companies; normalization, an acceptance of privacy risks as an inevitable reality; and powerlessness, a belief that avoiding negative consequences is impossible (Colnago et al, 2020). According to Wirth et al., to reduce privacy resignation, users should be shown that it is possible to protect their privacy, and privacy-protecting actions should be effective and within reach (Wirth et al., 2018). Additionally, the authors argue that privacy-enhancing tools should be introduced, and individuals should learn about their legal rights and about control strategies (Wirth et al., 2018).

- **Fatigue**

Privacy fatigue is a multi-faceted concept encompassing emotional exhaustion and a sense of cynicism toward the management of personal data online (Choi et al., 2018). Individuals experiencing high levels of privacy fatigue are more likely to remain passive and take no action when their personal information is misused (Choi et al., 2018).

Choi et al. further suggested that exhaustion and cynicism about privacy issues play a more significant role in shaping online behaviour than concern alone (Choi et al., 2018). The elevated time one spends agreeing or disagreeing with privacy policies online might also be

connected to privacy fatigue. Tools that support the management of privacy might help reduce the effect of privacy fatigue by simplifying such processes. By offering clearer choices, reducing cognitive load, and increasing users' sense of control, these tools can empower individuals to make more informed decisions.

2.8 Discussion

The issues identified in present-day textual privacy notices, along with the privacy risks associated with the proliferation and ubiquity of IoT devices, highlight the need for more user-friendly solutions. As the idea of legal visualizations gains prominence, mixed reality emerges as promising medium to display such visuals. MR remains underexplored in this context, and there is a growing opportunity to utilize immersive technologies for privacy awareness.

Prior work has indicated that XR would profit from user-tested privacy visualisations that communicate to the user what data is being collected, why this collection is being made, and how the data will be processed (Abraham et al., 2022). Additionally, research is still lacking regarding practical guidance for integrating privacy considerations into the design and development of XR technologies and the metaverse (Paneva et al., 2024).

As technology evolves, novel interaction and visualization methods should be explored to reflect advanced smart device configuration options (Windl et al., 2024b). These research gaps and the lack of such an app in the private market both motivate and call for the design and implementation of a mixed reality app in which these conditions can be realized.

Overcoming the privacy paradox, as well as privacy resignation and fatigue, is key to ensure more people have access to privacy controllers that respond to their preferences and needs. To the best of the author's knowledge, there has been no attempt to create a user-friendly mixed reality application that uses visualizations to fulfill this purpose. Such an application would specifically target interactions with IoT devices while allowing users to both become aware of privacy implications and adjust privacy settings.

MR was chosen as a future-proof, experimental medium that can support users in protecting their privacy. VR offers immersive environments, but lacks integration with the real world. AR improves upon this by overlaying virtual content onto physical surroundings, yet still maintains a separation between the two realms, which can reduce user immersion. Mixed reality merges the real and virtual environments, enabling real-time interaction between physical and digital objects. This integration allows MR to support context-aware applications, making it a powerful platform for solving practical problems in real-world settings (Rokhsaritalemi et al., 2020).

While adoption of XR technology has encountered barriers, such as cost or technical limitations and privacy or health concerns, the efficiency, performance, immersion, and enjoyment brought by this technology have contributed as drivers (Chuah, 2018). Other benefits of creating this system for MR include the possibility of hand interaction, which can be perceived as natural and intuitive as we grab and manipulate physical objects daily (Nguyen et al., 2023). Besides

State of the Art

the advantages previously described, similar work used extended reality to achieve related goals (Knutzen et al., 2021; Prange et al., 2021; Alce et al., 2017).

Chapter 3

Methodology

3.1 Design-Based Research

This study adopts DBR as its methodological framework to explore the most effective design elements for enhancing user awareness of privacy practices during interaction with IoT devices in mixed reality. DBR is a research methodology that integrates the process of designing interventions with the aim of solving real-world problems and contributing to theoretical knowledge (Anderson & Shattuck, 2012).

The primary aim of DBR is not only to design but also to test and refine solutions in real-world contexts through iterative cycles (Anderson & Shattuck, 2012). This methodology is well-suited for research in fields like HCI, and UX design, where designing effective, context-specific solutions is essential (Eriksson et al., 2025). DBR is particularly suited for this research as it emphasizes iterative design, real-world relevance, and collaboration between researchers and practitioners, which aligns with the goals of this thesis.

In the context of this study, DBR enables the iterative design of privacy-related elements in MR interfaces, allowing for continuous testing and refinement of these design features based on user feedback. This approach is ideal for investigating how different design elements can improve user awareness of privacy practices.

This research was carried out in several phases, structured around the principles of DBR as outlined by Reeves et al. (2006): Analysis, Development of Solutions, Reflection, Iterative Cycle, and another Development of Solutions followed by as many Iterative Cycles as necessary. Below, the main steps of each phase are listed, and also represented in Figure 3.1:

- **Analysis:** Literature Review, Needs assessment, Goal definition, Consultation with Legal Scholar
- **Development of solutions:** Use of personas, Creation of user stories, and a user flow chart, Design of Mockups
- **Reflection:** Creation and Distribution of an Online User Survey

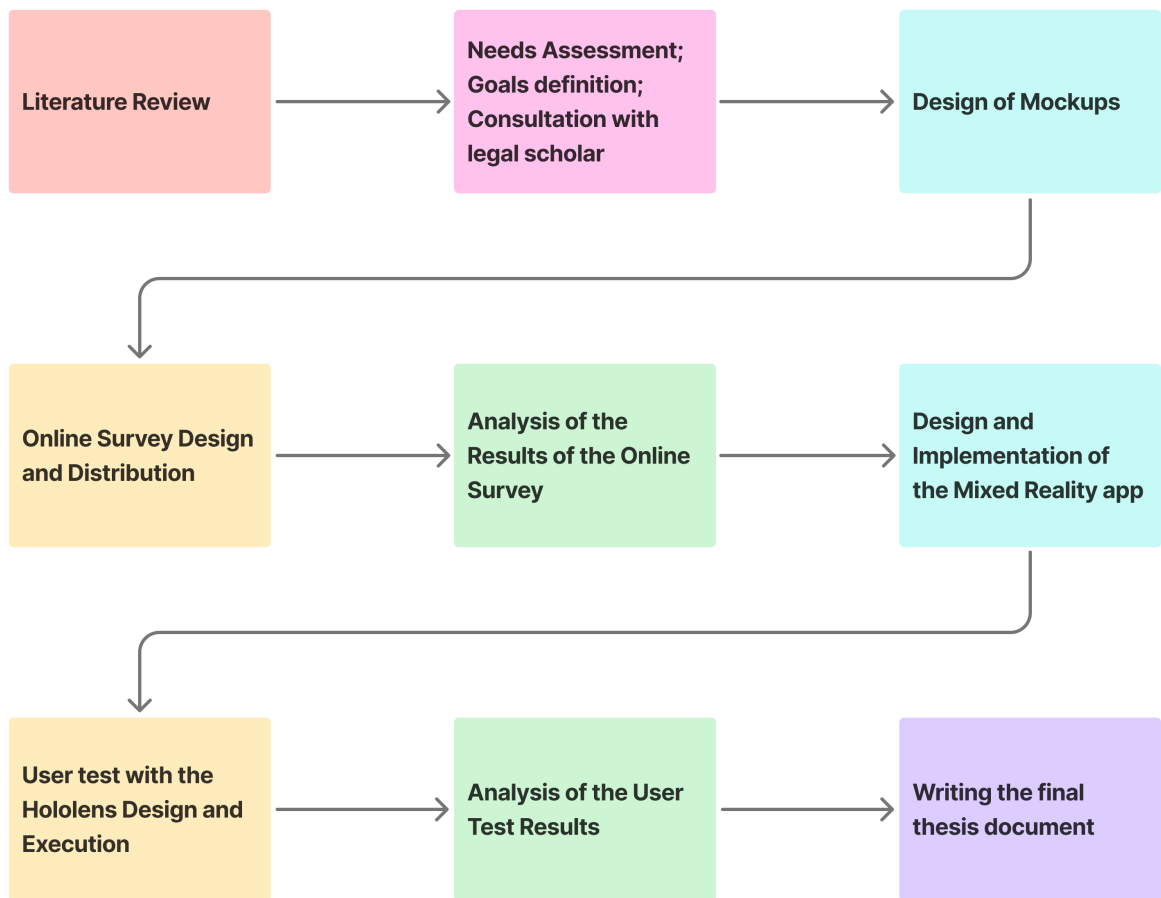


Figure 3.1: Diagram of the overall thesis process.

- **Iterative Cycle:** Analysis of the results of the Online Survey, Design and Prototype for the MR app
- **Development of Solutions:** Implementation of the MR Prototype using Unity
- **Iterative Cycle:** In-person User Test, Analysis of the results of the In-person User Test

Figure 3.1 shows that our process begins with a literature review, which revealed key insights that allowed us to define goals. We then consulted a legal scholar to build foundational knowledge of relevant privacy law concepts. These steps guided the initial design of the mockups.

Following the completion of the mockups, we created and distributed an online user survey. The survey results informed a new design iteration and the implementation of the designs in Unity for the mixed reality app. We then conducted user tests with the HoloLens, allowing participants to interact with the app. Finally, the entire process was documented in this thesis.

3.2 Literature Review

The literature review process began with 25 articles recommended by the research group. These initial sources were analysed thoroughly, and additional relevant work was identified through backward and forward citation analysis, reaching approximately 60 articles in total. Then, database searches were conducted using platforms such as the ACM Digital Library, IEEE Xplore, and Google Scholar. The search terms included “visual privacy,” “mixed reality privacy,” and “IoT privacy,” resulting in 110 relevant articles. After removing studies not directly aligned with the focus of this dissertation, the final selection consisted of 70 articles. Figure 3.2 summarizes this process.

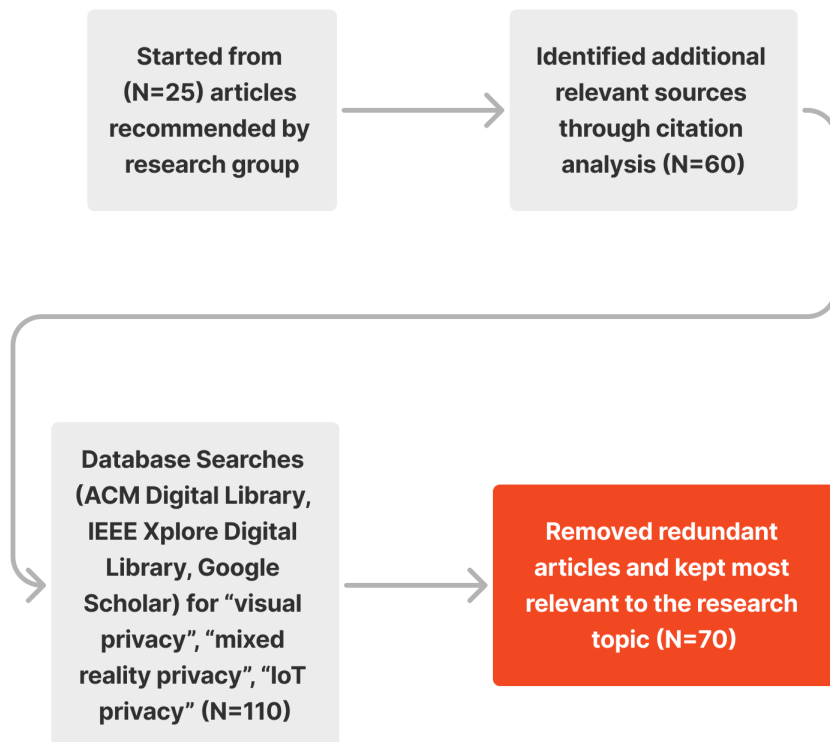


Figure 3.2: Diagram of the literature review process.

3.3 Consultation with Legal Scholar

During the first three months of this project, a legal scholar regularly joined the weekly meetings the author held with the Interactions Research Group. Although no systematic method was used to analyse the scholar's input, these meetings were instrumental in informing the project's understanding of privacy from a legal perspective. They helped in grounding the design decisions in legal frameworks (e.g., GDPR, Data Act), highlighting the importance of interdisciplinary collaboration when addressing privacy in this context.

A decision tree found in a paper by Windl et al. (2023) was a particularly relevant matter of discussion. The decision tree was created to guide users and designers in determining the most suitable privacy-preserving mechanism for various situations involving technology-facilitated privacy violations in the physical world. The ultimate goal of these parameters is to achieve a user state of "voluntary and aware", which aligns with the goals of this thesis. The tree (Figure 3.3) is composed of a series of decisions:

1. Obfuscating Data: The first decision assesses if it is possible to obfuscate data (i.e., employ privacy by design) to prevent a situation from being invasive from the start.
2. Constant vs. Ubiquitous Data Collection: If anonymisation is not possible, the next step examines whether a violation is constantly happening, such as through public surveillance (like CCTV). This helps to identify whether privacy notices would be ineffective.
3. User Control: The third decision assesses whether the user has control over the device collecting their data. If they do, they can take actions to mitigate privacy risks (e.g., unplugging the device). If not, the available mitigation options may be limited.

The app designed and implemented by the author aligns most closely with the privacy-preserving option categorized as "Mitigation Strategies / Assistive Tools". Other possibilities for enhancing privacy could include incorporating "Guerrilla Tools" as supplementary actions. "Guerrilla Tools" would be disruptive or critical actions that could be of interest to users who are in particularly sensitive or high-risk situations, especially those with strong privacy concerns (e.g., "Fundamentalists", see 4.1).

A similar approach to "Guerrilla Tools", albeit less extreme, involves the use of assistive tools found in the environment (not included in the decision tree). These may include simple measures such as covering a camera with another object or turning off a router. Some mockups were created to explore this concept; see Appendix C (7.4) for more details.

The decision tree and the input of the legal scholar helped build a foundational legal basis for this thesis. This knowledge enriched the research and influenced the design decisions. Another lesson learned was the inherent interdisciplinary nature of this topic and how collaboration can support improvements in the area.

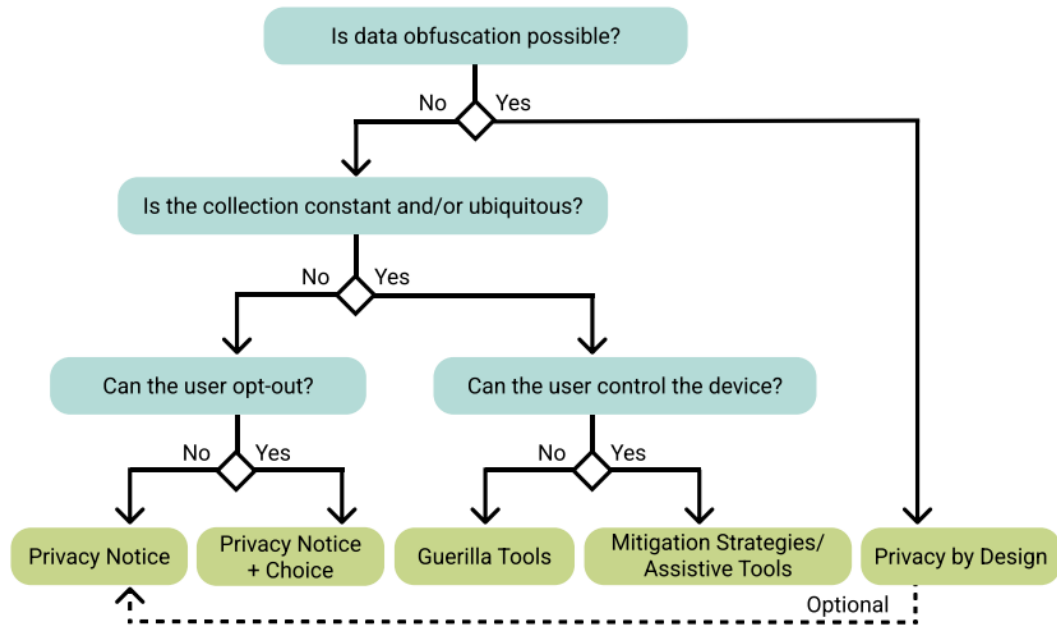


Figure 3.3: Decision tree by Windl et al. to decide on the best privacy preserving mechanism in the physical world based on the constraints of a situation (Windl et al., 2023).

3.4 Data Collection and Analysis

Data was collected through two different methods to ensure a comprehensive understanding of user experiences with privacy, IoT devices and MR: an online survey and an in-person user test. First, an online user survey was completed by 150 participants. This survey had as its main goal relating privacy personas (see 4.1) with different design elements. This survey was analysed using predominantly quantitative methods, with the exception of one open-ended survey question that was analysed qualitatively. Insights from this phase informed the development of a mixed reality application.

Then, an in-person user test was completed by 20 participants with the HoloLens. In this user test, participants experienced a prototype of the MR application. The test combined a task, questionnaires, and semi-structured interviews, and was analysed using both quantitative and qualitative methods.

A full description of the online survey and the in-person user test, including their design, procedures, and findings, is provided in the following chapters: the online survey is detailed in Chapter 5, and the user test in Chapter 6.

Methodology

Chapter 4

Requirements and Design

Informed by prior literature, collaboration with fellow researchers, user research conducted as part of this thesis, and user-centered design principles, a mixed reality application was designed and implemented. This chapter describes the design process of the app, named VISTA (Visual Interface for Smart Technology Awareness). The chapter starts by outlining the design process and the challenges encountered. Then, the design of mockups and of the prototype are described in more detail. The last subsection explains the decisions regarding the visual identity of the app.

VISTA is an MR app that allows users to find smart devices in a room and adjust privacy-relevant parameters. A smart smoke detector might have privacy-threatening sensors, for example, and go unnoticed (*Die Zeit*, 2024). With the help of the app, users would be able to identify the presence of this smoke detector and turn off its sensors, if they so desire. Note that the prototype simulates the functionalities described. Only the design and front-end development of the app were completed, while all other services were mocked for demonstration purposes during the user test.

For the purpose of this thesis, the app was developed for use in rental homes, such as AirBnB properties or similar short-term rental platforms. This context was chosen based on its relevance in previous literature and its continued potential for exploration. Additionally, in the online survey conducted for this thesis, when inquired about where they would use this app, 63% participants selected the option "Holiday Home", suggesting that this is one of the most relevant scenarios. All results from the user survey are presented in [5.1](#).

4.1 Privacy Personas

The literature review revealed that individuals have different perspectives regarding privacy. While some might be more concerned and take more action to protect themselves, others might be more relaxed concerning the sharing of personal data. These differences had to be considered when designing the system to ensure it accommodates diverse user preferences.

To enhance user awareness, one can tailor a system to be user-independent (e.g., privacy disclaimers on websites) or user-specific (e.g., feedback from Website's policy evaluations) (Pötzsch,

2009). Within the user-specific framework, the system can be adapted to the needs of groups or even individual users (Pötzsch, 2009). To make sure that the final prototype would resonate with as many users as possible while exploring the idea of user-specific privacy requirements, this thesis used personas to identify the preferences of user groups.

The concept of “persona” in the HCI community was originally introduced by Cooper (Chang et al., 2008). Personas are descriptive models of users and provide a more precise way of thinking and communicating about how groups of users behave, how they think, what they want to accomplish, and why (Cooper et al., 2014). Although personas are not representations of real users, they are assembled from the behaviors and motivations of many actual users (Cooper et al., 2014).

Given that personas should originate from research, and the limited time and scope of this project, no authorial research on personas was conducted. Instead, existing personas were searched for in the literature, analysed, and selected. Below, a summary of three established personas is included, from which one was chosen.

- **Westin**

Westin’s privacy personas (Kumaraguru & Cranor, 2005) are frequently used as a foundational model for this type of persona, despite criticism regarding their limited ability to predict behaviors and knowledge (King, 2014). Through over 120 studies on privacy concerns, Westin identified three key personas: the Fundamentalist, the Unconcerned, and the Pragmatist.

- **Biselli**

Biselli et al. (2022), using the same name convention as Westin, also identified 3 categories of personas: Fundamentalists (high knowledge, high privacy-enhancing behaviour), Pragmatists (moderate knowledge, moderate privacy-enhancing behaviour), and the Unconcerned (low knowledge, low privacy-enhancing behaviour).

- **Dupree**

Dupree et al. (2016) grouped attributes using the themes of privacy, knowledge, and motivation. This resulted in five persona clusters: Fundamentalist, Lazy Experts, Technicians, Amateurs, and Marginally Concerned. Each one of them has different degrees of privacy knowledge and motivation.

The set of personas by Dupree et al. was ultimately chosen to be used in this research for a few reasons. First, Dupree et al. tested this set of personas with designers and obtained positive results. Given that this thesis is primarily design-based, the favorable response from designers served as a strong indication of the personas’ suitability in this context.

These authors additionally ran persona self-identification tests with participants. Considering that we intended to let participants self-identify with the personas, this prior validation supported the decision to adopt their framework. Moreover, the Dupree et al. personas encompass five distinct categories, being in this way more comprehensive than other personas from the literature.

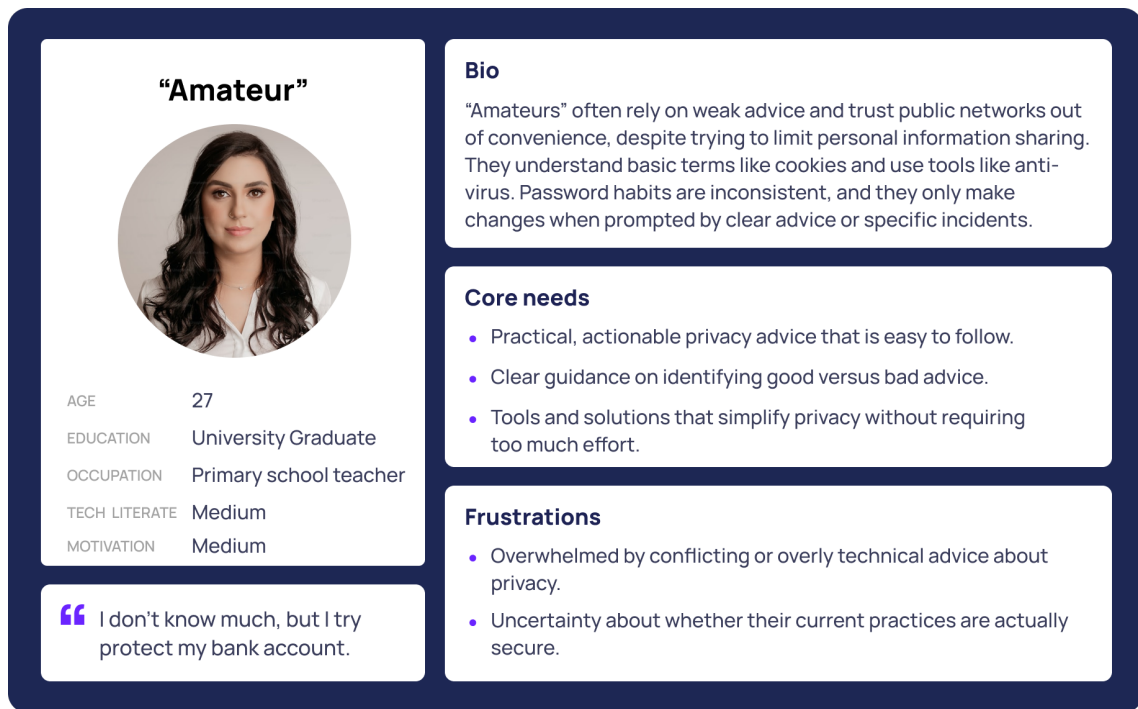


Figure 4.1: Amateur persona adapted from descriptions provided by Dupree et al.

However, using these personas proved challenging at times. Some of the texts used to describe the personas, essential for the self-identification process, contained politically charged terms, such as “fundamentalists” and sentences that participants might struggle to identify with, such as: “They [Amateurs] view others (somewhat inaccurately) as uneducated and unsecure compared to them.”

