

An HCI Approach to Privacy and Security in Mobile and Ubiquitous Applications

Mehrdad Bahrini



First Supervisor: Prof. Dr. Rainer Malaka

Second Supervisor: Prof. Dr. Florian Alt

Faculty 3 - Mathematics and Computer Science

University of Bremen

Digital Media Lab

Bremen, Germany

Submitted on 5 November 2024

Defended on 17 December 2024

A thesis submitted to the University of Bremen in partial
fulfillment of the requirements of the degree of
Doctor of Engineering (Dr.-Ing.).

© Mehrdad Bahrini, 2024

Declaration

I hereby declare that I am the sole author of this dissertation and that it is my original work. To the best of my knowledge, no portion of this work has been submitted in support of an application for another degree or qualification at this or any other university or institution of higher education. All sources used, whether directly or indirectly, are fully and accurately acknowledged in the references. I hold the University of Bremen harmless from any liability arising from third-party claims, including copyright infringement, breaches of confidentiality, defamation, or any other infringement of third-party rights.

Faculty: Faculty 3 - Mathematics and Computer Science

Degree: Doctor of Engineering (Dr.-Ing.)

Title: An HCI Approach to Privacy and Security
in Mobile and Ubiquitous Applications

Candidate (ID): Mehrdad Bahrini (2985234)

Signature of Student: _____

Date: 5 November 2024





To my dearest parents,

*In loving memory of my father,
whose spirit and wisdom guide me still.*

*And to my mother,
for her boundless love, strength, and unwavering support.*

With all my love and deepest gratitude.



Abstract

Privacy and security decisions are omnipresent in our digital lives, shaping and influencing our interactions across a broad spectrum of mobile and ubiquitous applications. In today's interconnected world, where personal data flows through numerous digital channels, our privacy and security choices have far-reaching implications. These decisions impact our safety and confidentiality and our trust in digital platforms and services. From managing sensitive information on social media to protecting financial transactions on mobile banking apps, our daily activities are intertwined with navigating and watching our digital identities. As technology advances, the complexity of these decisions grows, necessitating thoughtful consideration and informed choices to maintain control over our privacy and security in an increasingly interconnected and data-driven environment.

This dissertation explores the pivotal role of Human-Computer Interaction (HCI) strategies in improving user understanding, engagement, and decision-making in privacy and security tasks within mobile and ubiquitous applications. Through a variety of research methods and approaches, this work shows how techniques such as gamification, visualization, and augmented reality interfaces improve users' confidence in their ability to manage their privacy and security, enhance their knowledge of these concepts, and empower their overall engagement with privacy and security practices.

Findings emphasize that while privacy concerns are critical, bolstering knowledge and self-efficacy through interactive tools is essential for promoting informed and proactive privacy and security behaviors. The conducted studies advocate a paradigm shift towards empowering users with clear, actionable privacy goals and settings supported by intuitive, accessible interfaces. The implications of this work extend to what developers should consider when designing privacy and security mechanisms. By leveraging HCI approaches, developers can empower user ability and comprehension in mobile and ubiquitous environments, which enhances users' self-efficacy and motivation, enabling them to make informed decisions in digital environments.

Zusammenfassung

Entscheidungen zu Datenschutz und Sicherheit sind allgegenwärtig in unserem digitalen Leben und prägen unsere Interaktionen in einem breiten Spektrum mobiler und allgegenwärtiger Anwendungen. In der heutigen vernetzten Welt, in der persönliche Daten durch zahlreiche digitale Kanäle fließen, haben unsere Datenschutz- und Sicherheitsentscheidungen weitreichende Auswirkungen. Diese Entscheidungen beeinflussen nicht nur unsere Sicherheit und Vertraulichkeit, sondern auch unser Vertrauen in digitale Plattformen und Dienste. Von der Verwaltung sensibler Informationen in sozialen Medien bis hin zum Schutz finanzieller Transaktionen in mobilen Banking-Apps sind unsere täglichen Aktivitäten eng mit der Überwachung und Pflege unserer digitalen Identitäten verknüpft. Mit dem technologischen Fortschritt nimmt die Komplexität dieser Entscheidungen zu und erfordert eine sorgfältige Abwägung und fundierte Entscheidungen, um die Kontrolle über unseren Datenschutz und unsere Sicherheit in einer zunehmend vernetzten und datengetriebenen Umgebung zu wahren.