These sentences also introduced potential cultural biases, as some participants from certain cultures might find them acceptable, while others might not. To address this, we briefly explored rewriting the persona texts as part of exploratory research. This included attempts such as using GPT to rewrite the texts; changing pronouns from third-person to first-person; and presenting the original Dupree et al. text as 44 first-person statements in a random order. However, due to time and scope constraints, this exploration was abandoned within the context of this thesis, with results included in Appendix D (7.4).

Following this exploration, it was decided that the original Dupree et al. text would be used in our online survey with minor modifications for clarification and to avoid bias. The pronouns present in the text were changed from third-person to first-person to enhance self-identification. To further help participants better identify with the personas without being influenced by their names, the titles (Amateurs, Lazy Experts, Fundamentalists, Technicians, Marginally Concerned) were removed from the survey. Additionally, two sentences conveying negative attitudes toward others were omitted “I view others (somewhat inaccurately) as uneducated and unsecure compared to me” from Amateurs and “I view others as uneducated and insecure” from Fundamentalists. Figures 4.1 to 4.5 are graphical representations of the personas used.

Requirements and Design



Figure 4.2: Lazy Expert persona adapted from descriptions provided by Dupree et al.

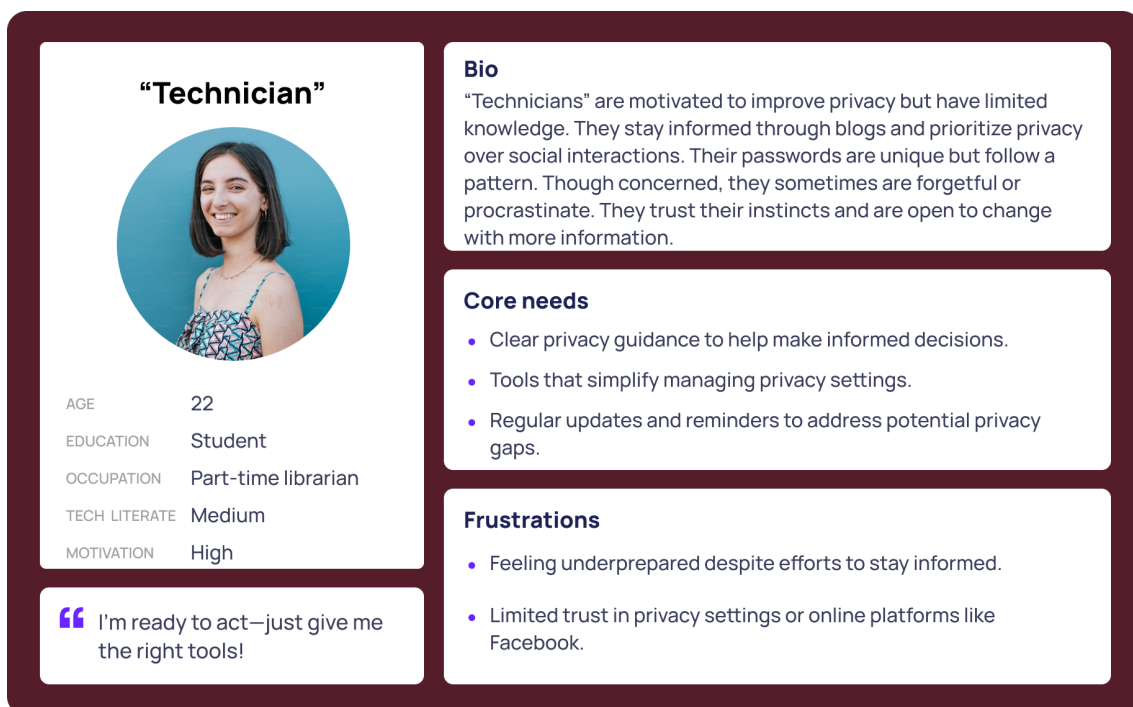


Figure 4.3: Technician persona adapted from descriptions provided by Dupree et al.

Requirements and Design



Figure 4.4: Fundamentalist persona adapted from descriptions provided by Dupree et al.

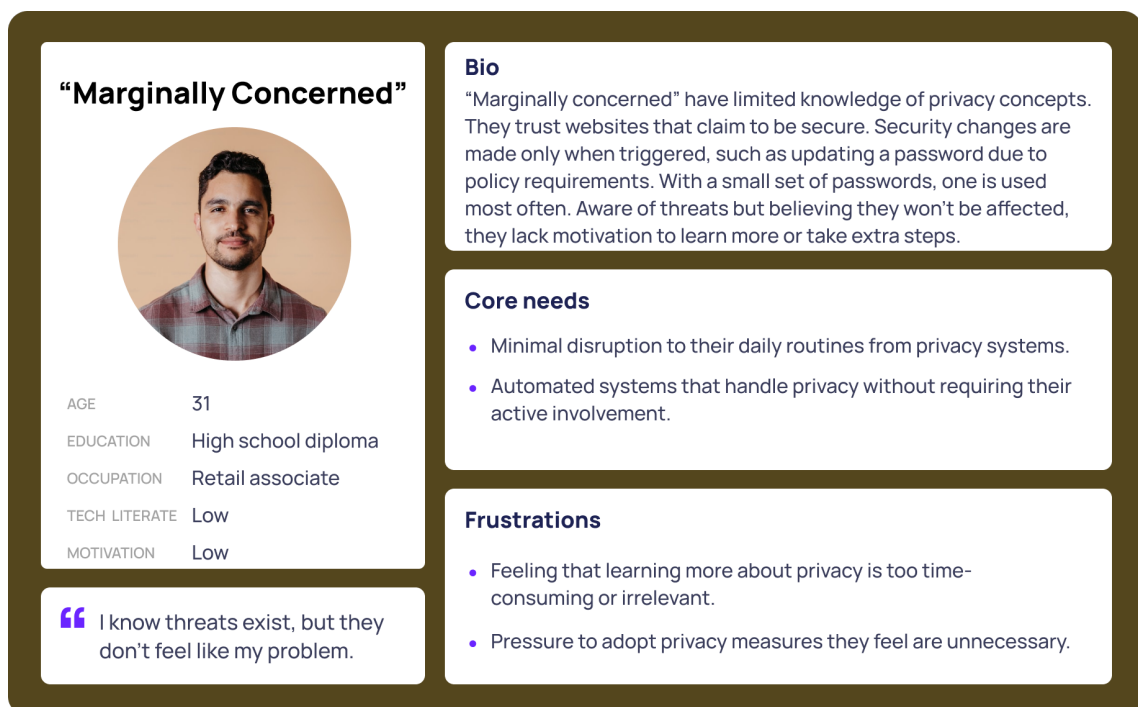


Figure 4.5: Marginally Concerned persona adapted from descriptions provided by Dupree et al.

4.2 Design tools and challenges

Design tools such as user stories and user flow charts were also employed throughout the design process. These traditional UX methods help in the visualization of system interaction and user needs. For instance, a user journey chart was created early in the project to contextualize and better understand the problem at hand. See Appendix A (7.4) for the user journey.

A user story is a short, simple description of a feature or requirement told from the perspective of the end user. It typically follows the format: *As a [type of user], I want to [do something] so that [I achieve a goal]*. (The Interaction Design Foundation, 2025). The user story considered for this project is the following:

As an Airbnb guest and privacy-concerned individual, I want to be aware of tracking devices in my accommodation, so I can turn off sensors and protect my privacy.

A user flow chart (or user flow) is a visual representation that maps out the steps a user takes to complete a specific task within a product or system. It outlines the user's journey through different screens, actions, and decision points, helping designers and developers understand how users interact with an interface to achieve their goals (The Interaction Design Foundation, 2025). An earlier version of the user flow chart is included in Appendix B (7.4). These charts were updated according to each iteration and to the progress of the thesis. A final version can be found in Figure 4.6.

A few challenges were encountered during the design process. First, while traditional user interfaces following the WIMP paradigm (Windows, Icons, Menus, Pointer) have been well-established for many years and have clear usability guidelines to support their development, comparable standards and guidelines are still largely missing in VR and AR environments (Doerner et al., 2022; Rokhsaritalemi et al., 2020). As a result, designing applications for extended reality (XR) remains challenging, particularly when aiming for strong usability. This challenge was partially mitigated by including interface-related questions in the online user survey.

Secondly, apps addressing privacy must comply with legal frameworks such as the GDPR and the Data Act, both of which are especially relevant in the context of personal data collection in smart environments. Based on the decision tree proposed by Windl et al. (see 3.3), a set of "legal" interface designs was developed for VISTA. These designs were conceptually aligned with legal constraints, but due to time and scope limitations, they were not implemented or tested.

The "legal" designs consisted of context-specific screens that would appear in situations where users were restricted from interacting with certain smart devices. For instance, a user might be unable to turn off a security camera at a supermarket. This restriction reflects the concept of legitimate interest, a legal basis under GDPR that permits data processing when necessary for the legitimate interests of an organization or third party, as long as those interests are not overridden by the rights and freedoms of the data subject.

In such cases, when a smart device's privacy notice cites legitimate interest, the user typically does not have the ability to control or disable data collection. The VISTA interface aimed to reflect

Requirements and Design

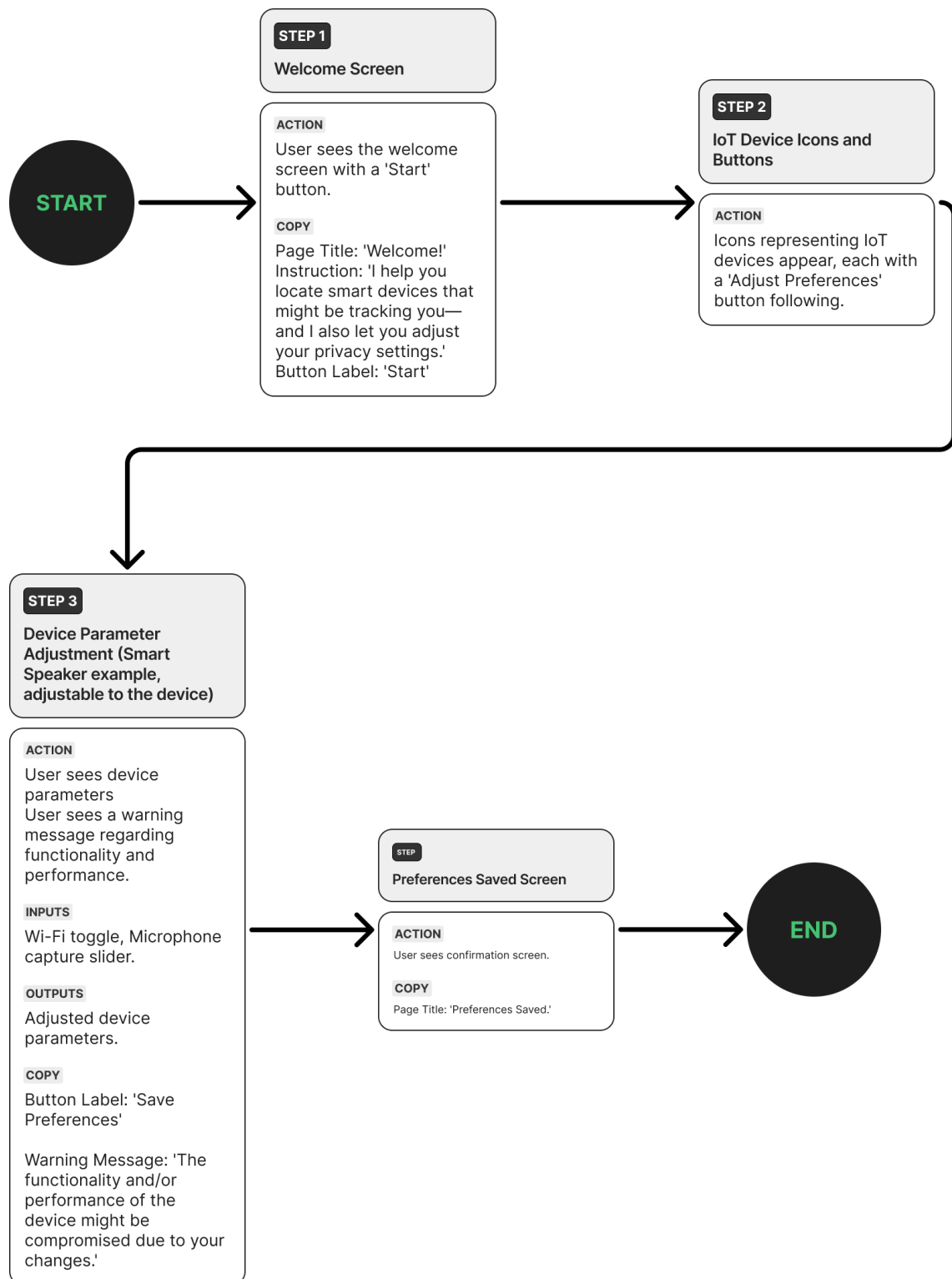


Figure 4.6: Final version of the user flowchart that informed the creation of the prototype.



Figure 4.7: Alce et al. (2017) design of a floating menu.

this by displaying explanatory screens aligned with the privacy notices of the devices in question. See Appendix C (7.4) for these "legal" designs.

The third challenge concerns the idea of smart environments containing multiple devices. In the future, environments such as smart offices or smart classrooms may become more widespread, potentially containing hundreds of IoT devices, which would increase the difficulty for users to monitor them effectively. The system designed here had to consider how to handle the presence of multiple devices, and how to support users in identifying them and adjusting their private preferences accordingly.

The solution encountered for this issue was to include a screen inspired by the floating menu created by Alce et al. (2017), in which all of the devices found in the room are displayed to the user in a simplified manner. Note that Alce et al. use navigation arrows to browse through items as well as a pagination indicator. Since our final setup only allowed for the display of five elements (five smart devices), this interface was simplified. See Figure 4.7 for the original elements included in Alce et al. (2017) and 4.8 for our version of the design.

Another key challenge determined for the app was having a way for users to identify hidden or difficult to identify smart devices within an environment. In MR, there are several ways to assist users in navigation. Two navigation patterns were identified by researchers as preferable to users: arrows and avatars (Lee et al., 2022). Inspired by these results, we decided to inquire users about their preference for self-exploration ("arrows") or assisted guidance ("avatar") in the online user survey to mitigate this problem.

A fourth relevant challenge concerns an issue more closely related to user interface design for MR, as discussed by Li et al. (Li et al., 2022): whether interfaces should be presented to users in a perspective central to their view ("user-centered") or in relation to objects in the environment



Figure 4.8: Our screen displays to the user the devices found in the room. The number of devices would be scalable by adding navigation arrows and a pagination indicator, similar to 4.7.

("object-centered"). This matter reflects the lack of established navigation and usability guidelines for MR. Still, in order to keep the system user-friendly, we decided to bring this matter to participants in the online user survey.

4.3 Design of Mockups and the Prototype

For the purpose of this thesis, mock-ups and a prototype were created. Both were initially created using Figma, a cloud-based design tool that allows teams to collaboratively create user interfaces, prototypes, and visual assets in real time. Even though Figma is not particularly suited for 3D design and prototyping, no other platforms are yet fully developed or widely adopted for this purpose in the same way Figma is for 2D design.

The mock-ups were created early in the project and were visual dummies used primarily to show participants in the online survey how the user interfaces of the MR application would look like. The mock-ups also served as a way for the author to present the design iterations to fellow researchers throughout the project. It is worth noting that no digital wireframes were created as part of this thesis. Figure 4.9 illustrates part of the Figma workflow for the creation of mockups.

Four sets of mockups were created in response to the user needs of the Dupree et al. personas. "UI1" was designed for the Technician persona, who was hypothesized to value control and efficiency. This screen offers the action of turning off all IoT devices in the environment with the click of a button. "UI2" was tailored to the Fundamentalist persona, who typically seeks granular control over privacy settings. This interface allows users to configure specific parameters for individual devices. "UI3" was created with the Lazy Expert in mind, since these users are knowledgeable

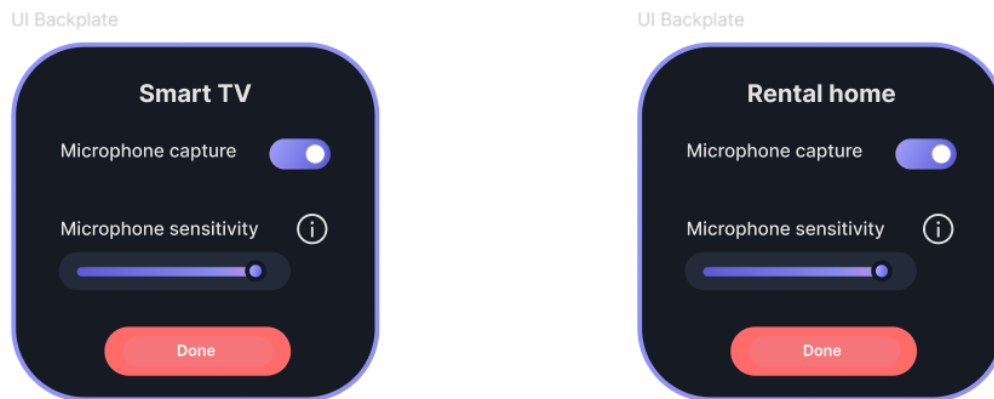


Figure 4.9: Figma screenshot showing a part of the workflow for designing the mockups.

but might prefer minimal interactions. This screen displays a message that the environment was scanned beforehand and privacy-threatening smart devices were automatically disabled.

Finally, "UI4" was designed for Amateurs, who are less experienced and may feel uncertain when managing privacy settings. This interface includes simplified options and offers the broad action of "Protect My Privacy". The Marginally Concerned persona was intentionally excluded from this stage of interface design, as individuals in this group are characterized by low engagement with privacy tools and were assumed to be unlikely users of the app. These mockups were chosen to be included in the user survey and can be found in Chapter 5.

After the results of the online survey were analysed, important conclusions were drawn, inspiring and informing further design iterations. A detailed discussion of the survey results will be presented in Chapter 5. The following paragraphs analyse how these findings influenced the prototype's development, aligning with user-centered design principles and the iterative nature of DBR.

"UI2", originally designed for Fundamentalists, was favoured by most participants in the online survey, despite initial assumptions that it would correspond to the preferences of only one user group. This UI had detailed parameters for each smart device, and indicated to users which controllers they could choose to disable or enable. As a result, screens for five different smart devices were created for the prototype, and these were based on "UI2". These screens are presented in Chapter 6.

In the online survey, participants were additionally given the option to choose between icons or a mascot for assistance in navigating the environment and in finding smart devices. Even though "arrows" were initially considered for navigation, icons were favoured due to their potential for enhancing privacy awareness as described in Chapter 2. Icons were preferred over the mascot by participants. For this reason, instead of including a mascot in the prototype to guide participants across the room, icons were chosen to signal to users where the smart devices would be.

Moreover, object-centered screens were preferred over user-centered screens by participants

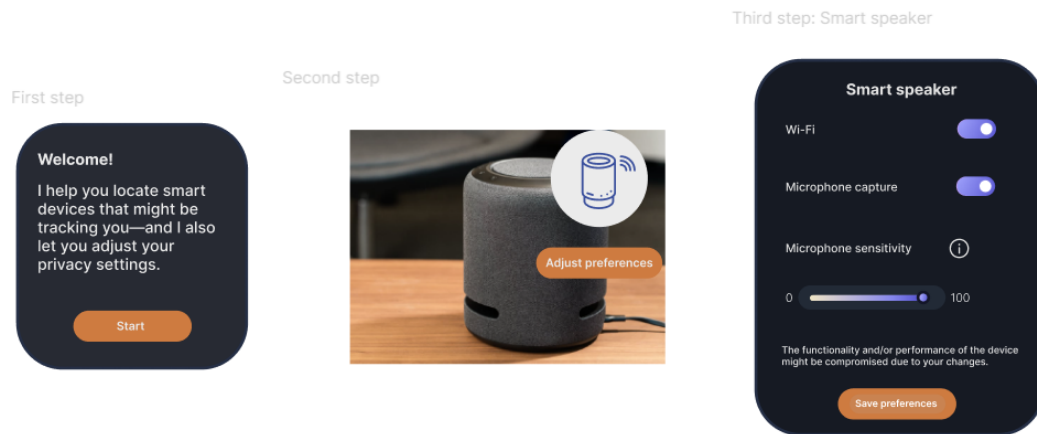


Figure 4.10: Figma screenshot displaying part of the workflow for designing the prototype.

in the online survey. Consequently, object-centered screens were implemented in the prototype. This meant that the interfaces for adjusting privacy preferences appeared in relation to real-life objects in the MR environment, rather than being positioned centrally in the user’s field of view.

Overall, the prototype simulated the design and functionality of the app proposed, and its design decisions were largely based on the results of the online survey. The prototype assisted in design iterations and was experienced by participants during the tests done with the HoloLens. Figure 4.10 displays part of the Figma workflow of the prototype. Considering the diverse interaction modalities enabled by the headset, a few modalities were included in the final prototype. The next subsection explores the interaction design decisions.

4.4 Interaction Design Decisions

The interaction design decisions of the prototype were intended to combine usability and alignment with established MR conventions. Key decisions were made to ensure that users could engage with the interface comfortably within the spatial context of MR. Users could interact with components included in the prototype through air tapping (mimicking physical button or toggle presses), or by using raycasting combined with the pinch gesture, both standard input methods of the headset used, the HoloLens 2. Raycasting lets users select objects through a beam that extends from the 3D cursor into the environment, and is a common interaction method of extended reality headsets (Doerner et al., 2022).

A menu was added to the prototype to ensure that users could access and hide the screen outlining the smart devices found in the environment. This simplified access to this information in case it was needed, while allowing users to hide it to avoid visual clutter. The menu also included a possibility to exit the MR app, and to pin its buttons close to the user’s field of view. The menu design can be seen in 4.11.

Basic gaze-based interaction was also incorporated: when users looked at a button, its label would “pop” forward, providing visual feedback that helped users navigate the interfaces. Other

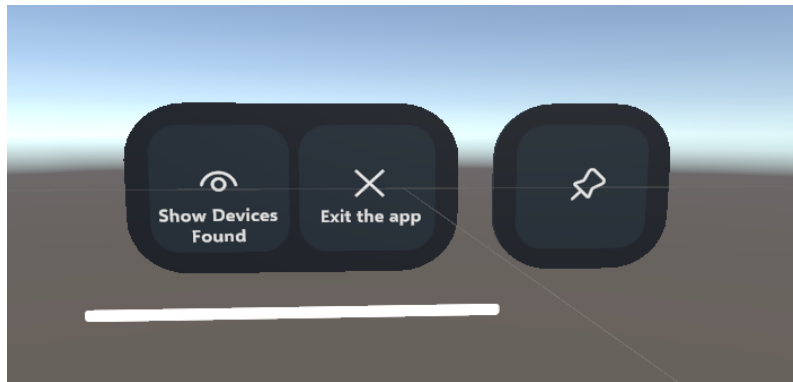


Figure 4.11: The menu included in the prototype.

gaze-based interactions were intentionally avoided so users could "freely observe" the environment without triggering unintended actions.

Sound feedback was incorporated to signal to participants the completion of specific tasks. Three distinct sounds were included in the final prototype: one to confirm button activation, another for toggle interaction, and a third to mark the end of the user flow, triggered upon interaction with all of the device screens.

Other modalities (e.g., voice commands) were not included to prevent clutter and keep the experience intuitive and natural. The modalities employed were chosen based on Microsoft recommendations for the scenario of the app, namely one in which spatial layout was relevant. For more details on how different interaction modalities apply to different scenarios, see ¹.

To ensure comfort, no holograms were placed closer than 1 meter or further than 5 meters from the user. See Figure 4.12 for a visual representation of the optimal zone for hologram placement. Additionally, to prevent neck strain, holograms were placed in the "optimal region" between 0 and 35 degrees. For more information on user comfort in MR, see ².

The implementation of the prototype was done using Unity. Unity is a cross-platform development environment widely used for creating interactive 2D and 3D applications, including games, simulations, and mixed reality experiences. It offers a component-based architecture, real-time rendering capabilities, and supports scripting primarily in C#, making it suitable for rapid prototyping and application development. Unity is particularly relevant in research and design contexts due to its flexibility and support for different platforms, enabling the creation of spatial user interfaces. See Figure 4.13 for a screenshot of our Unity workflow.

HoloLens 2

The Microsoft HoloLens 2, displayed in Figure 4.14, is a mixed reality head-mounted display developed by Microsoft, succeeding the original HoloLens. The HoloLens 2 Enterprise Edition

¹ See <https://learn.microsoft.com/en-us/windows/mixed-reality/design/interaction-fundamentals> for modality references.

² See <https://learn.microsoft.com/en-us/windows/mixed-reality/design/comfort>.

Requirements and Design

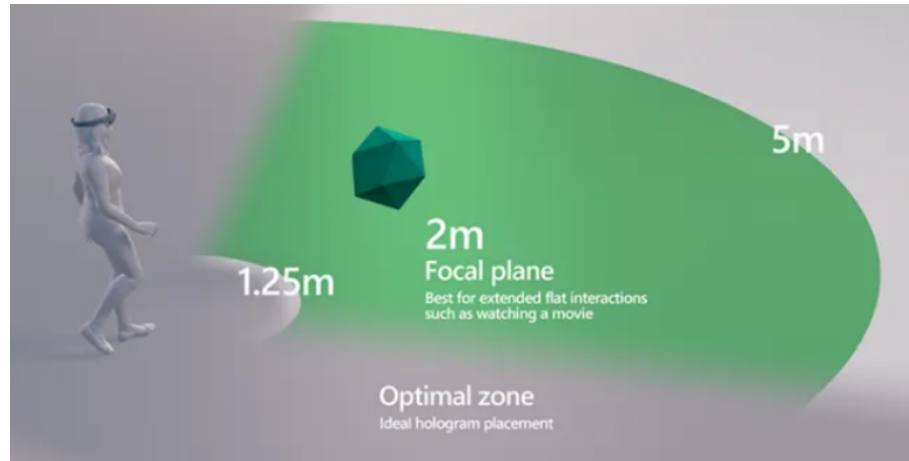


Figure 4.12: The optimal zone for hologram placement as recommended by Microsoft. Image by Microsoft.

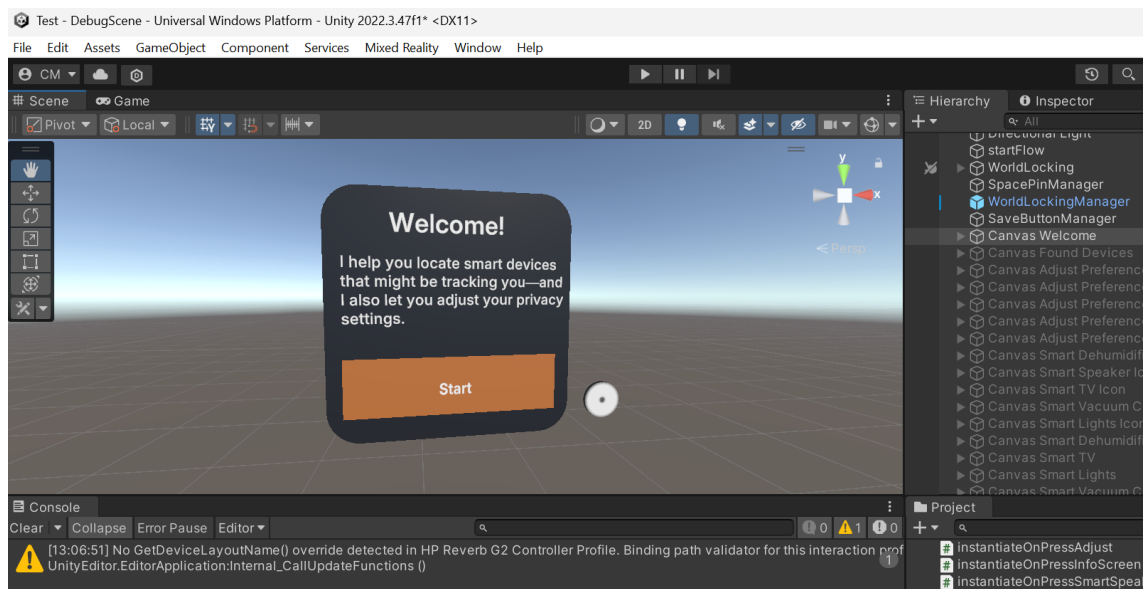


Figure 4.13: Unity screenshot showing a part of the workflow for designing and implementing the prototype.



Figure 4.14: HoloLens 2, image provided by Microsoft.

was released in February 2019. This device enables users to interact with holograms overlaid on the real world, making it useful for applications in education, healthcare, design, and research.

The HoloLens 2 features hand and eye tracking, voice commands, and spatial mapping, among other features. These capabilities support a wide range of mixed reality experiences without the need for external controllers. Even though Microsoft recently announced its discontinuation (Warren, 2024), the HoloLens is one of the leading mixed reality headsets currently available. It was chosen for this project due to its availability at the Interactions Research group, as well as its interaction possibilities that match the goals of the study.

MRTK3

The Mixed Reality Toolkit 3 (MRTK3) is the third generation of Microsoft's open-source Mixed Reality Toolkit for Unity. This toolkit was designed to facilitate the development of cross-platform mixed reality applications. Built on Unity's XR Management system and XR Interaction Toolkit, MRTK3 provides an extensible framework for developers, allowing for a faster and more efficient design process.

While other MR toolkits are available, MRTK3 was the most suitable choice for this project, both for consistency and for its direct integration with the HoloLens. In this project, several MRTK3 components were used to facilitate the development of the app as well as to take advantage of its rich set of features. Often, MRTK3 components were slightly altered for consistency with the visual identity of the app.

MRTK3 comes with a few sound files designed to give audible feedback to users after certain types of interaction. Some of these were used in VISTA, and when different sounds were required,

the author turned to Free Sound (<https://freesound.org/>). A total of three feedback sounds are included in the final prototype.

4.5 Visual Identity

The visual identity of the app was largely based on Microsoft's guidelines. See this Microsoft page for references regarding colour, light and materials ³. These recommendations include, for instance, a guide on how to use colour in mixed reality apps. The colour white appears particularly bright in MR and should, therefore, be used sparingly. It is typically used for typography only, and the recommended colour is the hex value of #EBEBEB. These recommendations were followed on the app for colour and typography.

A contrast-checking tool was used to assess the accessibility of the typography colour against the background colour. The evaluation confirmed that the contrast met accessibility standards for legibility. See Figure 4.18 for the test results. These results guarantee that the information presented is easily readable for a wider range of users, including those with visual impairments.

Microsoft further instructs that, in MR environments, cool colours tend to recede, while warm colours tend to "pop" and draw attention. As a result, buttons and other interactive elements were designed using warm colours to ensure they were visually prominent and attracted the attention of users. See Figure 4.15 for the final set of colours used.

Some colour adjustments were made from the initial mockups to the final prototype. Borders were removed due to implementation challenges in Unity. The original pink hue was replaced with an orange hue, as pink appeared too similar to red, a colour commonly associated with cancellation in UI elements. Additionally, the blue background was darkened slightly to enhance contrast in mixed reality environments.

The icons used were sourced from Flaticon (<https://www.flaticon.com/>), and were chosen based on clarity, simplicity, and faithful representations of smart home appliances. Figure 4.17 displays the final set of icons used. The typography used was "Inter". "Inter" is a popular and widely used sans-serif typeface designed for legibility and clarity, especially on digital screens. It comes in a wide range of weights (from Thin to Black), offering flexibility in usage across different design elements. It was used in three different weights as seen below in Figure 4.16.

³See <https://learn.microsoft.com/en-us/windows/mixed-reality/design/color-light-and-materials>

Colors



Figure 4.15: Colours used in the design of the MR app.



Figure 4.16: Typography used in the design of the MR app.



Figure 4.17: Icons depicting a vacuum cleaner, a TV, a dehumidifier, lights, and a speaker, all used in the final prototype of the app.

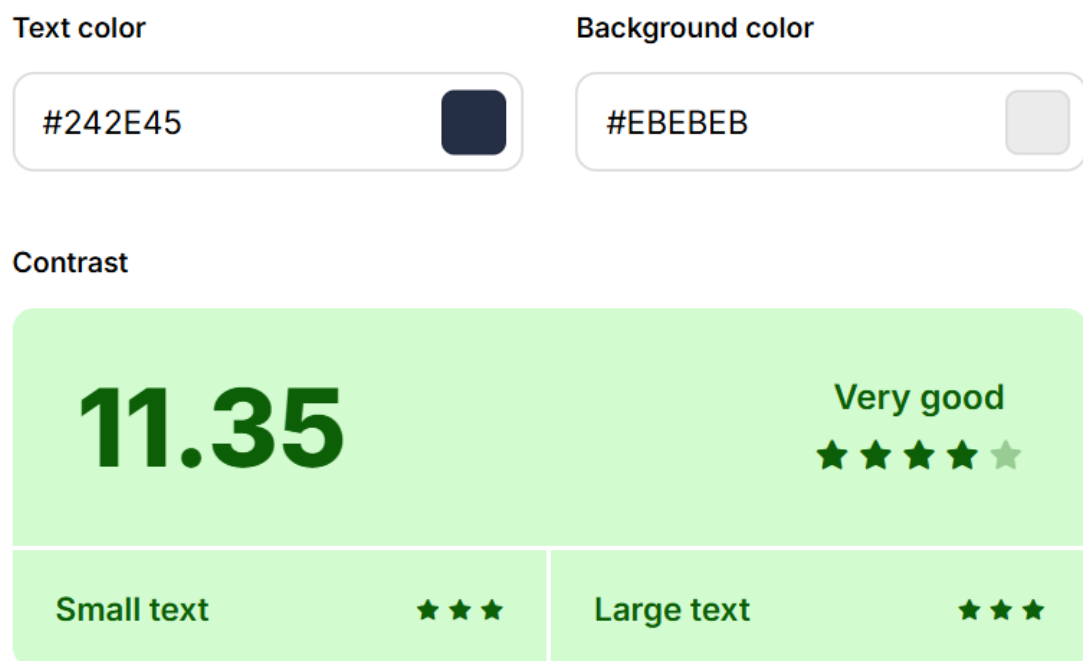


Figure 4.18: Results of the contrast check between text and background colours used in the interface. The tool confirmed that accessibility standards were met for legibility.

Requirements and Design

Chapter 5

Online Survey

This section describes in detail the online survey. The chapter opens with an overview of the survey's methodology, including its design and the key constructs assessed. Next, it presents the findings, including participant demographics, data derived from the IUIPC scale, persona assessments, and user interface feedback. A detailed analysis of these results follows, and the section concludes by addressing the limitations of the survey.

The online survey hypothesized that participants would find specific UI designs and navigation methods more useful based on the persona they identified with the most. For that purpose, 4 different UI designs were included in the survey (Figure 5.1 to 5.4), each corresponding to the expected needs of 4 of the Dupree et al. personas. The expected associations were:

1. "UI1" and Mascot will be rated as most useful by participants who related the most with Technicians.
2. "UI2" and Icons will be rated as most useful by participants who related the most with Fundamentalists.
3. "UI3" and Icons will be rated as most useful by participants who related the most with Lazy Experts.
4. "UI4" and Mascot will be rated as most useful by participants who related the most with Amateurs.
5. Participants who related the most with Marginally Concerned will give a low usefulness rate to all UIs, the mascot and the icons.

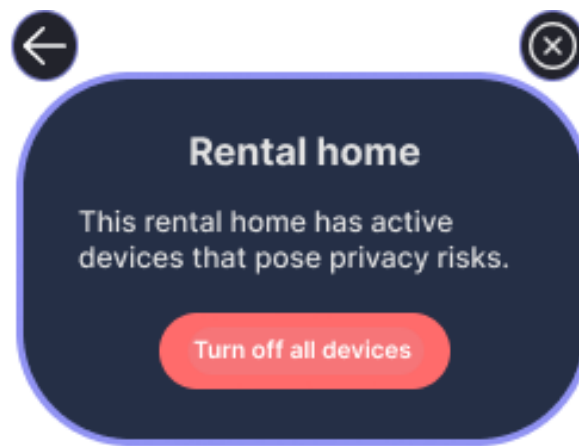


Figure 5.1: "UI1": "Turn off all devices" Screen – Designed for Technicians, who were hypothesized to prefer direct control over all IoT devices.

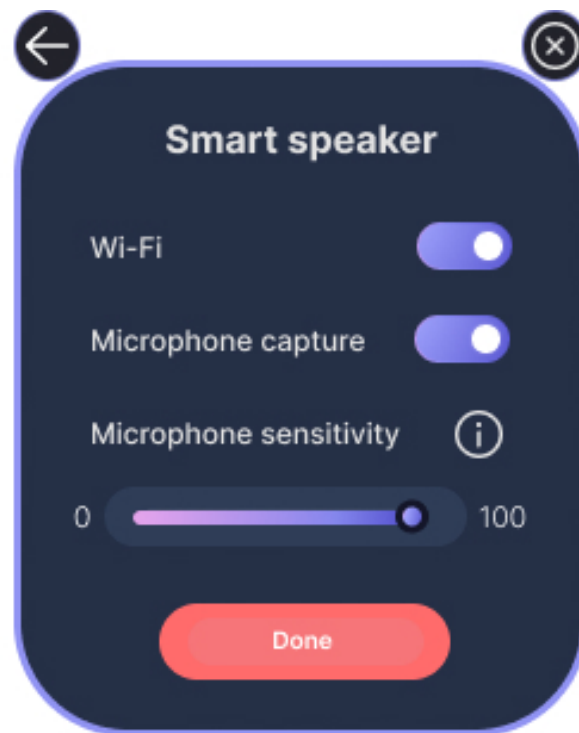


Figure 5.2: "UI2": "Parameters" Screen – Designed for Fundamentalists, who were hypothesized to aim for detailed customization of privacy settings.

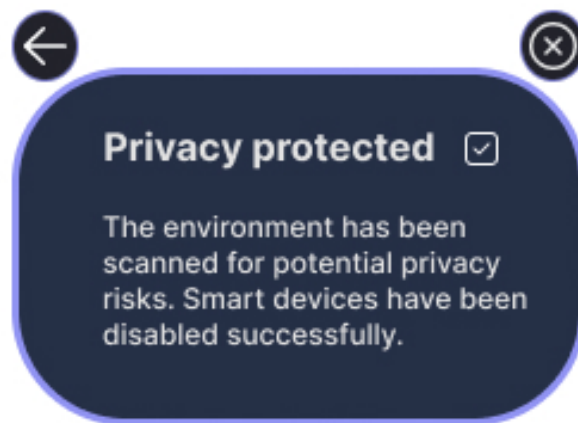


Figure 5.3: "UI3": "Scan" Screen – Designed for Lazy Experts, who were hypothesized to want a quick overview of connected devices with minimal effort.

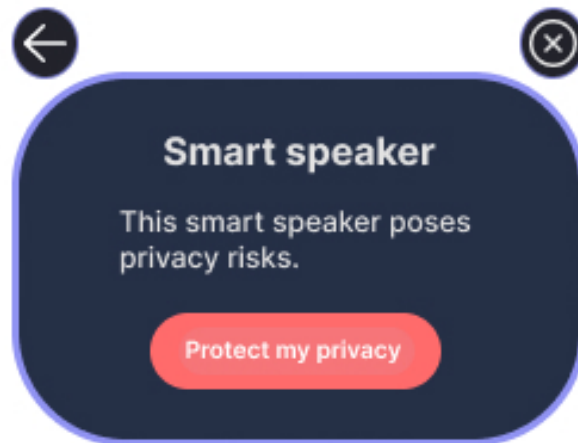


Figure 5.4: "UI4": "Protect" Screen – Designed for Amateurs, who were hypothesized to require guidance and simple privacy options. The Marginally Concerned persona was not assigned a specific UI, as this group is characterized by a lack of motivation to engage with privacy-related tools. It is hypothesized that individuals who identify with this persona would not actively use such a system.

Beyond testing the main hypotheses, additional analyses explored potential relationships between participant characteristics and their UI preferences. The following factors were also considered:

- Privacy Concerns: Identifying if participants with higher privacy scores are more likely to align with specific personas.
- IoT Ownership: Examining whether owning IoT devices influences UI selection.
- Technology Familiarity: Assessing whether familiarity with augmented reality (AR), virtual reality (VR), or IoT impacts UI preferences.

Online Survey

20

In this option, the rental home where you are at is automatically scanned by the system and all of its smart devices are automatically disabled. *

←

Privacy protected ☒

The environment has been scanned for potential privacy risks. Smart devices have been disabled successfully.

×

Not at all helpful Slightly helpful Moderately helpful Very helpful Extreme

How helpful would this function be?

☐ ☐ ☐ ☐

Figure 5.5: Example of a question of the online user survey.

- **Demographics:** Exploring whether education, age, or gender affects UI preferences.
- **User-Centered vs. Object-Centered Preferences:** Evaluating whether familiarity with AR/VR influences preference for user-centered or object-centered UI design.

The online survey was sent to 150 participants recruited through the platform Prolific. Prolific is a well-established platform that supports the recruiting of participants for research purposes. This platform has been used in recent HCI literature (Hadan et al., 2024; Windl et al., 2024b). The use of the platform allowed the survey to reach a larger pool of participants and to have participants from more diverse backgrounds. Prolific additionally allows participant screening: a gender quota (50% male, 50% female) was used to guarantee gender balance in the survey, and participants could only take this survey if they claimed fluency in English. See 5.5 for an example of a question present in the user survey.

Microsoft Forms was used to administer the survey. This platform was chosen for compliance with the GDPR (Microsoft, n.d.). Images were used to simulate the mixed reality environment. There were two attention checkers as required by Prolific for surveys longer than 5 minutes. A pre-test was done with members of the Interactions Research Group at the University of St.Gallen, as well as with individuals from the general public. After the pre-test, minor changes were made to improve the comprehensibility of the text.

A complete guide on the questions of the online survey can be found in Appendix F (7.4). The survey was structured as follows:

- **Informed Consent** The experiment was briefly described, and participants were asked to consent.
- **Demographics + Familiarity with XR and IoT + Ownership of IoT devices**

Participants were asked about their age, gender, and education, as well as their familiarity with augmented reality, virtual reality, and IoT devices. Additionally, they were asked to select the IoT devices they own. The gender terms used ("Man", "Woman", "Non-binary", "Prefer not to disclose") were based on recommendations for HCI research (Spiel et al., 2019).

- **IUIPC-8**

The IUIPC-10 is a well-established questionnaire that assesses privacy concerns among individuals. It is divided into three main categories: awareness, collection, and control. The IUIPC-8 is an updated version of the IUIPC-10 questionnaire. Gross et al. (2021) found that removing two questions from the original IUIPC questionnaire improved its validity and reliability. We used the IUIPC-8 questionnaire with a 5-point Likert scale (where higher scores indicate greater privacy concerns) to measure participants' general perception of privacy. Based on the interpretation by Gross et al., two statements were removed.

- **Self-identification with the Dupree et al. personas**

Participants were asked to self-identify with the Dupree et al. personas, following the approach used in Dupree et al., (2016) and Rudolph & Feth, (2019). The persona descriptions were slightly modified, as described in 4.1. Each of the five personas was presented as Text 1 to Text 5, and participants selected the one they related to the most.

Participants were asked to imagine they were at a rental home from the next point forward.

- **Self-exploration (icons) or guidance (mascot)**

To assess participants' preference for self-exploration or guided navigation, they were shown two options: icons indicating the location of IoT devices or a mascot guiding them to these devices. This navigation-related question was inspired by Lee et al., (2022). Participants rated the helpfulness of the icons or the mascot using a 5-point Likert scale.

- **Object-centered or user-centered**

To assess participants' preference for object-centered or user-centered screens, they rated their satisfaction with both using a 5-point Likert scale. This question was inspired by Li et al., (2022).

- **Privacy interfaces**

The mockups designed by the author for privacy preference adjustment were displayed to participants. Four different screens were designed to respond to the needs of four different personas. Participants were asked to rate how helpful each screen would be on a 5-point Likert scale.

- **Assessment questions**

The survey ended with seven questions evaluating the system. These questions were based on Prange et al., (2022). Participants were asked (all answered in 5-point Likert scales): how

useful the MR app would be for them; how safe it would make them feel; if it would help them in protecting their privacy. They were additionally asked where they would use such an application (4 options), how frequently (5 options), and why (only qualitative question of the survey; free text). The final question of the survey assessed whether the information participants would like to see on the app would vary depending on the device they are interacting with (4 options).

The online survey was analysed almost exclusively in a quantitative fashion, with the exception of Question 28, which was analysed qualitatively following the principles outlined by Braun and Clarke (Braun & Clarke, 2006). The process began with familiarisation through repeated reading of the responses, followed by the generation of initial codes based on interesting features across the dataset. These codes were then put together into potential themes, which were reviewed and refined to ensure coherence both within and across themes. Then, the themes were clearly defined and named to capture their essence, and the final phase involved producing a narrative that contextualized the findings.

A Miro board was used to organize the responses into themes and categories. Miro is a collaborative online whiteboard platform that allows users to brainstorm, plan, and visualize ideas using several tools such as sticky notes, diagrams, and flowcharts. For the purpose of qualitative analysis, sticky notes were used.

The quantitative data collected from the survey was analysed using Python. Various libraries, including pandas for data manipulation, NumPy for numerical analysis, and matplotlib/seaborn for visualisation, were utilized to process, clean, and interpret the results. Statistical analysis was conducted to identify trends and patterns relevant to the goals of the user survey.

5.1 Results

Demographics

Out of the 150 participants, 76 identified as men (50.7%), 72 as women (48%), 2 as non-binary (1.3%), and 1 participant preferred not to disclose (0.7%). Most participants stemmed from The Netherlands (68.7%). Other participants were from Finland (11.2%), Latvia (8.7%), and Switzerland (7.5%). The most common age group (mode) was 18-29. The most common education group (mode) was Higher Education. The survey took 10 minutes to complete on average, and we compensated each participant with 3£.

Familiarity and Device Ownership

Participants were asked to rate their familiarity with AR, VR and smart devices on a 5-point Likert scale ranging from "Not at all familiar" to "Extremely familiar". The results for familiarity with AR show that the majority reported some level of familiarity, with a concentration in the "Somewhat familiar" category (38.4%). For familiarity with VR, the majority of participants reported some level of familiarity, with a concentration in the "Moderately familiar" category (39.1%).

Online Survey

For familiarity with smart devices, all participants reported some level of familiarity, with most responses concentrated in Moderately Familiar (45.7%). Participants were asked to indicate which smart devices they currently own by selecting from a list of common device categories. The most frequently owned devices were smart TVs, followed by smart lights, smart home appliances, and smart speakers. A smaller number of participants reported owning an augmented or virtual reality headset. All results are summarised in Table 5.1.

Table 5.1: Familiarity with AR, VR, and Smart Devices, and Device Ownership

Technology	Not at all familiar	Slightly familiar	Moderately familiar	Very familiar	Extremely familiar
AR	9.3%	25.2%	38.4%	22.5%	4.6%
VR	0.7%	17.9%	29.8%	39.1%	12.6%
Smart Devices	0%	1.3%	16.6%	45.7%	36.4%

Smart Device Owned (top 5)	Participants (N)
Smart TV	117
Smart Lights	66
Smart Home Devices	53
Smart Speaker	47
Augmented or Virtual Reality Headset	30

To explore whether familiarity with AR or VR influences user preference for user-centered versus object-centered UIs, a Spearman's rank correlation analysis was conducted. All variables were ordinal and non-normally distributed, as confirmed by the Shapiro-Wilk and Anderson-Darling tests. No significant correlation was found between familiarity with AR or VR and satisfaction with the user-centered UI. However, weak but statistically significant correlations emerged between familiarity with AR ($\rho = 0.215, p = 0.008$) and VR ($\rho = 0.187, p = 0.022$) and satisfaction with the object-centered UI. See these results in Table 5.2.