Diese Dissertation untersucht die zentrale Rolle von Human-Computer Interaction-Strategien zur Verbesserung des Benutzerverständnisses, der Nutzerbindung und der Entscheidungsfindung in Datenschutz- und Sicherheitsaufgaben innerhalb mobiler und allgegenwärtiger Anwendungen. Durch eine Vielzahl von Forschungsmethoden und -ansätzen zeigt diese Arbeit, wie Techniken wie Gamification, Visualisierung und Augmented Reality-Schnittstellen das Vertrauen der Benutzer in ihre Fähigkeit stärken, ihre Privatsphäre und Sicherheit zu verwalten, ihr Wissen über diese Konzepte erweitern und ihr allgemeines Engagement für Datenschutz- und Sicherheitspraktiken fördern. Die Ergebnisse betonen, dass, obwohl Datenschutzbedenken wichtig sind, die Förderung von Wissen und Selbstwirksamkeit durch interaktive Werkzeuge wesentlich ist, um informierte und proaktive Verhaltensweisen in Bezug auf Datenschutz und Sicherheit zu fördern.

Die durchgeführten Studien plädieren für einen Paradigmenwechsel, der darauf abzielt, Benutzer mit klaren, umsetzbaren Datenschutz-Zielen und -Einstellungen zu befähigen, die durch intuitive, zugängliche Schnittstellen

unterstützt werden. Die Implikationen dieser Arbeit erstrecken sich darauf, was Entwickler bei der Gestaltung von Datenschutz- und Sicherheitsmechanismen berücksichtigen sollten. Durch die Nutzung von HCI-Ansätzen können Entwickler die Fähigkeit und das Verständnis der Nutzer in mobilen und allgegenwärtigen Umgebungen stärken, was deren Selbstwirksamkeit und Motivation steigert und ihnen ermöglicht, fundierte Entscheidungen in digitalen Umgebungen zu treffen.

Acknowledgements

I would like to express my profound gratitude to Prof. Dr. Rainer Malaka for his dedicated support and invaluable mentorship throughout my PhD journey. His optimism and wisdom have been a constant source of motivation, fostering an environment supportive of my academic and personal growth. I am equally thankful to Prof. Dr. Florian Alt for his valuable insights, thoughtful feedback, and enriching discussions that helped shape this dissertation. My sincere appreciation goes to my advisor, PD Dr. Karsten Sohr, whose guidance and expertise have been a cornerstone of my research journey. I am also grateful to Dr. Gerald Volkmann for our collaborations, where I coauthored federal research applications and contributed to impactful projects that broadened my experience. My heartfelt thanks go to my colleagues at the Digital Media Lab, especially Irmgard Laumann, Svenja Voß, Philipp Harms, Evgenia Sazonkina, and Gracia Kranz for their dedicated administrative support and kindness, which made my PhD experience truly memorable; their encouragement and passion have been invaluable companions on this journey. I would also like to thank the Digital Media Lab team for their feedback and contributions as coauthors in my scientific work, with special thanks to Nima Zargham, Nina Wenig, Dirk Wenig, Georg Volkmar, Johannes Pfau, and Thomas Münder for their collaborative spirit and generous support. I am immensely grateful to all the students who contributed to my research by completing their theses under my supervision. Their dedication and hard work were essential to the success of multiple studies in this dissertation. Finally, my deepest thanks go to my beloved family. I honor the loving memory of my father, whose influence and wisdom continue to guide and inspire me each day; his enduring presence remains a source of strength and motivation, even in his absence. To my mother, I owe boundless love and gratitude for her unwavering support, patience, and belief in me. Her encouragement has been a constant light through every challenge, reminding me of the values she instilled. I am also profoundly grateful to my brothers, whose steadfast support, understanding, and humor have been an anchor throughout this journey, reassuring me that I am never alone in this endeavor.

Contents

| | |
|--|-------------|
| List of Figures | xiii |
| List of Tables | xvii |
| Acronyms | xix |
| 1 Introduction | 1 |
| 1.1 Research Challenge | 2 |
| 1.2 Contributions | 5 |
| 1.3 Outline | 7 |
| 2 Background | 9 |
| 2.1 Ubiquitous and Mobile Computing | 10 |
| 2.2 Privacy and Security Mechanisms | 11 |
| 2.3 Theoretical Foundations of User Behavior | 17 |
| 2.4 Conceptual and Procedural Knowledge | 26 |
| 2.5 Games and Learning Interplay | 28 |
| 2.6 Knowledge Transfer and Building Self-Efficacy | 32 |
| 2.7 Integrating Theories with HCI Approaches | 37 |
| 3 Security Behavior Elements | 43 |
| 3.1 Motivational Drivers Analysis | 44 |
| 3.2 Individual Abilities Assessment | 86 |
| 3.3 Behavioral Prompts Identification | 139 |
| 4 Empowering User Behavior | 199 |
| 4.1 The Imperative for a Paradigm Shift | 200 |
| 4.2 Informed Behavior Using Interactive Interfaces | 247 |
| 5 Discussion | 343 |
| 5.1 Recap of Research Questions | 344 |
| 5.2 Integration with Theoretical Frameworks | 345 |

| | | |
|----------|---|------------|
| 5.3 | Implications and Contributions | 358 |
| 5.4 | Limitations and Future Directions | 360 |
| 6 | Conclusion | 361 |
| A | Study Materials | 365 |
| A.1 | Study 6 | 366 |
| A.2 | Study 7 | 368 |
| A.3 | Study 8 | 370 |
| A.4 | Study 9 | 371 |
| A.5 | Study 13 | 372 |
| B | Publications | 377 |
| | References | 379 |

List of Figures

| | | |
|------|---|-----|
| 2.1 | Diagram of the Social Cognitive Theory | 18 |
| 2.2 | Diagram of the Fogg Behavior Model | 23 |
| 2.3 | Self-Efficacy, Goals, and User Behavior | 37 |
| 2.4 | Extended Model of the Dissertation | 41 |
| 2.5 | Research Questions Addressing Relationships within the Model | 41 |
| | | |
| 3.1 | Introductory Conversation Interfaces | 48 |
| 3.2 | Gamified Android Settings Interfaces | 50 |
| 3.3 | Final Rating Interfaces | 51 |
| 3.4 | Positive or Negative Messages | 52 |
| 3.5 | <i>Menu</i> and <i>Menu + Hints</i> Variants | 54 |
| 3.6 | Awareness Progression Chart | 57 |
| 3.7 | Perceived Fun and Informative Content Charts | 58 |
| 3.8 | <i>What Could Go Wrong</i> : A Humorous Decision-Making Game | 62 |
| 3.9 | Additional Video Scenarios for the Study | 63 |
| 3.10 | Player Interaction with the Mobile Screen-Lock Options . . . | 64 |
| 3.11 | Navigating Hacking Risks and Rewinding Decisions | 65 |
| 3.12 | Engagement and Task Performance Charts | 68 |
| 3.13 | Contrasting Premises: <i>Save My Home</i> vs. <i>Hacker War</i> | 74 |
| 3.14 | Question Screens: <i>Save My Home</i> vs. <i>Hacker War</i> | 77 |
| 3.15 | Infographics as Supporting Knowledge | 78 |
| 3.16 | SUS and IMI Charts | 80 |
| 3.17 | Pathway from Self-Efficacy to Informed Behavior via Motivation | 85 |
| 3.18 | Infographics vs. Text as Supporting Knowledge | 90 |
| 3.19 | SUS and IMI Charts | 92 |
| 3.20 | Performance Comparison Chart | 93 |
| 3.21 | <i>HappyPermi</i> Screens: Start vs. List of Installed Apps | 98 |
| 3.22 | <i>HappyPermi</i> Screens: Permission vs. Data Flow | 100 |
| 3.23 | Pleasure Dimension of SAM Questionnaire | 101 |
| 3.24 | Arousal Dimension of SAM Questionnaire | 101 |