Table 5.2: Spearman's Rank Correlation Between Familiarity with AR and VR, and User-Centered or Object-Centered UI preference.

Variable Pair	ρ	p-value
AR-Fam $\times$ UC-UI	0.070	0.396
VR-Fam $\times$ UC-UI	0.050	0.539
VR-Fam $\times$ OC-UI	0.187	0.022
AR-Fam $\times$ OC-UI	0.215	0.008

Legend: AR-Fam = Familiarity with Augmented Reality, VR-Fam = Familiarity with Virtual Reality, UC-UI = User-Centered UI Satisfaction, OC-UI = Object-Centered UI Satisfaction.

To examine whether familiarity with AR, VR, or smart devices influences users' ratings of different UIs (UI1–UI4), the Kruskal-Wallis test was initially considered. However, due to insufficient data in certain familiarity categories, the analysis proceeded with Spearman's rank correlation. All familiarity and UI rating variables were measured using 5-point Likert scales and

confirmed to be ordinal and non-normally distributed, as determined by the Shapiro-Wilk and Anderson-Darling tests.

No significant correlations were identified between AR familiarity and any of the UI ratings. A weak, but statistically significant positive correlation was observed between VR familiarity and UI1 ($\rho = 0.157, p = 0.055$), suggesting that as VR familiarity increases, users may rate UI1 slightly higher. Additionally, a statistically significant negative correlation was found between IoT familiarity and UI4 ratings ($\rho = -0.209, p = 0.010$), indicating that increased familiarity with smart devices may be associated with lower perceived helpfulness of UI4. All other correlations did not reach statistical significance. Table 5.3 presents these results.

Table 5.3: Spearman's Rank Correlation Between Familiarity with AR, VR, and IoT, and UI Ratings.

Familiarity	UI	ρ	p-value
AR	UI1	-0.007	0.930
AR	UI2	-0.142	0.083
AR	UI3	-0.005	0.947
AR	UI4	-0.122	0.136
VR	UI1	0.157	0.055
VR	UI2	-0.072	0.383
VR	UI3	0.083	0.312
VR	UI4	-0.065	0.429
IoT	UI1	-0.037	0.651
IoT	UI2	-0.145	0.075
IoT	UI3	-0.048	0.560
IoT	UI4	-0.209	0.010

To investigate whether ownership of smart devices influences UI ratings, participants were grouped into Smart Device Owners (N=133) and Non-Owners (N=17) based on their responses. Given the comparison between two independent groups, the Mann-Whitney U test was used. No statistically significant differences were found between IoT owners and non-owners for any of the four UIs: UI1 ($p = 0.806$), UI2 ($p = 0.655$), UI3 ($p = 0.444$), and UI4 ($p = 0.446$). Table 5.4 summarises these results.

Table 5.4: Mann-Whitney U Test Comparing UI Ratings by IoT Ownership.

UI	U Statistic	p-value
UI1	1091.00	0.8060
UI2	1060.50	0.6551
UI3	1253.00	0.4441
UI4	1007.00	0.4463

IUIPC Results

The IUIPC is a well-established privacy questionnaire that measures perceptions of privacy. Higher IUIPC scores indicate higher privacy levels. The IUIPC-8 score is calculated by averaging participants' responses to 8 statements across three dimensions: Control, Awareness, and Collection (Gross, 2021). Each item is rated on a 5-point Likert scale ranging from "Strongly disagree" (1) to "Strongly agree" (5).

Subscale scores are calculated by averaging the responses within each dimension. See Table 5.5 for the IUIPC results of the participants of the online user survey. These results indicate relatively high levels of privacy concerns for all three areas when employing a similar interpretation as prior work (Hoyle et al., 2020).

Table 5.5: Average IUIPC scores, standard deviations, and coefficients of variation.

Category	Mean (SD, CV%)
Overall	4.29 (.85, 19.8%)
Awareness	4.62 (.59, 12.8%)
Control	4.25 (.67, 15.8%)
Collection	4.00 (.85, 21.3%)

To examine whether privacy attitudes differ across the privacy personas defined by Dupree et al., responses to each IUIPC statement were grouped by self-identified persona. The goal was to explore whether individuals who identify with different privacy personas rate the awareness, control, and collection statements differently. Average scores for each statement were calculated within each persona group, as seen in Table 5.6. To test for statistically significant differences, Kruskal-Wallis H-tests were conducted on each statement individually, as shown in Table 5.7.

Table 5.6: Average IUIPC Statement Scores by Persona.

Statement	Amateurs	Fundamentalists	Lazy Experts	Marginally Concerned	Technicians
awa1	4.58	4.67	4.67	4.35	5.00
awa2	4.64	4.67	4.65	4.58	5.00
ctrl1	4.27	4.33	4.27	4.16	4.67
ctrl2	4.07	4.56	4.45	4.00	4.11
coll1	3.76	4.56	4.09	3.61	3.56
coll2	4.18	4.44	4.24	3.55	3.89
coll3	4.22	4.33	4.29	3.84	3.78
coll4	4.00	4.33	4.07	3.32	3.89

Significant differences between persona groups were observed for awa1 ($H = 17.15$, $p = .0042$), ctrl2 ($H = 13.83$, $p = .0167$), and coll1 ($H = 11.61$, $p = .0405$). Post-hoc pairwise comparisons, namely the Dunn's test with Bonferroni correction, revealed that Technicians rated awa1

Table 5.7: Kruskal-Wallis Test Results, followed by Dunn's test with Bonferroni correction for UIIPC Statements by Persona.

Statement	H-statistic	p-value	Significant? ($p < .05$)
awa1	17.15	0.0042	Yes (Marginally Concerned vs. Technicians, $p = .016$)
awa2	5.02	0.4131	No
ctrl1	5.89	0.3170	No
ctrl2	13.83	0.0167	Yes (Lazy Experts vs. Marginally Concerned, $p = .025$)
coll1	11.61	0.0405	Yes (no significant pairwise differences)
coll2	10.23	0.0689	No
coll3	5.87	0.3187	No
coll4	10.18	0.0703	No

significantly higher than the Marginally Concerned ($p = .016$), and Lazy Experts rated ctrl2 significantly higher than the Marginally Concerned ($p = .025$).

Persona results

Participants were asked to identify which privacy persona text they related to the most (persona self-identification). As shown in Table 5.8, participants predominantly selected the "Lazy Experts" persona (36.4%), followed by "Amateurs" (29.8%) and "Marginally Concerned" (20.5%). Fewer participants chose "Technicians" or "Fundamentalists" (each 5.9%), and only 1.3% selected "None of the Above".

Mascot and Icons

Three questions in the survey evaluated the usefulness and preference of a "mascot" and "icons" using a 5-point Likert scale (ranging from "Not At All Helpful" to "Extremely Helpful"). For the mascot, the distribution of scores was not normal, as confirmed by both the Shapiro-Wilk

Table 5.8: Participant Self-Identification with Privacy Personas.

Persona	Percentage of Participants
Lazy Experts	36.4%
Amateurs	29.8%
Marginally Concerned	20.5%
Technicians	5.9%
Fundamentalists	5.9%
None of the Above	1.3%

and Anderson–Darling tests. The median mascot score was 3.0. Similarly, icon scores were also non-normally distributed, with a higher median of 4.0.

A Wilcoxon Signed-Rank Test indicated a statistically significant difference between the mascot and icon scores ($W = 349.00$, $p < .001$), indicating that participants found icons more helpful than the mascot. When asked directly about their preference, the majority of participants favored the icons (71.5%), followed by the mascot (18.5%). Table 5.9 summarizes these findings.

Table 5.9: Participant Preference of Mascot and Icons.

User Preference	
Icons	71.5%
Mascot	18.5%
None of the above	5.3%
I am not sure	4.6%

User-Centered and Object-Centered screens

To evaluate UI placement, participants rated both the User-Centered and Object-Centered interfaces on a satisfaction scale. As shown in Table 5.10, both UIs had a median score of 3, but the Object-Centered UI had a slightly higher mean satisfaction score (3.01 vs. 2.78). Additionally, a greater proportion of participants reported being "Very" or "Extremely Satisfied" with the Object-Centered UI (39.%) compared to the User-Centered UI (29%). A Wilcoxon Signed-Rank Test confirmed that this difference was statistically significant ($W = 2940.0$, $p = 0.0186$), indicating a general preference for the Object-Centered UI, as shown in Table 5.10.

UI Usefulness

A Friedman test revealed a statistically significant difference in average satisfaction scores across the four UI variants ($\chi^2 = 72.20$, $p < .001$). Post-hoc pairwise comparisons using the Wilcoxon Signed-Rank Test with Bonferroni correction identified significant differences between most UI pairs, except between UI1 and UI2 ($p = 0.0884$). UI2 received the highest satisfaction rating ($M = 4.19$), but was not significantly preferred over UI1 ($M = 4.00$). Results are displayed in Table 5.11.

Table 5.10: Comparison of General Preference Between User-Centered and Object-Centered UIs.

Metric	User-Centered UI	Object-Centered UI
Mean Satisfaction Score	2.78	3.01
% Very or Extremely Satisfied	29%	39%
Wilcoxon Signed-Rank Test	Statistic = 2940.0, $p = 0.0186$	

Table 5.11: Average Satisfaction Scores and Significant Differences (Bonferroni-adjusted).

UI	Avg. Score	Significant Differences
UI1	4.00	UI3 ($p = 0.0158$), UI4 ($p = 0.0000$)
UI2	4.19	UI3 ($p = 0.0000$), UI4 ($p = 0.0000$)
UI3	3.77	UI1 ($p = 0.0158$), UI2 ($p = 0.0000$), UI4 ($p = 0.0263$)
UI4	3.46	UI1 ($p = 0.0000$), UI2 ($p = 0.0000$), UI3 ($p = 0.0263$)

Main Hypothesis

The main hypothesis predicted a relationship between personas, UI preferences, and preference for mascot and icons. This hypothesis was not supported by the data. As shown in Figure 5.6, all persona groups favoured "UI2". Additionally, as shown before, most participants, regardless of persona, preferred icons.

Descriptive results

As illustrated in Figure 5.7, 50% of participants rated the application as "Very useful" and 32% as "Extremely useful." Only a small minority found it "Not at all useful" (2%) or "Slightly useful" (6%). Participants were also asked whether such an application would make them feel safer. As shown in Figure 5.8, nearly half (48%) indicated that it would make them feel "A lot safer," and an additional 30% selected "Extremely safer." Fewer participants chose moderate or low safety impacts, with only 3% reporting "Not at all safer."

Participants were asked whether they believed the application would help them protect their privacy. The majority responded positively, with 40% indicating it would help "Very" and 30% selecting "Extremely." Moderate support was reported by 15% of participants, while only a small portion chose lower confidence levels: 9% selected "Slightly" and just 6% responded "Not at all."

Participants were then asked where they would most likely use the application. The majority (63%) reported that they would use it in a holiday home such as an AirBnB or other temporary accommodation. This was followed by 19% who indicated use in their own home, and 13% who would use it in a relative's or friend's home. A small group (6%) selected "Other" contexts.

Then, participants were asked how frequently they would use such an application. As shown in Figure 5.9, 43% reported they would use it "Occasionally, for specific places," while 30% would use it "The first time they visit a place" and 23% "Every time." Only 4% indicated they would never use the app, and no participants selected "Other."

Finally, participants were asked whether the type of information they would like to see on the application should vary depending on the smart device they are interacting with. A majority of 44% responded "Yes," another 37% selected "Maybe". Only 13% said they were "Not sure," and just 5% responded "No".

Online Survey



Figure 5.6: Average UI rating per persona group, showing that the initial hypothesis was incorrect.

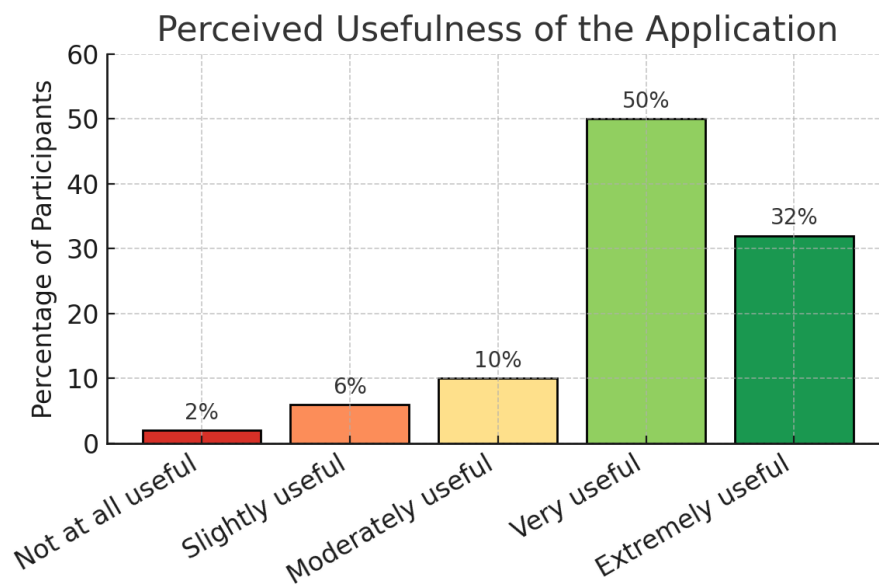


Figure 5.7: Participant answers to the question "Would an application like this be useful for you?"

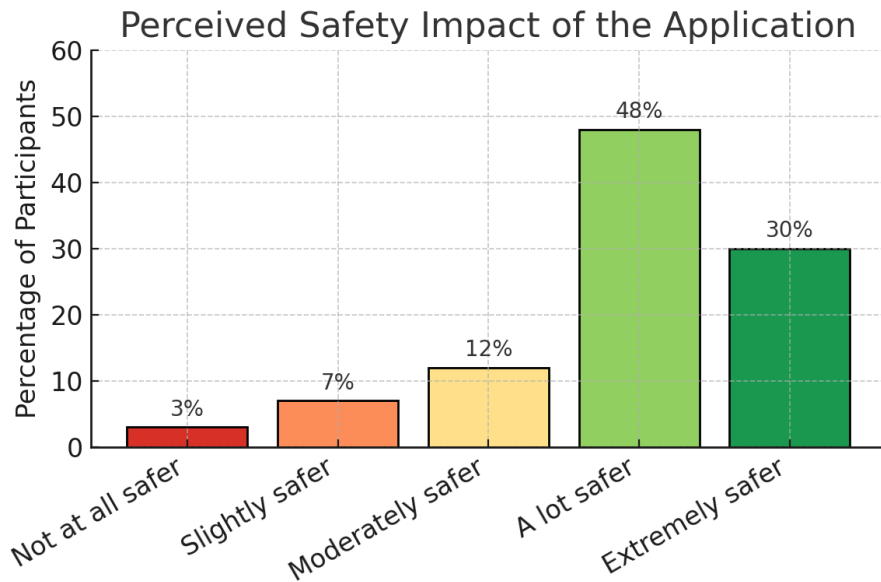


Figure 5.8: Participant answers to the question "Would having access to such an application make you feel safer?"

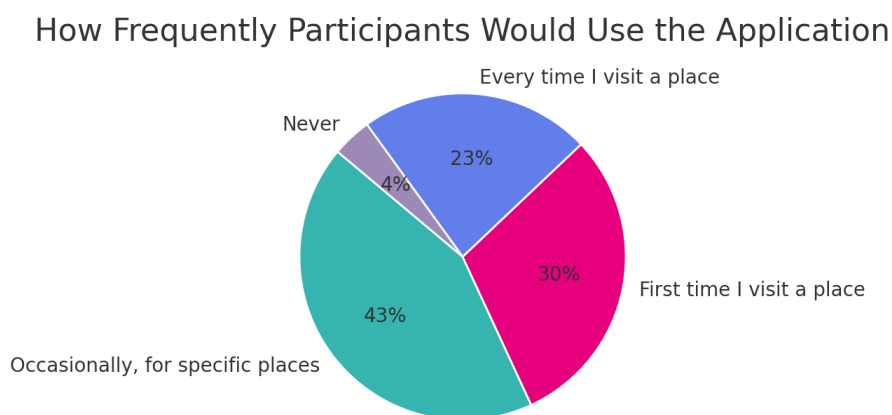


Figure 5.9: Participant answers to the question "How frequently would you use this application?"

Results of the Qualitative Question

An open-ended question was included in the survey to gather participants' opinions on the potential purpose and utility of the application. The question, "Why would you use such an application? For which purpose?", was not mandatory; however, it received responses from 142 out of 150 participants.

The qualitative data collected from this question were analysed to identify recurring themes and categories regarding the participants' motivations and intended use cases for the application. The analysis was done as described in Chapter 3, following the approach outlined by Braun & Clarke (2006).

The results are summarized in Table 5.12. The most frequently mentioned theme was concern surrounding being in unfamiliar places, such as rental homes, which highlights a vulnerability users associate with smart environments. Participants also emphasized the importance of being able to identify devices and understand potential privacy risks. Other notable themes include the need for access controls, safety and privacy reassurance, and the ability to turn off devices.

5.2 Discussion

Based on participant feedback, the mixed reality application showed potential for further development. Most participants rated the concept as "Very" or "Extremely Useful", indicating interest and value in this type of application. This suggested that continuing to work on the concept and building on the mixed reality format aligned with user expectations and preferences.

The rental home scenario used in the online user study resonated well with participants. Many found it relatable and appropriate for exploring privacy concerns and IoT device interactions. Additionally, participants preferred the use of icons, rather than the use of a mascot. This suggests that for privacy-related applications, users might prefer to explore the environment instead of being guided, but more evidence needs to be gathered in future studies for further evaluation.

Compared to similar work (Rudolph et al., 2019), the most notable difference between persona distribution is that in our study, over one-third of participants (36.42%) identified as Lazy Experts, while this group represented only 18% in the Rudolph et al. sample. Moreover, the findings suggest that while overall IUIPC scores are relatively consistent across personas, certain statements reveal meaningful differences in how users perceive and engage with privacy issues based on their persona alignment.

Participants favored object-centered interfaces over user-centered ones. This preference indicates that users found it more natural to interact with interfaces anchored to objects in the environment, rather than with floating or head-locked elements. This result was somewhat unexpected, as in device-rich environments, it could be more cumbersome to interact with multiple screens positioned at different locations. Therefore, this preference should be further tested in actual MR environments to determine whether it remains consistent when interacting with a greater number of devices.

Online Survey

Table 5.12: Results of the free-text question ("Why would you use such an application? For which purpose?") included in the online survey. This analysis was done using the Braun & Clarke method (Braun&Clarke, 2006).

Code	Definition	Quote	Count
Unfamiliar place	Participants expressed concern about privacy when in an unfamiliar location, such as an AirBnB.	"To alleviate my privacy concerns when renting an AirBnB."	35
Identify devices	Participants indicated that the application could assist them in identifying devices present in the room.	"Especially to help identify smart cameras or smart assistants."	24
Privacy risks	Participants mentioned privacy risks that could be mitigated in case they had this or a similar app.	"To know if I am tracked or someone is watching me"	18
Access controls	Participants wanted to access privacy controls.	"To more easily control all the settings of smart devices without having to do everything manually."	15
Privacy or safety	Participants gave short responses like 'privacy' or 'safety'.	"For safety."	15
Turn Off Devices	Participants wanted to be able to turn off smart devices.	"When things feel sketchy. I would mostly use it to turn off as many things as possible."	12
Quality of Life	Participants expressed that the application could improve their life quality.	"To make sure I can feel private and comfortable inside the place."	11
Would Not Use	Participants who would not use the application.	"I would not use the application. I feel like there could be a bit of dishonesty about disabling the smart devices."	8
Knowledge	Participants wanted to learn more about privacy in the context of smart devices.	"To educate myself and get conscious about my environment."	8
Hidden devices	Participants conveyed that finding hidden devices in the environment would be one potentially helpful functionality of the application.	"If it could also find cameras hidden in mirrors and alarm clocks, it would be perfect(...)"	8
Reduce manual effort	Participants stated that using the application could reduce the need for manual changes and/or save time.	"Because adjusting settings on each device separately would take time, expertise, and effort."	5
Security protection	Participants indicated a desire for general security features such as updates, guides, or security-related feedback.	"Get security updates, guides, and feedbacks[sic]"	3

The findings further suggest that users with higher familiarity with immersive technologies may show a slight preference for object-centered UIs. Nonetheless, this pattern might reflect a general preference for object-centered UIs across participants rather than a direct effect of familiarity. The survey results also implicate that smart device ownership does not significantly impact user preferences for any of the tested interfaces. However, the substantial imbalance in group sizes (133 owners vs. 17 non-owners) may have limited the sensitivity of the test and should be taken into account when interpreting the findings.

"UI2" (originally designed for the "Fundamentalists") was the most consistently preferred interface, regardless of participants' self-identified personas. This finding contradicts the original hypothesis that different personas would align with specific UI designs. The result was unexpected, as UI2 requires more time and effort to use, as each smart device parameter must be configured individually. It was initially assumed that only participants with high levels of privacy knowledge and motivation ("Fundamentalists") would find this interface helpful, but this expectation was not supported by the data.

This overall preference for UI2 could be interpreted as a manifestation of the privacy paradox, in which in this case users would claim to value privacy and prefer interfaces that allow for more control, but their actual behaviour may not align with these stated preferences. Another possibility is to interpret these results as suggesting that having access to such tools might increase user interest in more detailed privacy-preserving behaviors, similarly to previous work where users moved beyond default settings when given access to appropriate privacy controls (Fernandez et al., 2021) or displayed a desire to learn more about different sensors when presented with an interactive label (Windl et al., 2024b). The in-person user test that followed aimed to explore these possibilities through a more qualitative approach.

5.3 Limitations

The sample of the online user survey was composed mostly of participants from The Netherlands, and was, therefore, not representative of other European populations. Secondly, participants were screened for fluency in English, excluding European participants who might not be fluent in this language.

While the survey provided participants with visual representations and descriptions of different UI designs, icons, and mascots, these were presented in a static 2D format rather than within an actual MR environment. This limits the ecological validity of the findings, as participant responses may not fully reflect how they would feel or behave when interacting with these elements in an immersive MR scenario. Factors such as spatial interaction, depth perception, gesture-based controls, and environmental distractions could significantly influence satisfaction in ways that this online survey could not capture. As a result, user preferences and perceived helpfulness reported in the survey may differ from actual user experiences during live MR interaction.

Online Survey

Chapter 6

User Test with the HoloLens

The second experiment was an in-person user test in which participants experienced our prototype using the HoloLens 2. This chapter describes the methodology used and details the results of the mixed reality experiment. It presents findings from both the baseline and experimental conditions, the semi-structured interviews, and the self-efficacy and response efficacy assessments. A discussion of the results and study limitations follows.

Building on the work of Jin et al (2022), who explored smart home privacy-protective behaviours (SH-PPBs) and found that users often rely on ad-hoc approaches at the physical layer (e.g., physically blocking smart devices or manually powering them off), this test aimed to evaluate the impact of the app under two different conditions: a baseline condition with no technological assistance, and an experimental condition in which participants interacted with the app.

In the baseline condition, it was expected that users would use ad-hoc strategies to protect their privacy. This condition further aimed at simulating a real-life rental home scenario in which guests generally would not have technological support when attempting to manage smart devices in the context of privacy. In the experimental condition, participants experienced the VISTA app. Then, we compared the actions of participants in both conditions.

The study followed a within-subject design, and the order of conditions was randomized to reduce learning effects. The main hypothesis explored was:

- Participants will report higher levels of self-efficacy and response efficacy after the experimental condition (using the mixed reality app) compared to after the baseline condition.

This test was conducted in the Living Lab (6.1), a specially designed space that simulates a realistic living room environment. The purpose of the lab is to enable researchers to carry out experiments that feel natural and authentic for participants, while still maintaining a controlled setting for accurate data collection. The lab was kept in its usual state, without any added elements or changes. It was used to simulate an AirBnB.



Figure 6.1: The "Living Lab" of the Institute of Behavioural Sciences at the University of St. Gallen in St. Gallen, Switzerland.

We used different smart devices for each condition, with the exception of the smart TV, which remained in the room for both due to setup constraints. In the baseline condition, the devices included a toy robot, a smart purifier, a microphone, a camera, and the smart TV. In the experimental condition, participants encountered a smart speaker, a smart vacuum cleaner, a smart dehumidifier, smart lights, and the same smart TV. An example of a smart device used can be found in 6.2. The positioning of devices differed between conditions, but remained consistent across participants within each condition. One device was always hidden in both setups, with hiding spots chosen to be of comparable difficulty.

Before the start of the experiment, participants completed a brief questionnaire. This questionnaire was identical to the first half of the previously conducted online survey and included demographic and privacy-related questions, such as persona self-identification. In both conditions, participants received the following instructions: "Make this AirBnB more private for your friends/family who are going to arrive soon. You are free to move around and interact within the room as you wish, provided that you do not cause any damage to the devices."

The choice to ask participants to think of their friends or family was based on the rationale that people tend to consider how others will perceive their behaviour when making decisions (Nolan et al., 2008). Additionally, most individuals are interested in maintaining their relationships and avoiding conflict, including in situations in which they want to avoid potential negative reactions from peers due to fear of a privacy threat (Rauschnabel et al., 2018).

Before the first condition, participants were given a consent form and a brief explanation of the study. Then, they received a printed mock AirBnB listing. The listing was created using a template with components from the AirBnB website, and the listed smart devices followed AirBnB's rec-



Figure 6.2: A smart vacuum cleaner, one of the objects used in the in-person user test.

ommendations. For more information on what these recommendations are, see ¹. See Appendix H (7.4) for the listing used.

In the baseline condition (without the mixed reality app), participants were instructed to interact with the physical room for up to five minutes. A short semi-structured interview was conducted to collect qualitative insights, and participants completed a short questionnaire measuring self-efficacy and response efficacy on a 7-point Likert scale (Strongly Disagree to Strongly Agree).

In the experimental condition (with the mixed reality app), participants started by calibrating the HoloLens for their eyes and briefly learning how to use the glasses. Then, they followed the app's user flow. See Figure 6.3 to 6.7 for the five smart device screens shown to participants. While the prototype included additional screens, buttons, icons, and interface elements, these five represent some of the most important screens in the prototype.

After completing the app's user flow, participants were invited to take part in another semi-structured interview and to answer a set of questionnaires, including the SUS and measures of self-efficacy and response efficacy, all measured in a 7-point Likert scale (Strongly Disagree to Strongly Agree).

Response-efficacy is the individual's belief in the effectiveness of the recommended behaviour, while their perceived ability to carry it out is self-efficacy (Zhang et al., 2017). Both were considered highly relevant measurements for this experiment since they are fundamental psychological determinants influencing an individual's acceptance, engagement, and successful application of

¹ See <https://www.airbnb.com/help/article/3061>

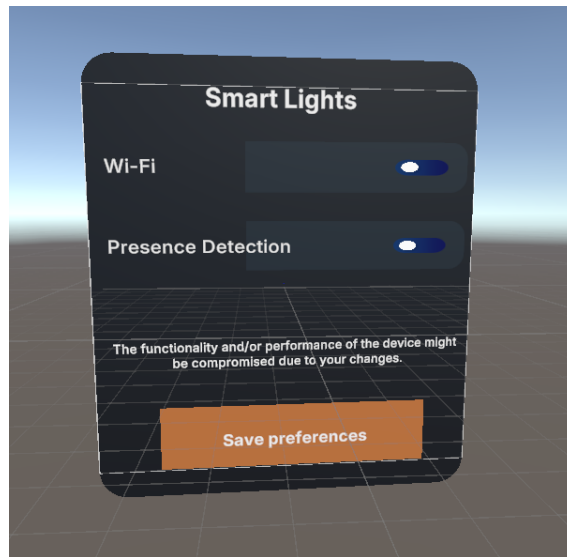


Figure 6.3: Smart lights interface, where users can adjust their privacy preferences by disconnecting the device from Wi-Fi, or disabling its presence detection capabilities.



Figure 6.4: Smart dehumidifier interface, where users can adjust their privacy preferences by disconnecting the device from Wi-Fi, or disabling its voice control or presence detection capabilities.

User Test with the HoloLens



Figure 6.5: Smart speaker interface, where users can adjust their privacy preferences by disconnecting the device from Wi-Fi, or adjusting the microphone level. Note that a help button was also included in case users did not understand the meaning of "microphone level" and how it impacts privacy. If clicked, a help screen would open with a simple explanation.

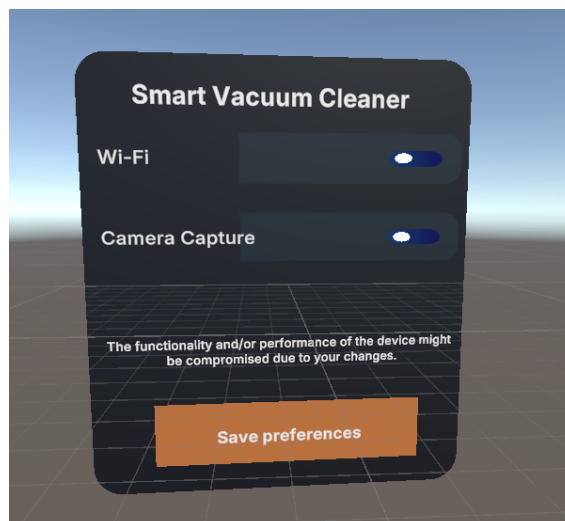


Figure 6.6: Smart vacuum cleaner interface, where users can adjust their privacy preferences by disconnecting the device from Wi-Fi, or disabling its camera capture.

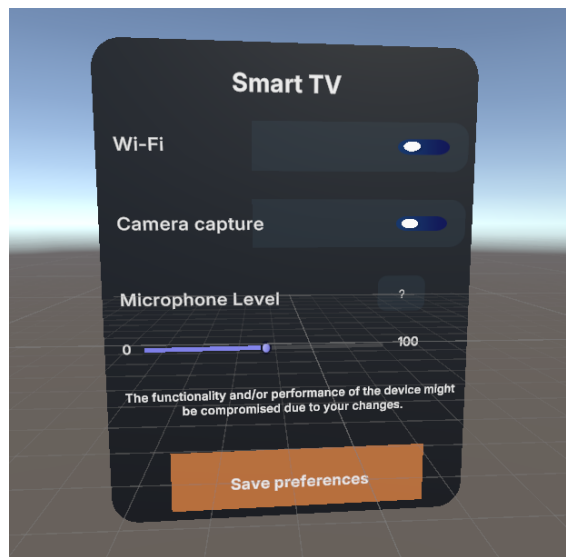


Figure 6.7: Smart TV interface, where users can adjust their privacy preferences by disconnecting the device from Wi-Fi, or adjusting the microphone level. Note that a help button was also included in case users did not understand the meaning of "microphone level" and how it impacts privacy. If clicked, a help screen would open with a simple explanation.

new interventions. The statements included in the questionnaires completed by participants measure these parameters after both conditions and were inspired by the work of Kang & Oh, 2023 and Meier & Krämer, 2024.

The SUS is a highly established questionnaire put forward by Brooke (Brooke, 1996). Several versions of the SUS have been created since. To ensure consistency with most of the existing published work, the standard version is recommended (Lewis, 2018). The version included in this experiment has minor modifications (the word 'cumbersome' was replaced by 'awkward') according to recommendations by Bangor et al. (2008) and Finstad (2006). Additionally, a 7-point Likert scale was used instead of the more frequently used 5-point scale. That was done to ensure consistency with the other Likert scale questions present in this experiment.

The complete set of questionnaire items for both conditions, including the SUS and the guiding questions for the semi-structured interview, can be found in Appendix G (7.4). Participants answered the SUS after experiencing the app and before any other debriefing or discussion as recommended by Brooke (1996).

Twenty five participants were recruited through an internal platform of the University of St. Gallen. A pre-test was done with five of these participants to ensure the consistency of the procedure. The experiment was done in individual sessions. On average, 4 sessions per day were conducted, in a total of 6 days. Each session lasted approximately 40 minutes. Participants were compensated with 25 CHF.

Interview recordings were initially transcribed using OpenAI's Whisper automatic speech recognition (ASR) model to convert audio into text. Following this, the transcripts were checked against the original audio to ensure accuracy. The interviews were then analysed according to the

Braun & Clarke methodology (Braun&Clarke, 2006). The process was the same as outlined in the previous chapter, involving familiarisation, coding, theme development, and narrative synthesis. The quantitative data collected from the questionnaires was analysed using Python and its relevant libraries (pandas, NumPy, matplotlib) for data cleaning, manipulation, visualization, and statistical testing.

6.1 Results

Demographics

All participants resided in Switzerland, but had 8 different nationalities, including German, Austrian, Ukrainian, Chinese, among others. 50% identified as women, and 40% identified as men, while 10% preferred not to disclose. The option "non-binary" was included, but was not selected by any participant. 95% of participants belonged to the 18-29 age group, while 5% belonged to the 30-39 age group. The most common level of education completed (mode) was Bachelor's degree (50%).

Familiarity and Device Ownership

Participants were generally familiar with AR, with 44% declaring to be "Somewhat familiar" with this technology. In relation to VR, 52% declared being "Somewhat familiar". Concerning smart devices, 52% said they were "Moderately familiar". The most common option selected for owning smart devices was "I do not own smart devices". Results are summarized in Table 6.1.

Table 6.1: Familiarity with AR, VR, and Smart Devices, and Device Ownership

Technology	Not at all familiar	Slightly familiar	Moderately familiar	Very familiar	Extremely familiar
AR	0%	45%	40%	15%	0%
VR	0%	25%	55%	20%	0%
Smart Devices	0%	15%	20%	60%	5%

Smart Device Owned	Participants (N)
I do not own smart devices	12
Smart TV	6
Smart Speaker	4
Smart Lights	2
Smart Home Appliances	1

*

IUIPC Results The IUIPC results were calculated in the same manner as indicated in Section 5.1, which employed the IUIPC-8 questionnaire as adapted from the original IUIPC-10 (Gross et al., 2021). This version excludes two items to enhance the scale's validity and reliability. We used a 5-point Likert scale where higher scores reflect greater privacy concerns. The findings suggest that privacy concerns remain relatively high across all three domains, consistent with the interpretations used in previous studies (Hoyle et al., 2020). See Table 6.2 for the IUIPC results, including overall scores and scores per category.

Table 6.2: Average IUIPC scores and standard deviations by category

Category	Mean (SD)
Overall	4.34 (.62, 14.3%)
Awareness	4.60 (.55, 12%)
Control	4.53 (.55, 12.1%)
Collection	4.12 (.89, 21.5%)

Persona Results

Participants were asked to self-identify with the Dupree et al. personas. The persona self-identification results reveal a relatively even distribution among the persona categories, with "Technicians", "Marginally Concerned" and "Amateurs" all receiving 25%. Notably, the persona "Fundamentalists" was not chosen by any participant. Table 6.3 displays all results.

Table 6.3: Participant Self-Identification with Privacy Personas

Persona	Percentage of Participants
Technicians	25%
Marginally Concerned	25%
Amateurs	25%
Lazy Experts	20%
None of the above	5%
Fundamentalists	0%

Table 6.4: Semi-structured interview after the baseline condition: codes, definition, participant quotes, and count. This analysis was done using the Braun&Clarke method (Braun&Clarke, 2006).

Code	Definition	Quote	Count
Unplugging	Participants removed smart devices from power or checked if they were plugged.	"I unplugged everything, or made sure it was not plugged."	10
Confusion regarding the type of device	Participants struggled to identify which device they saw, or if it was a smart device.	"I looked at this robot or whatever it was."	9
Turning the camera around	Participants turned the camera around so it did not face the room.	"I think I put it underneath the shelf, and the camera is supposed to face nothing."	9
Covering sensors	Participants mentioned they would cover sensors if that was possible, or they did cover it with other objects, such as pillows or jackets.	"I wanted to tape it [camera] over, but I didn't have tape."	6
Looking for hidden devices	Participants looked for potentially hidden devices in the room.	"I checked (...) the seating if there's like something [smart device] hidden"	5
Comfort	Participants only associated privacy with comfort, primarily reorganizing the room to make it more "cozy".	"I think I focus more on comfort so that there's more light in the room."	6
Non-device related actions	Participants took physical non-device related actions to make the space more private, such as closing curtains.	"So first I closed the curtains so that it feels more private and that, for example, people won't see from outside."	4
Non-threatening smart devices	Participants considered some smart devices not to be privacy-threatening.	"I checked the air purifier, but it seemed to me like it's a fairly normal appliance that can't jeopardize my privacy that much."	3

6.2 Baseline Condition

Semi-structured Interview

The semi-structured interviews completed after the baseline condition revealed a variety of privacy perceptions and behaviours when faced with the proposed task. Some participants engaged in ad-hoc privacy-preserving actions, including but not limited to unplugging devices, changing the angle of the camera, or covering devices with pillows or jackets. Others engaged in actions not immediately related to the smart devices, such as closing curtains or closing windows.

A few participants searched for smart devices, but declared not being able to find them. A number of participants did not immediately think of smart devices when asked to make the room more private. These participants described changes done to the room as more related to "comfort". A few did not perceive that their privacy was violated by some of the devices. The findings can be found in Table 6.4

Self-efficacy and Response efficacy results

After the baseline condition, participants were asked to answer a questionnaire measuring self-efficacy and response efficacy on a 7-point Likert scale. The summarized results of this questionnaire are shown in Table 6.5 and should be interpreted in comparison with Table 6.8.

Table 6.5: Scores for Self-efficacy and Response efficacy after the baseline condition.

Score Type	Mean	SD	CV (%)
Overall	3.69	1.31	35.5
Self-Efficacy	3.38	1.40	41.4
Response-Efficacy	4.10	1.49	36.3

6.3 Experimental Condition

Semi-structured Interview

The semi-structured interviews conducted after the experimental condition highlighted the choices of participants when interacting with the prototype. Some participants chose to disable microphone and camera captures, while others preferred to disconnect smart devices from Wi-Fi. Some participants felt more concerned about certain devices than others. For instance, a few participants did not feel that their privacy was invaded by the smart dehumidifier or the smart lights, but declared that the smart TV or the smart speaker interfered with their privacy.

When asked about the usefulness of the app, some participants stated that the system would support them in becoming more aware, making more informed decisions, or feeling safer. A number of participants highlighted the trade-off between device functionality and privacy (e.g., watching Netflix versus protecting privacy by disconnecting the TV from Wi-Fi). A number of participants saw the app's potential for AirBnB use, while a few participants identified other relevant use cases for the app, such as managing a large smart living room without having to move around.

A smaller number of participants indicated that the app did not support them in protecting their privacy, and mentioned preferring to use physical actions, such as unplugging the devices. Others explained that protecting their privacy was not a priority at the moment, or that they did not have sufficient knowledge about the issue. A few participants discussed the privacy implications of the headset itself, expressing uncertainty about using it to manage IoT devices. Others reported that they enjoy using smart devices and would prefer to maintain their full functionality.

User Test with the HoloLens

Table 6.6: Semi-structured interview after the experimental condition: codes, definition, participant quotes, and count. This analysis was done using the Braun&Clarke method (Braun&Clarke, 2006). (Part 1)

Code	Definition	Quote	Count
Disabling micro-phones and cameras	Participants disabled microphones and/or cameras found in the room.	"I mostly disallowed the cameras and microphone."	15
Privacy-preserving impact	Participants stated feeling more informed, aware, or safer regarding their privacy.	"It makes me more aware of the devices and it makes me feel less private than if I hadn't used the glasses."	12
Disabling Wi-Fi	Participants reported disabling the Wi-Fi connection of some smart devices.	"And I made sure that not all relevant or not all the smart appliances were necessarily connected to the Wi-Fi if I don't really need them being online, for example."	7
Trade-off between functionality and privacy	Participants considered the trade-off between using the smart devices (functionality) and their privacy-threatening characteristics.	"The only thing I basically left unchanged is the speaker thing, because I mean the only functionality of it is basically that it understands you."	5
Other uses for the app	Participants mentioned other potential uses for the app, such as for individuals organizing large public events.	"I could see it more from a security perspective so for individuals who for whatever reason have to control a certain area or a certain building before some public events"	5
AirBnB use	Participants reported they would use the app in an AirBnB setting.	"It could be useful if I'm, for example, traveling and I'm staying somewhere in a hotel or an AirBnB."	5
Disabling presence detector	Participants reported disabling the presence detector of the smart lights and/or of the smart dehumidifier to protect their privacy.	"(...)everything that was with presence, switched them off(...)."	5
Headset privacy risks	Participants reflected on the privacy risks related to the mixed reality headset.	"Here it is a smart device [headset], it is actually itself making the room not private because it has microphones, it has cameras."	4

Table 6.7: Semi-structured interview after the experimental condition: codes, definition, participant quotes, and count. This analysis was done using the Braun&Clarke method (Braun&Clarke, 2006). (Part 2)

Code	Definition	Quote	Count
App does not support privacy protection	Participants reported that VISTA would not assist them in protecting their privacy.	"I'm not sure I would use it. I think I would just do manual things which are faster and more effective."	3
Non-privacy-threatening AirBnB	Participants expressed that they did not feel like their privacy was threatened by the smart devices found in the AirBnB.	"I mean, I don't see a problem in privacy in these smart devices being able to connect to Wi-Fi."	2
Non-threatening smart devices	Participants considered some smart devices not to be privacy-threatening.	"And the vacuum cleaner, which is for me more like an object and not that interactive, I didn't make any adjustments."	3
Not a priority or Lack of knowledge	Participants indicated that privacy is not a priority for them or that they lack the knowledge surrounding this topic.	"I'm honestly not that concerned about my privacy."	2
Appreciated smart functions	Participants declared appreciation for some functions of the smart devices, and that they would rather have them on.	"I liked the light settings and so on."	2

Self-efficacy and Response efficacy results

After the experimental condition, participants were asked to answer a questionnaire measuring self-efficacy and response efficacy. This questionnaire was measures in a 7-point Likert scale. Results are displayed in Table 6.8 and should be interpreted in comparison with Table 6.5.

Table 6.8: Scores for Self-efficacy and Response efficacy after the experimental condition.

Score Type	Mean	SD	CV (%)
Overall	4.54	1.16	25.6
Self-Efficacy	4.11	1.39	33.8
Response-Efficacy	5.12	1.14	22.2

SUS results

The results show a final SUS score of 66.58, with a standard deviation of 17.42. This score falls slightly below the commonly cited average benchmark of 68, suggesting that users rated the

system’s usability as marginally below average. The coefficient of variation was calculated to be 26.17%, indicating a moderate degree of variability in user responses.

Table 6.9: SUS results.

Metric	Value
Overall average SUS score	66.58
Standard deviation (SD)	17.42
Coefficient of Variation (CV)	26.17%

Hypothesis

The hypothesis considered that participants would report higher levels of self-efficacy and response efficacy after the experimental condition (using the mixed reality app) compared to after the baseline condition. To test this hypothesis, a series of paired-samples *t*-tests was conducted to compare participants’ scores between both conditions. Results showed a statistically significant increase in the overall score under the experimental condition ($M_{\text{diff}} = 0.857$, $t(19) = -2.285$, $p = .034$, $d = 0.511$), indicating a moderate effect size. For self-efficacy, the mean difference was positive but not statistically significant ($M_{\text{diff}} = 0.738$, $t(19) = -1.640$, $p = .117$, $d = 0.367$). A significant improvement was observed in response efficacy scores under the experimental condition ($M_{\text{diff}} = 1.017$, $t(19) = -2.672$, $p = .015$, $d = 0.598$), also reflecting a moderate effect size.

Table 6.10: Paired t-test results comparing Baseline and Tech conditions (n = 20).

Score Type	Mean Difference	t-statistic	p-value	Cohen’s d
Overall Score	0.857	-2.285	0.0340	0.511
Self-Efficacy Score	0.738	-1.640	0.1174	0.367
Response Efficacy Score	1.017	-2.672	0.0151	0.598

6.4 Discussion

The semi-structured interviews in both baseline and experimental conditions highlighted the different preferences and behaviours of participants in the context of privacy. While some participants actively engaged with privacy-preserving actions, others claimed to find these irrelevant or difficult to achieve, and preferred not to alter the environment. These findings highlight the need for user-specific privacy interfaces that adapt to different user needs.

Considering the SUS results, while the system shows acceptable usability, the relatively high standard deviation and CV suggest that user experiences were not entirely consistent. Some participants found the usability above average, while others gave it fairly low ratings, indicating that the interfaces might better align with specific user groups. This finding was expected since the privacy interface implemented in the prototype was originally created for the "Fundamentalists" persona.

The results suggest that the experimental condition positively influenced participants' perceived efficacy, especially in terms of their response to privacy-related risks. The effect on self-efficacy alone did not reach statistical significance. Still, compared to the baseline condition, the scores increased, indicating that the intervention had a positive impact on participant perception of privacy protection.

6.5 Limitations

Most participants were university students aged 18-29. Therefore, the results do not reflect older populations or those with other education levels. The user test was further restricted to those who spoke English and resided in Switzerland. Some participants had never used a mixed reality headset before and learned its basic modes of interaction on the spot, which could have impacted the perceptions on usability, influencing the SUS results.

The prototype created may not reflect real-time integration with IoT devices, reducing realism in the experiment. Furthermore, the smart environment was simulated rather than being a fully connected, real AirBnB setting. These simulations could have affected test outcomes by reducing the realism of the experience.

Some device-specific constraints can further be acknowledged as VISTA was designed and implemented exclusively for Microsoft's HoloLens 2. Participants in the in-person user test also only used the HoloLens 2. While other headsets are available for commercial and research purposes, such as the the Magic Leap 2 or Meta Quest Pro, they were not considered in this study. Furthermore, this research mostly studied the rental home scenario as described earlier, but other scenarios might pose equally significant risks to privacy, such as smart offices, or smart schools.

The screen shown in the prototype was initially designed for the "Fundamentalists" persona. Since it was chosen as the preferred option by all persona groups in the online survey, we included it in the prototype for user testing. However, a key limitation is that no participants who self-identified as "Fundamentalists" took part in the user test, so we could not assess how well this interface performs specifically with that group.

Chapter 7

Conclusion

7.1 Discussion

The results of the online survey challenged initial expectations: participants overall preferred "UI2", an interface that provided granular control over each device found in the smart environment. Options to simplify or automate the user flow were rejected by participants (e.g., "automatically" scanning the environment for smart devices), who preferred more elaborate steps to individually control privacy parameters (e.g., turning off the presence sensor of a smart light set).

These findings might be interpreted as a sign of the privacy paradox, as discussed in previous chapters. However, the overall preference for "UI2" could also be analysed as an increased user interest in more detailed privacy-preserving controls when appropriate tools are available, as found in prior work (Fernandez et al., 2021; Windl et al., 2024b).

Moreover, our results align with previous work by highlighting the diversity of individual privacy needs and differing perceptions of what constitutes a privacy violation (Windl et al., 2023). This further confirms that designers should make use of user research tools (e.g., privacy personas) to create privacy solutions that align with individual user preferences.

Although not the main focus of this study, the informative character of the MR privacy app proposed here carries implications for immersive learning environments. Our approach, including context-aware overlays, the visualization of abstract concepts projected onto the real world, and observed behavioral changes following exposure to specific stimuli is consistent with key themes found in immersive learning research (Beck et al., 2020).

We continue to reaffirm the importance of educating users about privacy in interconnected environments and guiding them toward this information (Windl et al., 2023). This study emphasises the general public's interest in learning more about privacy in smart environments. Having a way to compare the privacy levels of different smart devices through a metric system might be helpful in this context (Windl et al., 2024b), but such a system would need to be regulated by independent third parties and policymakers.

The trade-off between informing users and enhancing awareness versus alarming users and causing distress is beyond the scope of HCI research (Windl et al., 2023), but should be considered

by social scientists who can examine the psychological and behavioral implications of privacy-related interventions. Finally, different privacy behaviours and preferences, illustrated in this thesis by the Dupree et al. privacy personas (Dupree et al., 2016), need to be further explored by user experience researchers and social scientists, especially in light of the privacy paradox and rapid technological advancements.

7.2 Limitations

Besides the limitations already discussed in the context of the user survey and the user test, additional limitations apply to the project as a whole. Due to a lack of existing guidance on how to design a privacy-focused MR app for managing IoT interactions, this work explored a methodological framework to address this gap. This resulted in an MR app that fulfills basic requirements found in the user research phase.

The app was regarded as valuable by participants in both the user survey and the user test. However, it lacked more advanced information, such as why user data is collected by IoT devices and how this data is processed. Including this information would help complement and enrich the app (Abraham et al., 2022). However, due to time and scope constraints, as well as the need to first identify and test more basic functionalities, this information was not included.

While accessibility was considered in terms of colour contrast, further accessibility limitations emerged. Since in both the user survey and the user test, the most common age group was 18-29, little to no input from elderly individuals was collected. Furthermore, accessibility features related to disability were not addressed during this study phase. These aspects suggest broader gaps that should be considered in future iterations.

7.3 Conclusion

This study has looked at effective ways to present privacy notices in smart environments, focusing on how visualizations can enhance user awareness of privacy practices. These visualizations were delivered through a mixed reality (MR) interface. By focusing on the research question, “*What are the most effective design elements to enhance user awareness of privacy practices during interaction with IoT devices in MR?*”, this dissertation aimed at advancing the understanding of privacy communication and design strategies specific to these emerging technologies.

Employing a DBR methodology allowed for design iterations and evaluations intended to improve privacy awareness. Through cycles of mockup and prototyping creation, as well as a user survey and a user test, the study identified design features that influence user privacy awareness, such as icons, object-centered interfaces, and fine-grained parameters that allow users to adjust preferences (e.g., disabling or enabling sensors).

The user survey shed light on the behaviours and preferences of users regarding privacy in smart environments, indicating a clear interest in an MR app that supports privacy protection.

Conclusion

After experiencing the prototype during the user test, participants demonstrated statistically significant improvements in response efficacy, showing that they felt more capable and confident in responding to privacy threats with the assistance of the proposed MR interfaces when compared to having no technological support.

This thesis makes a methodological contribution by integrating user research methods (e.g., privacy personas) with the DBR approach and incorporating input from interdisciplinary scholars. The findings contribute valuable insights into the design of privacy-assisting MR applications and highlight the potential of this medium for effective privacy communication.

In conclusion, this work provides a foundation for developing user-centered privacy designs in MR settings for smart environments. It supports further research into immersive and context-aware privacy interventions that align with users' preferences and behaviours in increasingly connected environments. It does so by using user research methods, the DBR methodology, and through collaboration with interdisciplinary scholars.

7.4 Future Work

Due to time and scope constraints, as mentioned in previous chapters, the "legal screens" (see Appendix 7.4 for the current design of these screens) have not been implemented or tested. These screens were created based on discussions with a legal scholar and on the decision tree by Windl et al. (Windl et al., 2024). Future work should implement and test the legal screens with participants to assess their usability and their potential for privacy assistance. If these designs achieve positive results, it could be a step towards system compliance with the GDPR and the Data Act.

This thesis focused on the scenario of a smart rental home. Future researchers could explore other relevant scenarios, such as smart cities, smart offices, or smart schools. Each of these scenarios might present unique privacy challenges that are worth exploring. For instance, smart schools raise concerns about data collection in the presence of minors, while smart offices may involve situations where individuals feel pressured to consent to data collection due to power dynamics.

Future work should also explore more effective methods for enabling participants to self-identify with, or be accurately assigned to, specific persona categories. This is particularly important given the challenges encountered when applying the Dupree et al. personas, as discussed in Chapter 4. One potential approach could involve developing a dedicated questionnaire to assist participants in identifying with relevant personas. Preliminary exploratory research in this direction was conducted by us and is documented in Appendix 7.4.

In the future, the mixed reality app could be adapted for other headsets other than the HoloLens, such as the Magic Leap 2 or Meta Quest Pro, thereby broadening its accessibility. Additionally, a mobile version could be developed to match users' current mental models and further enhance usability. Accessibility options that might align more closely with the needs of elderly or disabled individuals should be considered in future iterations, examples being voice-controlled interfaces for navigating privacy settings, or haptic feedback to confirm interactions with privacy elements.

Conclusion

Finally, as a culmination of the research and to disseminate our contributions to the broader academic community, the findings presented in this thesis will be prepared as an article to be submitted for publication. We aim to target a leading conference in HCI, namely CHI 2026 (Conference on Human Factors in Computing Systems 2026).

Bibliography

- [1] Abraham, M., McGill, M., & Khamis, M. (2024). What you experience is what we collect: User experience based fine-grained permissions for everyday augmented reality. *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 1–24.
<https://doi.org/10.1145/3613904.3642668>
- [2] Alce, G., Roszko, M., Edlund, H., Olsson, S., Svedberg, J., & Wallergård, M. (2017). [Poster] AR as a user interface for the internet of things—Comparing three interaction models. *2017 IEEE International Symposium on Mixed and Augmented Reality (ISMAR-Adjunct)*, 81–86.
<https://ieeexplore.ieee.org/abstract/document/8088454>
- [3] Anderson, T., & Shattuck, J. (2012). Design-based research: A decade of progress in education research? *Educational Researcher*, 41(1), 16–25.
<https://doi.org/10.3102/0013189X11428813>
- [4] Barth, S., Ionita, D., de Jong, M. D., Hartel, P. H., & Junger, M. (2021). Privacy rating: A user-centered approach for visualizing data handling practices of online services. *IEEE Transactions on Professional Communication*, 64(4), 354–373.
<https://doi.org/10.1109/TPC.2021.3106718>
- [5] Beck, D., Morgado, L., O’Shea, P. (2020). Finding the gaps about uses of immersive learning environments: A survey of surveys. *Journal of Universal Computer Science*, 26(8), 1043-1073.
- [6] Bellman, S., Johnson, E. J., & Lohse, G. L. (2001). On site: To opt-in or opt-out? It depends on the question. *Communications of the ACM*, 44(2), 25–27.
<https://doi.org/10.1145/359205.359241>
- [7] Bellotti, V., & Sellen, A. (1993). Design for privacy in ubiquitous computing environments. In G. De Michelis, C. Simone, & K. Schmidt (Eds.), *Proceedings of the Third European Conference on Computer-Supported Cooperative Work* (pp. 77–92). Springer Netherlands.
https://doi.org/10.1007/978-94-011-2094-4_6
- [8] Bermejo Fernandez, C., Lee, L. H., Nurmi, P., & Hui, P. (2021). PARA: Privacy management and control in emerging IoT ecosystems using augmented reality. *Proceedings*

BIBLIOGRAPHY

- of the 2021 International Conference on Multimodal Interaction*, 478–486.
<https://doi.org/10.1145/3462244.3479885>
- [9] Biselli, T., Steinbrink, E., Herbert, F., Schmidbauer-Wolf, G. M., & Reuter, C. (2022). On the challenges of developing a concise questionnaire to identify privacy personas. *Proceedings on Privacy Enhancing Technologies*.
<https://petsymposium.org/popets/2022/popets-2022-0126.php>
- [10] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- [11] Brooke, J. (1996). SUS—A quick and dirty usability scale. *Usability Evaluation in Industry*, 189(194), 4–7.
- [12] Brown, B. (2001). *Studying the internet experience* (HP Laboratories Technical Report HPL-2001-49). Hewlett-Packard Labs.
<https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=563a300a287ff45eb897d100f26d59d4d87c62c2>
- [13] Brunschwig, C. R. (2014). On visual law: Visual legal communication practices and their scholarly exploration. In E. Schweighofer et al. (Eds.), *Zeichen und Zauber des Rechts: Festschrift für Friedrich Lachmayer* (pp. 899–933). Editions Weblaw.
- [14] Brunschwig, C. R. (2019). Contract comics and the visualization, audio-visualization, and multisensorization of law. *University of Western Australia Law Review*, 46, 191–220.
- [15] Chang, Y., Lim, Y., & Stolterman, E. (2008). Personas: From theory to practices. *Proceedings of the 5th Nordic Conference on Human-Computer Interaction*, 439–442.
<https://doi.org/10.1145/1463160.1463214>
- [16] Cho, H. (2022). Privacy helplessness on social media: Its constituents, antecedents and consequences. *Internet Research*, 32(1), 150–171.
<https://doi.org/10.1108/INTR-07-2020-0403>
- [17] Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81, 42–51.
<https://doi.org/10.1016/j.chb.2017.12.001>
- [18] Chow, R. (2017). The last mile for IoT privacy. *IEEE Security & Privacy*, 15(6), 73–76.
<https://doi.org/10.1109/MSP.2017.4251117>
- [19] Chuah, S. H.-W. (2018). Why and who will adopt extended reality technology? Literature review, synthesis, and future research agenda. *SSRN*.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3300469

BIBLIOGRAPHY

- [20] Cloarec, J. (2020). The personalization–privacy paradox in the attention economy. *Technological Forecasting and Social Change*, 161, 120299. <https://doi.org/10.1016/j.techfore.2020.120299>
- [21] Colnago, J., Feng, Y., Palanivel, T., Pearman, S., Ung, M., Acquisti, A., Cranor, L. F., & Sadeh, N. (2020). Informing the design of a personalized privacy assistant for the internet of things. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. <https://doi.org/10.1145/3313831.3376389>
- [22] ICO. (2024, September 10). *Cookies*. Retrieved October 5, 2024, from <https://ico.org.uk/for-the-public/online/cookies/>
- [23] Cooper, A., Reimann, R., Cronin, D., & Noessel, C. (2014). *About face: The essentials of interaction design* (4th ed.). John Wiley & Sons.
- [24] Correia, J., & Compeau, D. (2017). *Information privacy awareness (IPA): A review of the use, definition and measurement of IPA*. ScholarSpace. <https://scholarspace.manoa.hawaii.edu/handle/10125/41646>
- [25] Culnan, M. J. (2000). Protecting privacy online: Is self-regulation working? *Journal of Public Policy & Marketing*, 19(1), 20–26. <https://doi.org/10.1509/jppm.19.1.20.16944>
- [26] Das, A., Degeling, M., Smullen, D., & Sadeh, N. (2018). Personalized privacy assistants for the internet of things: Providing users with notice and choice. *IEEE Pervasive Computing*, 17(3), 35–46. <https://doi.org/10.1109/MPRV.2018.03367731>
- [27] De Guzman, J. A., Thilakarathna, K., & Seneviratne, A. (2020). Security and privacy approaches in mixed reality: A literature survey. *ACM Computing Surveys*, 52(6), 1–37. <https://doi.org/10.1145/3359626>
- [28] Delgado Rodriguez, S., Prange, S., Vergara Ossenber, C., Henkel, M., Alt, F., & Marky, K. (2022). PriKey—Investigating tangible privacy control for smart home inhabitants and visitors. *Proceedings of the Nordic Human-Computer Interaction Conference*, 1–13. <https://doi.org/10.1145/3546155.3546640>
- [29] Doerner, R., Geiger, C., Oppermann, L., Paelke, V., & Beckhaus, S. (2022). Interaction in virtual worlds. In R. Doerner, W. Broll, P. Grimm, & B. Jung (Eds.), *Virtual and augmented reality (VR/AR): Foundations and methods of extended realities (XR)* (pp. 201–244). Springer International Publishing. https://doi.org/10.1007/978-3-030-79062-2_6
- [30] Draper, N. A., Pieter Hoffmann, C., Lutz, C., Ranzini, G., & Turow, J. (2024). Privacy resignation, apathy, and cynicism: Introduction to a special theme. *Big Data & Society*, 11(3), 20539517241270663. <https://doi.org/10.1177/20539517241270663>

BIBLIOGRAPHY

- [31] Dupree, J. L., Devries, R., Berry, D. M., & Lank, E. (2016). Privacy personas: Clustering users via attitudes and behaviors toward security practices. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 5228–5239.
<https://doi.org/10.1145/2858036.2858214>
- [32] Efroni, Z., Metzger, J., Mischau, L., & Schirmbeck, M. (2019). Privacy icons: A risk-based approach to visualisation of data processing. *European Data Protection Law Review*, 5, 352–366. <https://doi.org/10.21552/edpl/2019/3/7>
- [33] Emami-Naeini, P., Agarwal, Y., Cranor, L. F., & Hibshi, H. (2020). Ask the experts: What should be on an IoT privacy and security label? *2020 IEEE Symposium on Security and Privacy (SP)*, 447–464. <https://doi.org/10.1109/SP40000.2020.00032>
- [34] Eriksson, E., Baykal, G. E., & Torgersson, O. (2025). Design-based research in human–computer interaction: A scoping review. *Interacting with Computers*, 36(1), iwaf030. <https://doi.org/10.1093/iwc/iwaf030>
- [35] European Commission. (2024, October 10). *Data Act*.
<https://digital-strategy.ec.europa.eu/en/policies/data-act>
- [36] Federal Communications Commission. (2025). *U.S. Cyber Trust Mark*. Retrieved May 21, 2025, from <https://www.fcc.gov/CyberTrustMark>
- [37] Feng, Y., Yao, Y., & Sadeh, N. (2021). A design space for privacy choices: Towards meaningful privacy control in the internet of things. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–16.
<https://doi.org/10.1145/3411764.3445148>
- [38] Fineman, B., & Lewis, N. (2018). Securing your reality: Addressing security and privacy in virtual and augmented reality applications. *EDUCAUSE Review*. Retrieved May 21, 2025, from er.educause.edu/.../securing-your-reality
- [39] Goldberg, L. R. (1990). An alternative "description of personality": The big-five factor structure. *Journal of Personality and Social Psychology*, 59(6), 1216–1229.
<https://doi.org/10.1037/0022-3514.59.6.1216>
- [40] Groß, T. (2021). Validity and reliability of the scale internet users' information privacy concerns (IUIPC). *Proceedings on Privacy Enhancing Technologies*, 2021(2), 26–45.
<https://doi.org/10.2478/popets-2021-0026>
- [41] Hadan, H., Wang, D. M., Nacke, L. E., & Zhang-Kennedy, L. (2024). Privacy in immersive extended reality: Exploring user perceptions, concerns, and coping strategies. *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 1–24.
<https://doi.org/10.1145/3613904.3642104>

BIBLIOGRAPHY

- [42] Hagan, M. (2020). Legal design as a thing: A theory of change and a set of methods to craft a human-centered legal system. *Design Issues*, 36(3), 3–15.
https://doi.org/10.1162/desi_a_00598
- [43] Hargittai, E., & Marwick, A. (2016). "What can I really do?": Explaining the privacy paradox with online apathy. *International Journal of Communication*, 10, 3737–3757.
<https://ijoc.org/index.php/ijoc/article/view/4658>
- [44] Harkous, H., Fawaz, K., Shin, K. G., & Aberer, K. (2016). PriBots: Conversational privacy with chatbots. *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*.
<https://www.usenix.org/conference/soups2016/workshop-program/wfpn/presentation/harkous>
- [45] He, Y., Bahirat, P., Knijnenburg, B. P., & Menon, A. (2020). A data-driven approach to designing for privacy in household IoT. *ACM Transactions on Interactive Intelligent Systems*, 10(1), 1–47. <https://doi.org/10.1145/3241378>
- [46] Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). *Privacy cynicism: A new approach to the privacy paradox*. BI Norwegian Business School.
<http://biopen.bi.no/bi-xmlui/handle/11250/2432299>
- [47] Holtz, L.-E., Nocun, K., & Hansen, M. (2011). Towards displaying privacy information with icons. In S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes, & G. Zhang (Eds.), *Privacy and identity management for life* (pp. 338–348). Springer Berlin Heidelberg.
https://doi.org/10.1007/978-3-642-20769-3_27
- [48] Hoyle, R., Stark, L., Ismail, Q., Crandall, D., Kapadia, A., & Anthony, D. (2020). Privacy norms and preferences for photos posted online. *ACM Transactions on Computer-Human Interaction*, 27(4), Article 30. <https://doi.org/10.1145/3380960>
- [49] Iannella, R., Finden, A., & Creations, S. (2010). Privacy awareness: Icons and expression for social networks. *Proceedings of the 8th Virtual Goods Workshop and the 6th ODRL Workshop*, 1–15.
https://www.researchgate.net/profile/Renato-Iannella/publication/267997512_Privacy_Awareness_Icons_and_Expression_for_Social_Networks/links/55d6c4ae08ae9d65948bef84/Privacy-Awareness-Icons-and-Expression-for-Social-Networks.pdf
- [50] Information Commissioner's Office. (n.d.). *Cookies*. <https://ico.org.uk/for-the-public/online/cookies/>
- [51] International Association of Privacy Professionals (IAPP). (n.d.). *IAPP resources*. Retrieved May 5, 2025, from <https://iapp.org/resources/glossary/>

BIBLIOGRAPHY

- [52] IoT Analytics. (2024). *State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally*.
<https://iot-analytics.com/number-connected-iot-devices/>
- [53] Iqbal, U., Bahrami, P. N., Trimananda, R., Cui, H., Gamero-Garrido, A., Dubois, D. J., Choffnes, D., Markopoulou, A., Roesner, F., & Shafiq, Z. (2023). Tracking, profiling, and ad targeting in the Alexa Echo smart speaker ecosystem. *Proceedings of the 2023 ACM on Internet Measurement Conference*, 569–583.
<https://doi.org/10.1145/3618257.3624803>
- [54] Jin, H., Guo, B., Roychoudhury, R., Yao, Y., Kumar, S., Agarwal, Y., & Hong, J. I. (2022). Exploring the needs of users for supporting privacy-protective behaviors in smart homes. *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, Article 19. <https://doi.org/10.1145/3491102.3517602>
- [55] Kang, H., & Oh, J. (2023). Communication privacy management for smart speaker use: Integrating the role of privacy self-efficacy and the multidimensional view. *New Media & Society*, 25(5), 1153–1175. <https://doi.org/10.1177/14614448211026611>
- [56] Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2009). A “nutrition label” for privacy. *Proceedings of the 5th Symposium on Usable Privacy and Security*, Article 1. <https://doi.org/10.1145/1572532.1572538>
- [57] Kelley, P. G., Cesca, L., Bresee, J., & Cranor, L. F. (2010). Standardizing privacy notices: An online study of the nutrition label approach. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1573–1582.
<https://doi.org/10.1145/1753326.1753561>
- [58] King, J. (2014). *Taken out of context: An empirical analysis of Westin’s privacy scale*. Workshop on Privacy Personas and Segmentation.
<https://cups.cs.cmu.edu/soups/2014/workshops/privacy/slpl.pdf>
- [59] Knutzen, K., Weidner, F., & Broll, W. (2021). Exploring augmented reality privacy icons for smart home devices and their effect on users’ privacy awareness. *2021 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct)*, 409–414.
<https://doi.org/10.1109/ISMAR-Adjunct54149.2021.00080>
- [60] Kumaraguru, P., & Cranor, L. F. (2005). *Privacy indexes: A survey of Westin’s studies* (Technical Report CMU-ISRI-05-138). Carnegie Mellon University.
<http://reports-archive.adm.cs.cmu.edu/anon/anon/home/ftp/usr0/ftp/isri2005/CMU-ISRI-05-138.pdf>
- [61] Lee, J., Jin, F., Kim, Y., & Lindlbauer, D. (2022). User preference for navigation instructions in mixed reality. *2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*, 802–811. <https://doi.org/10.1109/VR51125.2022.00099>

BIBLIOGRAPHY

- [62] Lewis, J. R. (2018). The System Usability Scale: Past, present, and future. *International Journal of Human-Computer Interaction*, 34(7), 577–590.
<https://doi.org/10.1080/10447318.2018.1455307>
- [63] Li, Y., Hu, Y., Wang, Z., & Shen, X. (2022). Evaluating the object-centered user interface in head-worn mixed reality environment. *2022 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)*, 414–421.
<https://doi.org/10.1109/ISMAR55827.2022.00060>
- [64] Litman-Navarro, K. (2019, June 12). We read 150 privacy policies. They were an incomprehensible disaster. *The New York Times*.
<https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html>
- [65] MacLean, C. E. (2016). It depends: Recasting internet clickwrap, browsewrap, I agree, and click-through privacy clauses as waivers of adhesion. *Cleveland State Law Review*, 65, 45–78.
- [66] Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1–32.
<https://doi.org/10.1145/3359183>
- [67] Mathur, A., Kshirsagar, M., Mayer, J. (2021, May). What makes a dark pattern... dark? Design attributes, normative considerations, and measurement methods. In *Proceedings of the 2021 CHI conference on human factors in computing systems* (pp. 1–18).
- [68] McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 4(3), 543–568.
- [69] McDonald, A. M., Reeder, R. W., Kelley, P. G., & Cranor, L. F. (2009). A comparative study of online privacy policies and formats. In I. Goldberg & M. J. Atallah (Eds.), *Privacy enhancing technologies* (pp. 37–55). Springer.
https://doi.org/10.1007/978-3-642-03168-7_3
- [70] McParlan, J., & van der Linden, D. (2021). Privacy labels should go to the dogs. *Proceedings of the 8th International Conference on Animal-Computer Interaction*, 1–10.
<https://doi.org/10.1145/3493842.3493888>
- [71] Meier, Y., & Krämer, N. C. (2024). The privacy calculus revisited: An empirical investigation of online privacy decisions on between- and within-person levels. *Communication Research*, 51(2), 178–202.
<https://doi.org/10.1177/00936502221102101>

BIBLIOGRAPHY

- [72] Mellinkoff, D. (2004). *The language of the law*. Wipf and Stock Publishers.
<https://books.google.com/books?hl=en&lr=&id=-zr7DwAAQBAJ&oi=fnd&pg=PR7&dq=The+Language+of+the+Law+By+David+Mellinkoff&ots=iHf8S32-bX&sig=ztxG0SDvXa0rsM9SmT-OEBWr80U>
- [73] Mohammadi, N. G., Pampus, J., & Heisel, M. (2019). Pattern-based incorporation of privacy preferences into privacy policies: Negotiating the conflicting needs of service providers and end-users. *Proceedings of the 24th European Conference on Pattern Languages of Programs*, 1–12. <https://doi.org/10.1145/3361149.3361154>
- [74] Nguyen, R., Gouin-Vallerand, C., & Amiri, M. (2023). Hand interaction designs in mixed and augmented reality head mounted display: A scoping review and classification. *Frontiers in Virtual Reality*, 4, 1171230. <https://doi.org/10.3389/frvir.2023.1171230>
- [75] Nielsen, J. (1994). *Usability engineering*. Morgan Kaufmann. <https://books.google.com/books?hl=en&lr=&id=95As2OF67f0C&oi=fnd&pg=PR9&dq=nielsen+usability&ots=3dBGylfs-r&sig=BXmw1CVPooPItwAj1wKw5LGWl3k>
- [76] Nolan, J. M., Schultz, P. W., Cialdini, R. B., Goldstein, N. J., & Griskevicius, V. (2008). Normative social influence is underdetected. *Personality and Social Psychology Bulletin*, 34(7), 913–923. <https://doi.org/10.1177/0146167208316691>
- [77] Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. <https://doi.org/10.1145/3313831.3376321>
- [78] Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 23(1), 128–147. <https://doi.org/10.1080/1369118X.2018.1486870>
- [79] Paneva, V., Strauss, M., Winterhalter, V., Schneegass, S., & Alt, F. (2024). Privacy in the metaverse. *IEEE Pervasive Computing*, 23(3), 73–78. <https://doi.org/10.1109/MPRV.2024.3381720>
- [80] Passera, S. (2012). Enhancing contract usability and user experience through visualization—An experimental evaluation. *2012 16th International Conference on Information Visualisation*, 376–382. <https://doi.org/10.1109/IV.2012.62>
- [81] Passera, S., & Haapio, H. (2013). Transforming contracts from legal rules to user-centered communication tools: A human-information interaction challenge. *Communication Design Quarterly*, 1(3), 38–45. <https://doi.org/10.1145/2466489.2466498>

BIBLIOGRAPHY

- [82] Pettersson, J. S. (2015). A brief evaluation of icons in the first reading of the European Parliament on COM (2012) 0011. In J. Camenisch, S. Fischer-Hübner, & M. Hansen (Eds.), *Privacy and identity management for the future Internet in the age of globalisation* (pp. 125–135). Springer International Publishing.
https://doi.org/10.1007/978-3-319-18621-4_9
- [83] Pötzsch, S. (2009). Privacy awareness: A means to solve the privacy paradox? In V. Matyáš, S. Fischer-Hübner, D. Cvrček, & P. Švenda (Eds.), *The future of identity in the information society* (pp. 226–236). Springer Berlin Heidelberg.
https://doi.org/10.1007/978-3-642-03315-5_17
- [84] Prange, S., Shams, A., Piening, R., Abdelrahman, Y., & Alt, F. (2021). PriView—Exploring visualisations to support users’ privacy awareness. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–18.
<https://doi.org/10.1145/3411764.3445067>
- [85] Microsoft. (n.d.). *Privacy and compliance*. Retrieved March 20, 2025, from
<https://support.microsoft.com/en-us/office/privacy-and-compliance-9c1e3d75-1ae3-4587-adf6-616ed694e440>
- [86] Rauschnabel, P. A., He, J., & Ro, Y. K. (2018). Antecedents to the adoption of augmented reality smart glasses: A closer look at privacy risks. *Journal of Business Research*, 92, 374–384. <https://doi.org/10.1016/j.jbusres.2018.08.008>
- [87] Reeves, T. (2006). Design research from a technology perspective. In J. van den Akker, K. Gravemeijer, S. McKenney, & N. Nieveen (Eds.), *Educational design research* (pp. 64–78). Routledge. <https://doi.org/10.4324/9780203088364>
- [88] Reilly, D., Salimian, M., MacKay, B., Mathiasen, N., Edwards, W. K., & Franz, J. (2014). SecSpace: Prototyping usable privacy and security for mixed reality collaborative environments. *Proceedings of the 2014 ACM SIGCHI Symposium on Engineering Interactive Computing Systems*, 273–282.
<https://doi.org/10.1145/2607023.2607039>
- [89] Rokhsaritalemi, S., Sadeghi-Niaraki, A., & Choi, S.-M. (2020). A review on mixed reality: Current trends, challenges and prospects. *Applied Sciences*, 10(2), 636.
<https://doi.org/10.3390/app10020636>
- [90] Rossi, A., & Lenzini, G. (2021). Which properties has an icon? A critical discussion on data protection iconography. In T. Groß & T. Tryfonas (Eds.), *Socio-technical aspects in security and trust* (pp. 211–229). Springer International Publishing.
https://doi.org/10.1007/978-3-030-55958-8_12

BIBLIOGRAPHY

- [91] Rossi, A., & Palmirani, M. (2017). A visualization approach for adaptive consent in the European data protection framework. *2017 Conference for E-Democracy and Open Government (CeDEM)*, 159–170. <https://doi.org/10.1109/CeDEM.2017.22>
- [92] Rowland, C., Goodman, E., Charlier, M., Light, A., & Lui, A. (2015). *Designing connected products: UX for the consumer Internet of Things*. O'Reilly Media.
<https://books.google.com/books?hl=en&lr=&id=hv1xCQAAQBAJ>
- [93] Rudolph, M. P., & Feth, D. (2019). Usable specification of security and privacy demands: Matching user types to specification paradigms. *Mensch und Computer 2019 - Workshopband*, 10–18420. <https://doi.org/10.18420/muc2019-ws-121>
- [94] Schaub, F., Balebako, R., Durity, A. L., & Cranor, L. F. (2015). A design space for effective privacy notices. *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, 1–17. <https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub>
- [95] Schermer, B. W., Custers, B., & van der Hof, S. (2014). The crisis of consent: How stronger legal protection may lead to weaker consent in data protection (SSRN Scholarly Paper No. 2412418). *Social Science Research Network*.
<https://doi.org/10.2139/ssrn.2412418>
- [96] Skarbez, R., Smith, M., & Whitton, M. C. (2021). Revisiting Milgram and Kishino's reality-virtuality continuum. *Frontiers in Virtual Reality*, 2, 647997.
<https://doi.org/10.3389/frvir.2021.647997>
- [97] Sloan, R. H., & Warner, R. (2014). Beyond notice and choice: Privacy, norms, and consent. *Journal of High Technology Law*, 14(2), 370–412.
- [98] Soumelidou, A., & Tsohou, A. (2020). Effects of privacy policy visualization on users' information privacy awareness level: The case of Instagram. *Information Technology & People*, 33(2), 502–534. <https://doi.org/10.1108/ITP-03-2019-0115>
- [99] Soumelidou, A., & Tsohou, A. (2021). Towards the creation of a profile of the information privacy aware user through a systematic literature review of information privacy awareness. *Telematics and Informatics*, 61, 101592.
<https://doi.org/10.1016/j.tele.2021.101592>
- [100] Spiel, K., Haimson, O. L., Lottridge, D. (2019). How to do better with gender on surveys: a guide for HCI researchers. *Interactions*, 26(4), 62-65.
- [101] Stewart, E. (2019, December 10). Why every website wants you to accept its cookies. *Vox*.
<https://www.vox.com/recode/2019/12/10/18656519/what-are-cookies-website-tracking-gdpr-privacy>

BIBLIOGRAPHY

- [102] Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT privacy and security: Challenges and solutions. *Applied Sciences*, 10(12), 4102. <https://doi.org/10.3390/app10124102>
- [103] Thakkar, P. K., He, S., Xu, S., Huang, D. Y., & Yao, Y. (2022). "It would probably turn into a social faux-pas": Users' and bystanders' preferences of privacy awareness mechanisms in smart homes. *CHI Conference on Human Factors in Computing Systems*, 1–13. <https://doi.org/10.1145/3491102.3502137>
- [104] Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. *Current Opinion in Psychology*, 31, 105–109. <https://doi.org/10.1016/j.copsyc.2019.08.025>
- [105] Warren, T. (2024, October 1). Microsoft is discontinuing its HoloLens headsets. *The Verge*. <https://www.theverge.com/2024/10/1/24259369/microsoft-hololens-2-discontinuation-support>
- [106] Weiser, M. (1991). The computer for the 21st century. *ACM SIGMOBILE Mobile Computing and Communications Review*, 3(3), 3–11. <https://doi.org/10.1145/329124.329126>
- [107] Interaction Design Foundation. (n.d.). *What are user flows?* Retrieved May 6, 2025, from <https://www.interaction-design.org/literature/topics/user-flows>
- [108] Interaction Design Foundation. (n.d.). *What are user stories?* Retrieved May 6, 2025, from <https://www.interaction-design.org/literature/topics/user-stories>
- [109] Information Commissioner's Office. (2024, December 17). *What is the 'legitimate interests' basis?* <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/what-is-the-legitimate-interests-basis/>
- [110] Williams, M., Nurse, J. R., & Creese, S. (2017). Privacy is the boring bit: User perceptions and behaviour in the internet-of-things. *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, 181–18109. <https://doi.org/10.1109/PST.2017.00029>
- [111] Windl, M., & Feger, S. S. (2024). Designing interactive privacy labels for advanced smart home device configuration options. *Proceedings of the 2024 Designing Interactive Systems Conference*, 3372–3388. <https://doi.org/10.1145/3643834.3661527>
- [112] Windl, M., Schlegel, M., & Mayer, S. (2024). Exploring users' mental models and privacy concerns during interconnected interactions. *Proceedings of the ACM on Human-Computer Interaction*, 8(MHCI), Article 23. <https://doi.org/10.1145/3676504>

BIBLIOGRAPHY

- [113] Windl, M., Winterhalter, V., Schmidt, A., & Mayer, S. (2023). Understanding and mitigating technology-facilitated privacy violations in the physical world. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–16.
<https://doi.org/10.1145/3544548.3580909>
- [114] Wirth, J., Maier, C., & Laumer, S. (2018). The influence of resignation on the privacy calculus in the context of social networking sites: An empirical analysis. *Proceedings of the 39th International Conference on Information Systems*.
<https://core.ac.uk/download/pdf/301378530.pdf>
- [115] Wolfangel, E. (2024, October 24). Rauchmelder bei Vonovia: Der Spion an meiner Decke [Smoke detectors at Vonovia: The spy on my ceiling]. *Die Zeit*.
<https://www.zeit.de/digital/datenschutz/2024-10/rauchmelder-vonovia-mieter-datenschutz-smart>
- [116] Wolford, B. (2018, November 7). What is GDPR, the EU’s new data protection law? *GDPR.Eu*. <https://gdpr.eu/what-is-gdpr/>
- [117] Zeng, E., & Roesner, F. (2019). Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study. *28th USENIX Security Symposium (USENIX Security 19)*, 159–176. <https://www.usenix.org/conference/usenixsecurity19/presentation/zeng>
- [118] Zhang, X., Han, X., Dang, Y., Meng, F., Guo, X., & Lin, J. (2017). User acceptance of mobile health services from users’ perspectives: The role of self-efficacy and response-efficacy in technology acceptance. *Informatics for Health and Social Care*, 42(2), 194–206. <https://doi.org/10.1080/17538157.2016.1200053>
- [119] Ziegeldorf, J. H., Morchon, O. G., Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks*, 7(12), 2728-2742.

Appendix A - User Journey

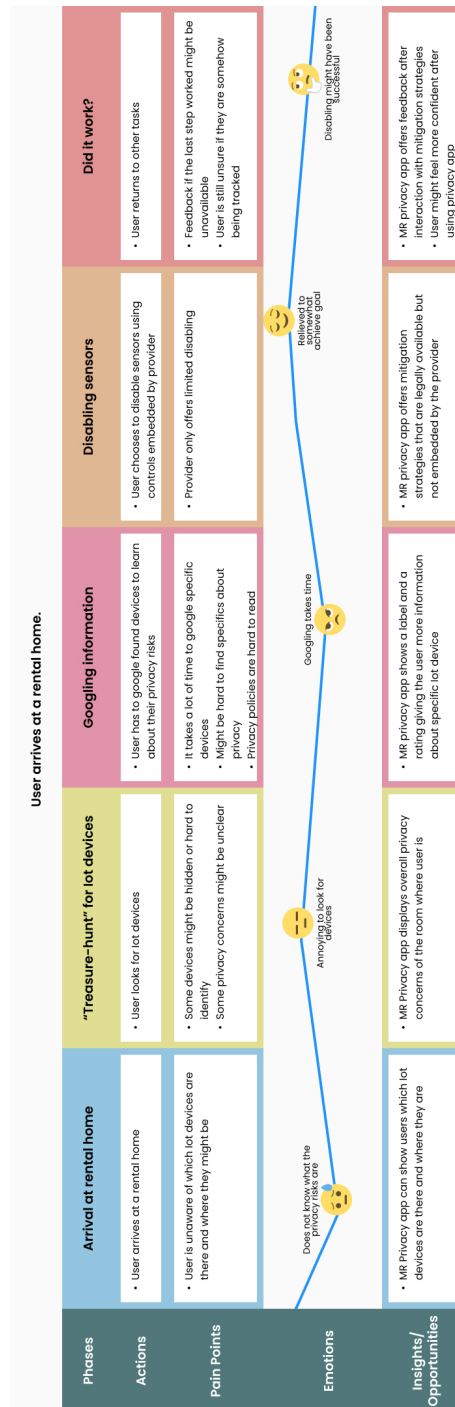


Figure 1: User journey mapping the process of encountering privacy-threatening smart devices in rental homes.

Appendix B: Earlier version of the user flow chart

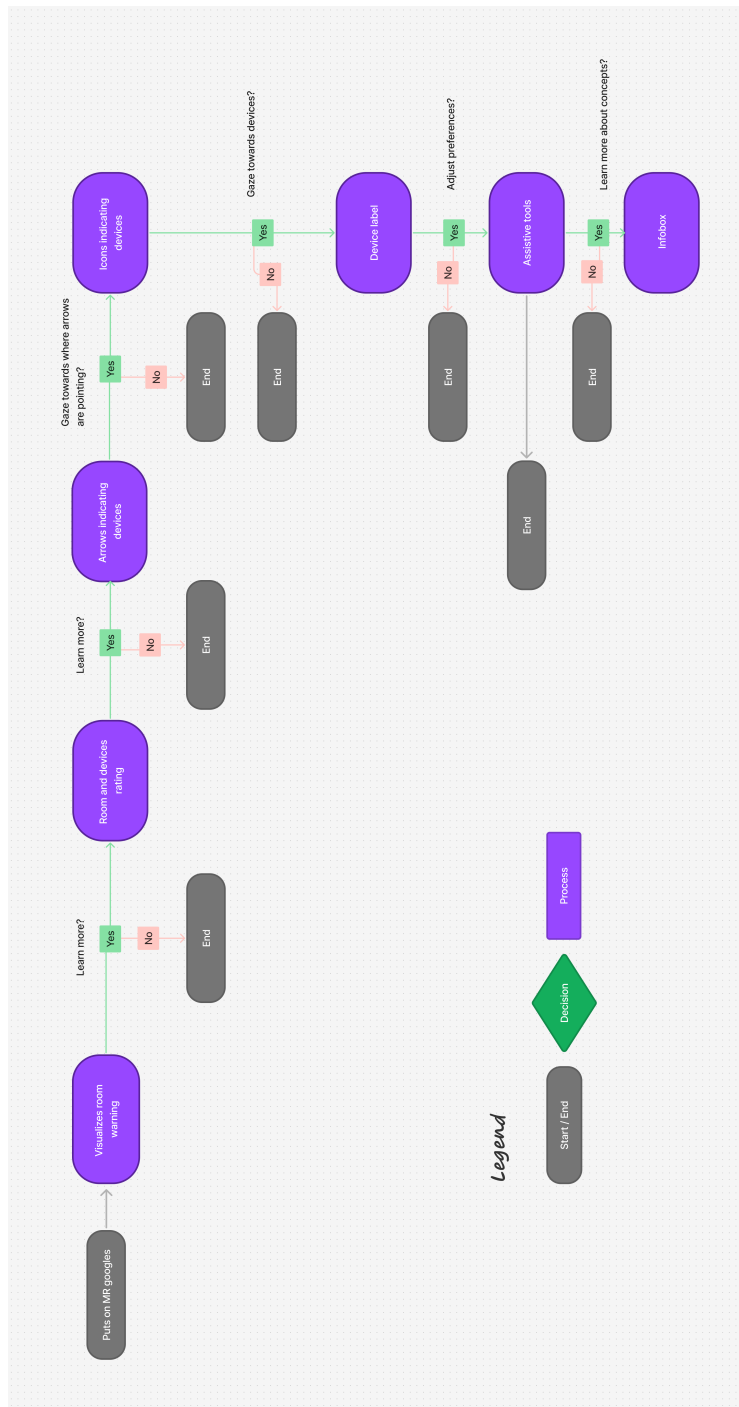


Figure 2: Early version of the user flowchart representing the steps of VISTA.

Appendix C: Legal Designs

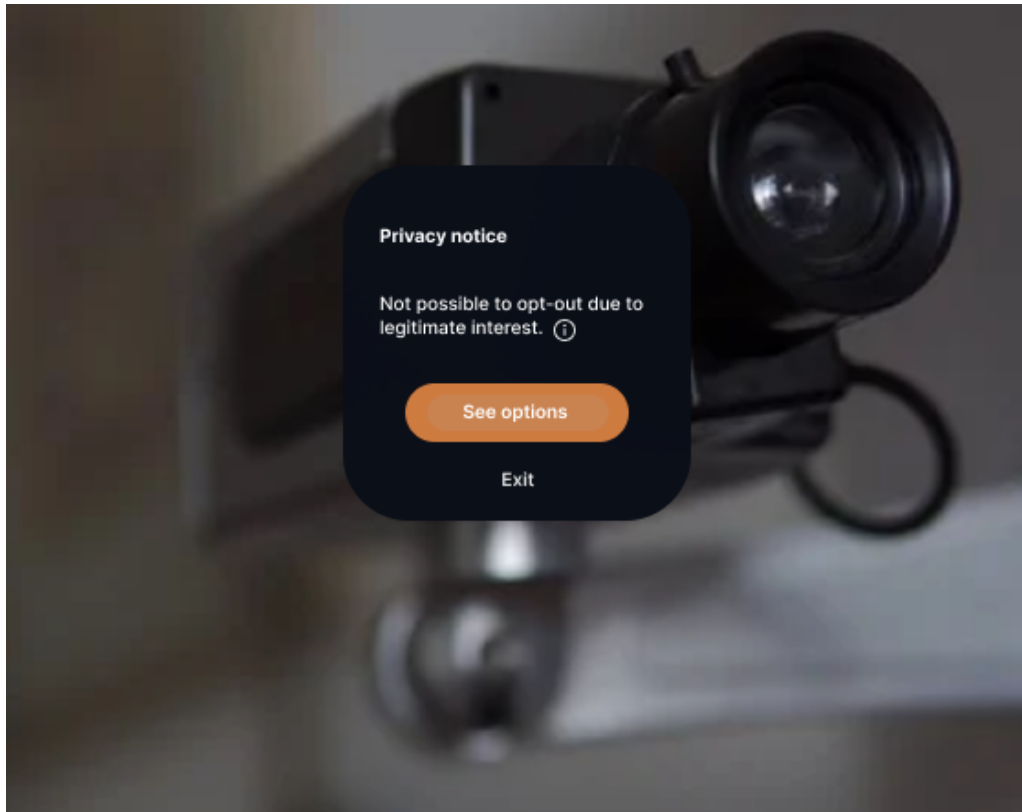


Figure 3: This screen lets users know that it is not possible to influence the data collection of a smart device (here, a camera) due to legitimate interest. The user can then choose to learn more about legitimate interest, click a button to "see options", or exit. "See options" would make the system suggest alternative measures, such as switching off a router.

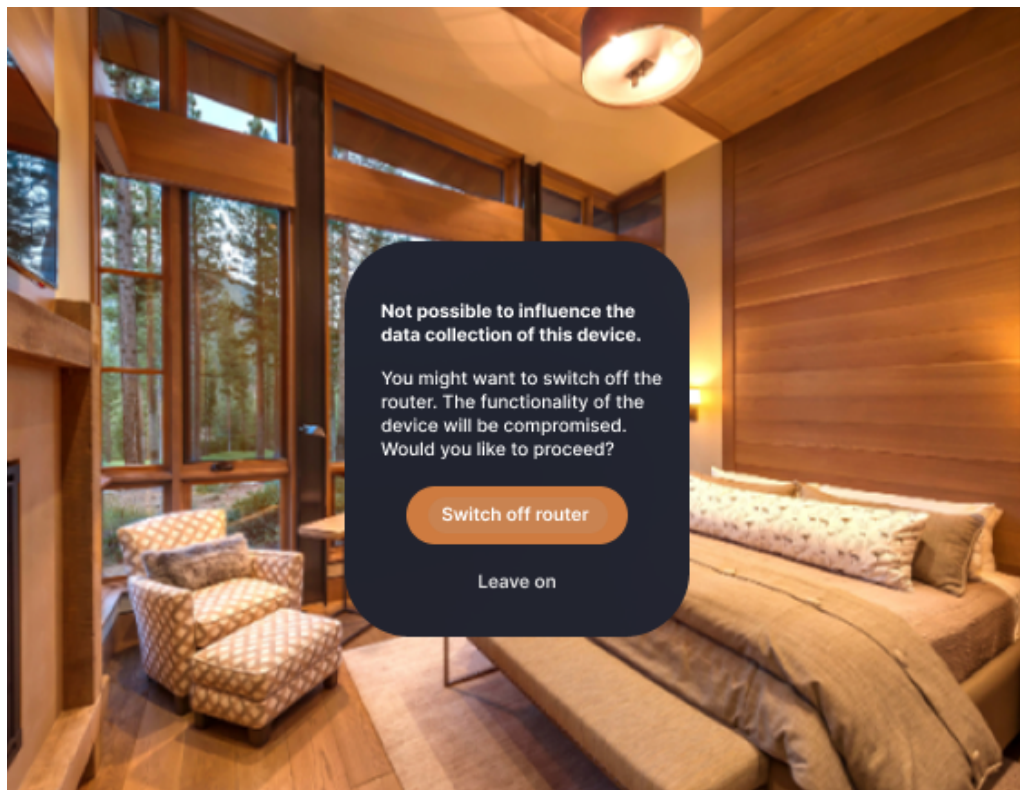


Figure 4: Screen warning users that it is not possible to influence the data collection of a particular device. This could be due to contractual necessity, for instance. In this case, the system would suggest alternative solutions found in the environment, such as switching off the router, as shown above.

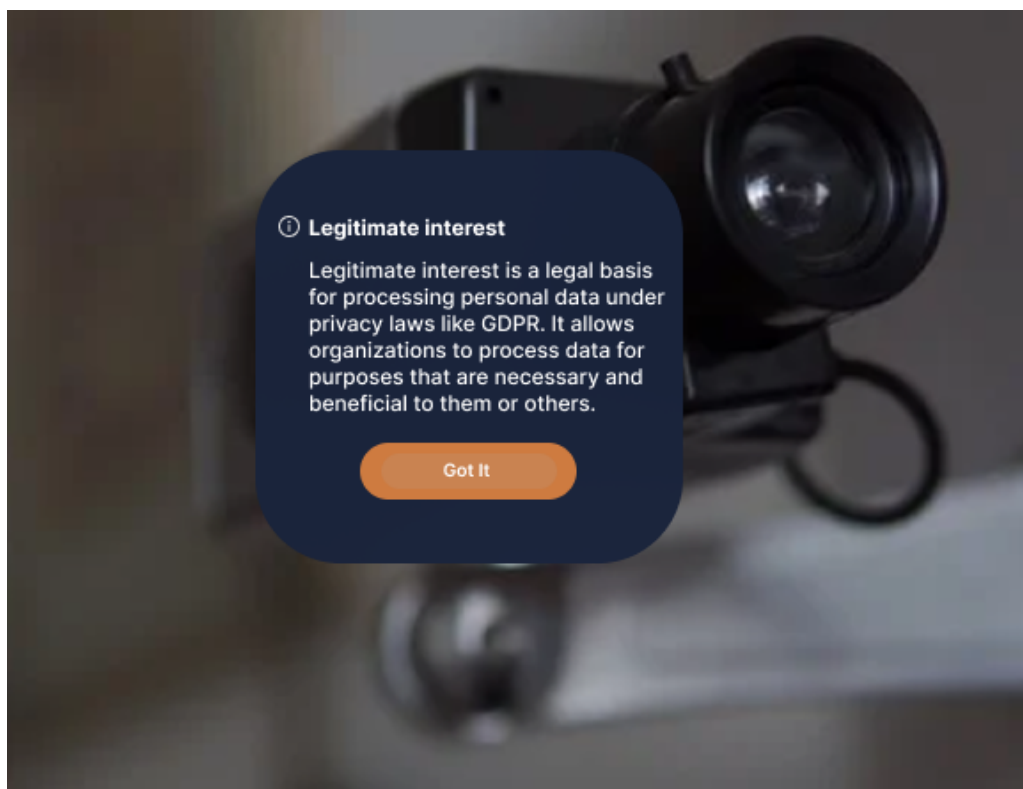


Figure 5: This screen explains to a user the meaning of the term "legitimate interest".

Appendix D: Abandoned Exploratory Analysis

Before launching the online user survey, an exploratory study was conducted to assess how participants would map themselves to one of the five Dupree et al. personas (see Chapter 3 for a more thorough description of those personas and the issues around their use). The goal of this exploration was to develop a questionnaire inspired by the Big 5 Personality Test in which participants could find out in the end which one of the five Dupree et al. personas they had the most in common with.

The Big Five model is a widely validated taxonomy capturing individual differences across Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism (Goldberg, 1990). It served as a basis for developing a new questionnaire and also for calculating its results.

This brief study involved six volunteers, either from the Interactions Research Group or from the author's personal friend circle. Due to limitations in scope and time, as well as inconsistent mapping results, this exploration was abandoned in favor of using the original persona texts provided by Dupree et al., with modifications as listed in Chapter 3.

Participants answered three different questionnaires. The first questionnaire (Survey #1) presented the Dupree et al. persona texts altered by GPT. The second questionnaire (Survey #2) had the Dupree et al. persona texts with minor modifications, presented in the format of 44 statements, with its results calculated in Big 5 fashion. The third questionnaire (Survey #3) had the original Dupree et al. texts, with no modification.

We hypothesized that participants would have the same persona result (or in the case of Survey #2, same top-scoring persona) across all three questionnaires. This result would then validate the "Big Five translation" as a proxy to the original Dupree et al. texts, and potentially improve the process of identifying to which persona each participant corresponds.

Methods

- **Online User Questionnaires:** Developed in Microsoft Forms; participants completed three distinct surveys (Survey #1–#3) to evaluate persona mapping.
- **Participants:** $n = 6$ colleagues from the Interactions Research Group and the researcher's personal network.
- **Tasks:** Each participant completed Survey #1 (GPT-altered persona descriptions), Survey #2 (44 Big 5–style statements scored per standard factor weights), and Survey #3 (original persona texts), then provided open-ended feedback on clarity.
- **Data Collected:** Persona assignments for each survey, Big 5–derived trait scores (from Survey #2), and individual survey completion times.

Lessons Learned

Although not pursued further, this exploration revealed valuable insights for future work. Specifically, developing a new privacy questionnaire—or, more broadly, a novel mechanism that lets participants directly align themselves with persona archetypes—could become a valuable methodological tool in studies where personas serve as key design assets and participant self-identification strengthens both evaluation and iteration.

Table 1: Persona assignments across three survey formats in the exploratory pilot (Top and 2nd result)

Participant	Survey 1 (GPT-altered)	Survey 2 (44 statements)	Survey 3 (Original)	Comments
P1	Lazy Experts (Top); Fundamentalists (2nd)	Lazy Experts 3.7 (Top); Amateurs 3.7 (Top)	Lazy Experts (Top); Technicians (2nd)	Lazy Experts consistently top; tie with Amateurs in Survey 2.
P2	All personas tied	Fundamentalists 3.6 (Top); Technicians 3.5 (2nd)	Lazy Experts (Top); Fundamentalists (2nd)	Inconclusive; no consistency across surveys.
P3	Amateurs (Top); Marginally Concerned (2nd)	Amateurs 4.3; Lazy Experts 3.7	Marginally Concerned (Top); Lazy Experts (2nd)	Amateurs consistently top; Lazy Experts second in Survey 3.
P4	Marginally Concerned & Technicians (Tie Top); Lazy Experts & Amateurs (Tie 2nd)	Amateurs 3.8; Technicians 3.5	Marginally Concerned (Top)	Marginally Concerned appears twice as top.
P5	Lazy Experts & Technicians (Tie Top); Fundamentalists (2nd)	Amateurs 3.6; Fundamentalists 3.6	Lazy Experts (Top); Fundamentalists (2nd)	Lazy Experts appears twice as top.
P6	Lazy Experts (Top); Fundamentalists (2nd)	Amateurs 3.6; Fundamentalists 3.6	Technicians (Top); Amateurs & Lazy Experts (Tie 2nd)	Inconclusive; no consistency across surveys.

Appendix E: Consent Forms

Informed Consent for Survey Participation

Project Description: My name is Camilla Becker, and I am a Master's student in Multimedia at the Faculty of Engineering, University of Porto, under the supervision of Professor Maria van Zeller from the Faculty of Engineering of the same university and Professor Simon Mayer, from the School of Computer Science, University of St.Gallen. This research focuses on enhancing the user awareness of privacy practices during interaction with IoT devices in mixed reality.

Procedure:

During this survey, you will be asked to answer a few questions and analyze a few images. Data on your answers will be collected for scientific purposes.

Confidentiality:

All information collected during this test will be strictly confidential and used solely for research and development purposes. No personal information that could identify you will be shared with third parties without your explicit consent.

Voluntariness:

Your participation is entirely voluntary. You may choose not to participate or withdraw your consent at any time without any penalty. If you decide to withdraw from the study, all data collected up to that point will be deleted.

Benefits and Risks:

Although there are no direct benefits to you for participating in this study, your contribution will be valuable in improving a future application. We do not anticipate any significant risks associated with your participation.

Contact:

If you have any questions or concerns about this survey or your rights as a participant, please contact Camilla Becker via email at up202302008@up.pt or Jannis Strecker at jannisrene.strecker@unisg.ch.

Consent:

By clicking "I consent" you indicate that you have read and understood the information provided above and voluntarily consent to participate in this survey. You understand that the collected data will be handled to ensure participant anonymity, used solely for research purposes, and destroyed after analysis and the conclusion of the student's master's degree, within a maximum period of two years.

Figure 6: Consent form used in the online user survey.

Appendix E

St. Gallen, April/May 2025

Information and consent sheet for the study:
""Using Augmented Reality to interact with smart devices at a rental home""

Objective of the research

You are being invited to participate in a user study investigating privacy in the context of smart devices use in shared spaces. This research is conducted by Camilla Becker (University of Porto) under the supervision of Dr. Simon Mayer (University of St.Gallen) and Dr. Maria Van Zeller (University of Porto). You'll be asked to complete a series of simple tasks and answer some questions.

The Study in a Nutshell

The study will happen as described in the sheet "Experiment Procedure for Participants". Make sure you have read this sheet. Both parts of the experiment will take place in a lab setting and will last in total approximately 1 hour (Address: The Living Lab, Tellstrasse 25 (4th Floor), 9000 St.Gallen).

Processing of your information

Personal Data and Research Data will be anonymized and stored confidentially.

This concerns the following data:

- Demographic data, including your age, gender, level of education, and personality traits,
- Audio recording of your responses in the interview.

Confidentiality of the information

Confidential information or personal data relating to you will not be publicized in any way; no one will be able to trace this information/data back to you. The recordings and written notes from the study will only be shared among the participating researchers. Transcribed data will be used for publication and will be retained for a period of two years. If necessary, the research data will be made available in anonymous form to persons outside the research group (e.g., to monitor scientific integrity).

Voluntary basis

Participation in this research is completely voluntary. No physical, legal, or economic risks are associated with your participation in this research. You don't need to answer any questions which you don't want to answer. As a participant, you can stop participating in the research at any time or, without stating reasons, withdraw your permission to use your information in the research. If you decide to stop participating in the research, this will not have any adverse consequences for you.

Further questions or concerns

This research will be carried out by researchers at University of St. Gallen and University of Porto. If you have any specific questions regarding the handling of personal data, please contact the lead researchers.

If you have questions or would like to withdraw from the study at any time, please email the Executive Researchers, Camilla Becker (up202302008@up.pt) or Jannis Strecker (jannisrene.strecker@unisg.ch)

Figure 7: Consent form used in the in-person user test.

Appendix F: Online Survey Questions

Survey Questions

1. What is your ID? *Question relevant only for Prolific Users*

Type: Single-line text input

2. Gender

Type: Single choice

- Woman
- Man
- Non-binary
- Prefer not to disclose
- Other

3. Age

Type: Single choice

- 18-29
- 30-39
- 40-49
- 50-59
- 60+

4. What is the highest level of education you have completed?

Type: Single choice

- High school or less (or equivalent)
- Unfinished university or associate's degree (or equivalent)
- Bachelor's degree (or equivalent)
- Master's or Doctorate (or equivalent)
- Other

5. How familiar are you with augmented reality?

Type: Likert scale

6. How familiar are you with virtual reality?

Type: Likert scale

7. How familiar are you with smart devices?

Type: Likert scale

8. Which smart devices do you own?

Type: Multiple choice

- Smart Speakers
- Smart Lights
- Smart TVs
- Smart Home Appliances
- AR/VR Headset
- I do not own smart devices.
- I am not sure.
- Other

9. Please indicate your agreement with each of the following statements.

Here IUIPC-8 statements (Gross et al., 2021)

Type: Likert scale

10. Please select 'Strongly agree' below. This is an attention check.

Type: Single choice

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

11. After reading the texts above, which one do you relate to most?

Text 1

I am knowledgeable about privacy and security. I am often a helper because I have a positive view of other's efforts (rather than viewing others as uneducated). I rationalize inaction through a belief that I am not a target. I do, however, take certain actions to protect myself: my password schemes are strong; I write down passwords securely or not at all; I only share passwords with those I trust; and I treat all information I put online as public domain. While I have advanced software manipulation skills, I use this ability to limit my need to interact with security.

Text 2

I have limited knowledge of security concepts and what I do know, I learned from word of mouth or some other informal source. I trust wireless networks and websites that claim to be secure. I like fallback authentication. I can only identify antivirus for software protection. I make changes based on triggers: a common example is switching my password because of a password policy. I have a small set of passwords, with one heavily favoured. I know threats exist, but I do not worry about them. I feel like it is unlikely that something will happen to me, so I am not motivated to do or learn more about security.

Text 3

I have begun learning about security concepts. The challenge is that I am not sufficiently motivated and/or knowledgeable to distinguish good advice from bad, and so still make changes to my practices based on weak or inaccurate advice. Although I have limited motivation, I use some software tools to protect my security, usually an anti-virus and something else—for example a built-in firewall or an ad blocker. I trust but often do not maintain the wireless networks I use. I place some limits on the information I give out. I typically have one stronger or some mid-level set of layered passwords. Finally, again despite limited motivation, given enough information, I will act to protect myself.

Text 4

I am a reluctant helper. I have little or no trust of security technology and watch carefully for security indicators on websites I visit. I have multi-layer password schemes, and important passwords are unique. I may also extend protection beyond the computer, for example by encrypting external storage devices. I am highly concerned about privacy: I may refuse to sign up for accounts and do not like corporate monitoring. Finally, I have a wide ranging of security concerns. I have advanced security knowledge and advanced software manipulation skills. I need fine-grained access to security settings.

Text 5

I am highly motivated but have less knowledge than others. I read online news and blogs to inform myself about security, and I try to understand information before I act on it. I have limited trust of privacy settings on sites like Facebook, am a passive user of social networking, and choose privacy over being social online. My passwords are weaker: I just have low and high security passwords, and, though unique and personal, my passwords were based on one thing. While I have physical security concerns (such as intrusion or viruses), I may also put things off or forget about them, despite being concerned. I tend to

trust their impressions, and I will “know that stuff when I see it.” If given enough information, I am willing to change their behaviors.

Type: Single choice

- Text 1
- Text 2
- Text 3
- Text 4
- Text 5
- None of the above

Now, immerse yourself in a situation in which you are on vacation and this is an apartment that you rented via Airbnb or a similar platform. You have never been here before. You rented the whole apartment for you and whoever is traveling with you. You do not know the host.

In this rental home, you use an app that can assist you with potential privacy concerns of smart devices using Augmented Reality.

In the questions below, you will learn more about the potential features of this app.



12. The app features a mascot that guides you around the rental home, helping you locate smart devices one by one. The mascot shows the most privacy-concerning device first, then guides you to other potentially concerning smart devices in the rental home (if any). How helpful do you think it would be to have a mascot guiding you around the

rental home?



Type: Likert scale

13. The app includes icons that indicate the location and type of each smart device. This allows you to independently explore the environment, searching for devices until you spot their icons. You are free to explore the rental home at your own pace. How helpful do you think it would be to have icons helping you identify the smart devices?



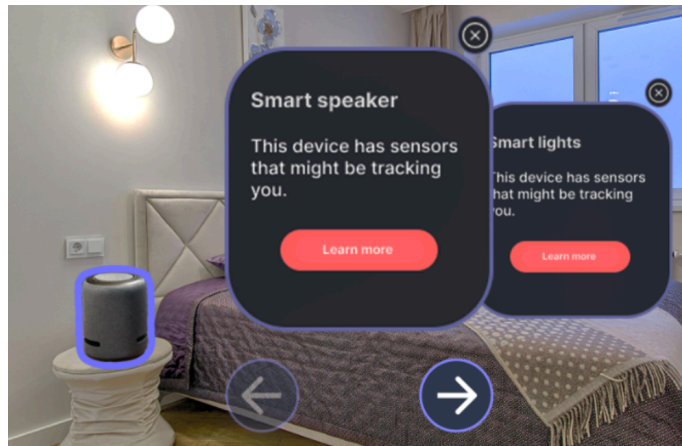
Type: Likert scale

14. After seeing the mascot and the icons, which would you prefer?

Type: Single choice

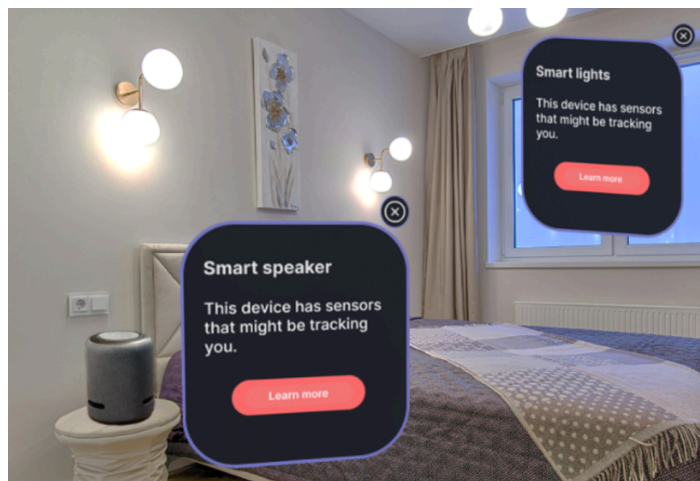
- Mascot
 - Icons
 - None of the above
 - I am not sure
15. To learn more about the devices you have just found, a screen will pop up in the center of your view. Use the arrows or swipe (left or right) to navigate through the screens. Each screen refers to one smart device found in the room where you are at. The smart

devices are additionally highlighted in purple. How satisfied would you be with screens in the center of your view?



Type: Likert scale

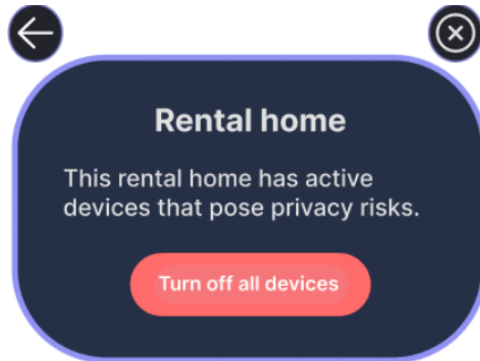
16. Instead of seeing the screens as described in the previous question, another way of visualizing more information about the smart devices (in this case, the speaker and the lights) is to see both screens simultaneously, with each one corresponding to its respective device and positioned close to it. How satisfied would you be with having multiple screens attached to the smart devices?



Type: Likert scale

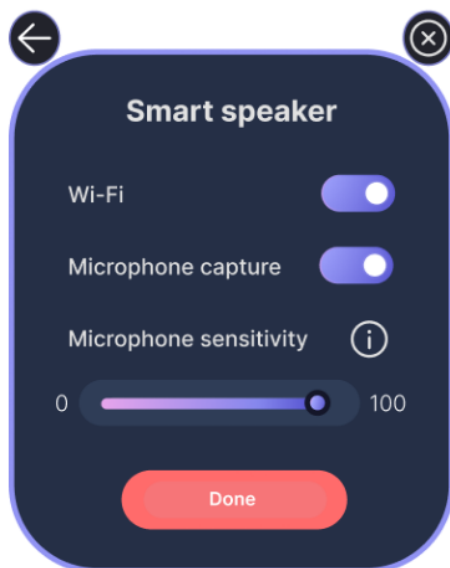
17. Now it's time to let the system know what your privacy preferences are. You could, for example, select a button that turns off all of the smart devices at the rental home where

you are at. How helpful would this function be?



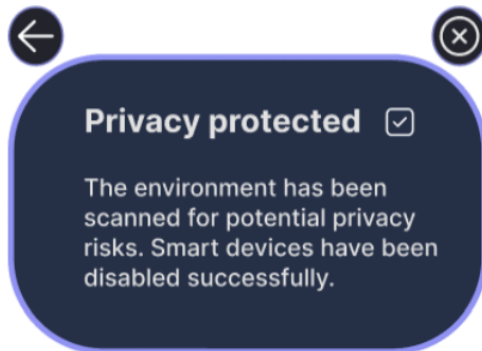
Type: Likert scale

18. Alternatively, you could customize the settings of each smart device (such as a smart speaker) to align with your preferences and enhance your privacy, for instance, by disabling the microphone. How helpful would this function be?



Type: Likert scale

19. In this option, the rental home where you are at is automatically scanned by the system and all of its smart devices are automatically disabled. How helpful would this function be?



Type: Likert scale

20. Another option would be to let the system make privacy decisions for you based on the device you are currently engaging with (in this example, a smart speaker). By clicking "Protect my Privacy", you let the system control the device. How helpful would this function be?



Type: Likert scale

21. The color task you are about to take part is very simple, when asked about your favorite color you must select 'Blue'. This is an attention check.

Based on the text you read above, what color have you been asked to enter?

Type: Single choice

- Black
- Yellow
- Orange
- Blue

- Green

After having learned about this privacy-themed app and its features, please answer the questions below.

22. Usefulness

Would an application like this be useful for you?

Type: Likert scale

23. Safety

Would having access to such an application make you feel safer?

Type: Likert scale

24. Privacy support

Do you think this app would help you protect your privacy?

Type: Likert scale

25. Where would you use such an application?

Type: Multiple choice

- Own Home
- Relative's or Friend's Home
- Holiday Home
- Other

26. How frequently would you use this application?

Type: Multiple choice

- Every time I visit a place
- First time I visit a place
- Occasionally, for specific places
- Never
- Other

27. Why would you use such an application? For which purpose?

Type: Single-line text input

28. Might the information you want differ by smart device?

Type: Single choice

- Yes
- No
- Maybe
- I am not sure

Appendix G: Questions used in the in-person User Test

User Test Questions

Short semi-structured interview after baseline condition (without technology)

- a. What steps did you take to make the space more private?
- b. Did you face any difficulties when attempting to make the space more private?
- c. Did you take any other actions to enhance privacy?

from questionnaire “Your Experience with Digital Privacy Tools (no technology condition)”

- 1. Please indicate any name (does not have to be your own).

Type: Single-line text input

- 2. Please indicate the date and time of your appointment for this experiment.

Type: Single-line text input

- 3. Please indicate your agreement with each of the following statements.

I feel confident in my ability to protect myself in this smart home.

I feel in control over the information I provide on smart devices in this smart home.

I feel confident in my ability to have full control over the information I provide on smart devices in this smart home.

I feel in control of who can view my information on smart devices in this smart home.

Type: Likert scale

- 4. Please indicate your agreement with each of the following statements.

I am able to make informed decisions about my privacy preferences.

I have control over decisions regarding my privacy preferences.

I can protect my privacy at this rental home.

Type: Likert scale

Short semi-structured interview after experimental condition (with the Hololens)

a.What steps did you take to make the space more private?

b.Did you face any difficulties when attempting to make the space more private?

c-Did you take any other actions to enhance privacy?

d-In what ways do you think an application like this could be useful to you?

e-How might having access to such an application affect your sense of privacy when using connected devices?

from questionnaire “Your Experience with Digital Privacy Tools (mixed reality condition)”

1.Please indicate any name (does not have to be your own).

Type: Single-line text input

2.Please indicate the date and time of your appointment for this experiment.

Type: Single-line text input

3.Please indicate your agreement with each of the following statements.

SuS Statements, version used was an updated version from the original, with the word “cumbersome” changed to “awkward” (See Lewis (2018))

Type: Likert scale

4.Please indicate your agreement with each of the following statements.

I feel confident in my ability to protect myself in this smart home.

I feel in control over the information I provide on smart devices in this smart home.

I feel confident in my ability to have full control over the information I provide on smart devices in this smart home.

I feel in control of who can view my information on smart devices in this smart home.

Type: Likert scale

5. Please indicate your agreement with each of the following statements. With the help of the app I experienced,...

...I am able to make informed decisions about my privacy preferences.

...I have control over decisions regarding my privacy preferences.

...I can protect my privacy at this rental home.

Type: Likert scale

Appendix H

Appendix H: Mock "AirBnB"-inspired listing



Start your search

Become a Host

St. Gallen Getaway

★ 5.0 · 7 reviews · Superhost · St. Gallen, Switzerland

Share Save



Your Modern Oasis in St. Gallen - Perfect for Groups & Collaboration

5 guests · 2 bedroom · 3 beds · 1 bath

 Entire home
You'll have the apartment to yourself

 Enhanced Clean
This Host committed to Airbnb's 5-step enhanced cleaning process. [Show more](#)

 Self check-in
Check yourself in with the keypad.

 Free cancellation before May 29

Escape to our bright and airy common space, designed for comfort and connection. This expansive room, flooded with natural light from large windows overlooking lush greenery, offers the perfect blend of relaxation and functionality.

Highlights:

- Spacious & Social: Two plush sofas invite conversation.
- Workspace Ready: A standing desk setup is ideal for remote work.
- Bright & Inviting: A calming and inspiring atmosphere with natural light.
- Smart Home Features: Enjoy the convenience of integrated IoT devices throughout the space.

What this place offers

 Garden view

 Wifi

 Free washer - in building

 Central air conditioning

 Smart devices

 Kitchen

 Pets allowed

 Dryer - in building

 Bicycles

Show all 37 amenities

Things to know

House rules

- 🕒 Check-in: After 4:00 PM
- 🕒 Checkout: 10:00 AM
- 🔒 Self check-in with lockbox
- 👶 Not suitable for infants (under 2 years)
- 🚭 No smoking
- 🐾 No pets
- 🎉 No parties or events

Health & safety

- 🧼 Committed to Airbnb's enhanced cleaning process. [Show more](#)
- 💰 Security Deposit - If you damage the home, you may be charged up to \$566 [Show more](#)

Cancellation policy

Free cancellation before Feb 14

[Show more](#)

Figure 8: Mock "AirBnB"-inspired listing used in the in-person user test.

116

Appendix I

Appendix I: Experiment Procedure for the in-person User Test (for participants)

Experiment Procedure for Participants

1. Welcome

Thank you for participating in our experiment. Please carefully read the provided information letter. If you agree with the described conditions, please provide your consent to participate in this experiment.

2. The Study

This study has two parts, both of which take place in a room set up to resemble a temporary stay (like an Airbnb). You will be asked to imagine you're staying there and that your friends or family will be joining you soon. You will move around the room and decide what you might do to make the space more private for them. If you agree to participate in this study, you additionally will:

-Complete a short online questionnaire about your experience with technology and your general views on privacy (likely you have already done that).

Part 1/Part 2 (clarify the order with the researcher)

1. This part is done without the use of any special tools. You'll receive a printed "AirBnB listing" and simple instructions. You can then walk around the room and take any actions you wish to make it feel more private (max. 10 minutes). Afterwards, we'll ask you a few short questions about your experience.
2. You'll fill out a short questionnaire about your confidence and thoughts during the first activity.

Part 2/Part 1 (clarify the order with the researcher)

1. This time, you will receive support from a digital application displayed through augmented reality glasses (you'll be guided through how to use them).
2. You'll learn how to use the headset, and the system will be set up for you.
3. You'll use the app to explore the room and decide how to make the space more private.
4. Afterwards, you'll be asked a few more questions about your experience
5. You'll fill out a short questionnaire about the system and your feelings about privacy again.

3. Questions?

Do you have any questions before we start the experiment? If you have no questions, we will start the experiment.

Figure 9: Experiment procedure outlining to participants the steps of the experiment.