| | | |
|------|---|-----|
| 3.25 | Dominance Dimension of SAM Questionnaire | 102 |
| 3.26 | SUS and SAM Charts | 104 |
| 3.27 | <i>APK-Info</i> Screenshots | 111 |
| 3.28 | <i>App Inspector</i> Screenshots | 112 |
| 3.29 | <i>Apk Analyzer</i> Screenshots | 113 |
| 3.30 | First-Time Launch of MASS App | 114 |
| 3.31 | First Tab: The Home Screen of MASS | 115 |
| 3.32 | Second Tab: Scanning a Desired App | 116 |
| 3.33 | Scan Results of MobSF in MASS | 118 |
| 3.34 | Pathway from Self-Efficacy to Informed Behavior via Ability . | 138 |
| 3.35 | Simon’s Introduction, App Store, and Flashlight Details . . . | 143 |
| 3.36 | App Installation and Initial Setup | 144 |
| 3.37 | Permissions, Financial, and Health Input Options | 145 |
| 3.38 | Simulator Versions | 146 |
| 3.39 | Privacy and Security Recommendations | 147 |
| 3.40 | Risk Perception Comparison Chart: Tools | 150 |
| 3.41 | Risk Perception Comparison Chart: Games | 151 |
| 3.42 | Risk Perception Comparison Chart: Health & Fitness | 152 |
| 3.43 | Risk Perception Comparison Chart: Social Media | 152 |
| 3.44 | Device Selection Screens | 161 |
| 3.45 | Navigation and Icon Explanations | 162 |
| 3.46 | <i>List</i> and <i>Tab-Based</i> Interfaces | 163 |
| 3.47 | <i>Device-based</i> Interface | 164 |
| 3.48 | SUS Scores Comparison Across Conditions | 168 |
| 3.49 | NASA-TLX Dimensions Comparison Across Conditions . . . | 170 |
| 3.50 | First Story: Why Privacy Matters? | 177 |
| 3.51 | Second Story: Amazon Echo Shared Audio | 178 |
| 3.52 | Third Story: Fictional Story | 179 |
| 3.53 | IP Camera Registration Screen | 179 |
| 3.54 | Personal Data Screen | 180 |
| 3.55 | IP Camera Cloud Subscription | 180 |
| 3.56 | Payment Information | 181 |
| 3.57 | Checkout Summary | 181 |
| 3.58 | Successful Cloud Subscription for the IP Camera | 182 |
| 3.59 | Initial Presentation of Privacy Choices | 182 |
| 3.60 | User-Customizable Privacy Choices | 183 |
| 3.61 | On-Demand: Navigation Bar | 183 |
| 3.62 | Configurable Choices Distributed Across Device Registration | 184 |
| 3.63 | At-Setup/Just-in-Time: Settings Interface | 185 |
| 3.64 | Privacy Choices Analyze | 185 |

| | | |
|------|---|-----|
| 4.1 | Smart Home Configuration Wizard | 203 |
| 4.2 | Light Bulb Configuration Screens | 204 |
| 4.3 | Camera Configuration Screens | 205 |
| 4.4 | Speaker Anonymization Configuration Screens | 205 |
| 4.5 | Speaker Logs and Access Control Configuration Screens | 206 |
| 4.6 | Data-Sharing Preferences and Communication Protocols | 207 |
| 4.7 | Privacy and Security Terms Familiarity | 212 |
| 4.8 | Research Model for the Study | 214 |
| 4.9 | The Accurate Data Flow Model of the Study | 215 |
| 4.10 | Overview of the Permissions Using MobSF | 226 |
| 4.11 | Analyzing a Health App With MobSF | 227 |
| 4.12 | Monitored Network Communication Using Burp Suite | 229 |
| 4.13 | Overview of Analysis Steps and Objectives | 231 |
| 4.14 | Number of Recipients in the Respective Categories | 232 |
| 4.15 | Server Locations of Third-Party Recipients | 233 |
| 4.16 | Data Sent Before Consent to the Privacy Policy | 234 |
| 4.17 | Dark Patterns Found in Privacy Policies Interfaces | 235 |
| 4.18 | Privacy Policy Screenshots | 236 |
| 4.19 | Leap Fitness Group Privacy Policy Interfaces | 238 |
| 4.20 | Registration, Room Selection, and Device Placement | 252 |
| 4.21 | Comparison of <i>Connector</i> and <i>Linker</i> Versions | 253 |
| 4.22 | Comparison of UEQ+ Subscales | 259 |
| 4.23 | Gender Comparison of UEQ+ Subscales (<i>Linker</i>) | 262 |
| 4.24 | Research Model for the Study | 272 |
| 4.25 | Presenting Selected Device in the AR App | 274 |
| 4.26 | Bosch Smart Home Controller One-Pager Privacy Policy | 275 |
| 4.27 | Smart Home Setup in the AR App | 277 |
| 4.28 | Bosch Smart Home Controller Configurable Options | 278 |
| 4.29 | Alexa Cloud and Connection 2D Interfaces | 279 |
| 4.30 | Participant Identification and Task Completion Tracking | 280 |
| 4.31 | Bremen Ambient Assisted Living Lab | 281 |
| 4.32 | User Study Procedure | 285 |
| 4.33 | The Accurate Data Flow Model of the SH-Setup | 290 |
| 4.34 | Sample Sketches From the Participants | 290 |
| 4.35 | Model Testing Results | 299 |
| 4.36 | UEQ Comparison Benchmarks Chart | 300 |
| 4.37 | Research Model for the Study | 307 |
| 4.38 | Presenting Selected Device in the 2D App | 309 |
| 4.39 | Task Completion Tracking in the 2D App | 310 |
| 4.40 | The Bremen Ambient Assisted Living Lab (BAALL) | 311 |

| | | |
|------|---|-----|
| 4.41 | User Study Procedure | 314 |
| 4.42 | Participant Demographics Comparison: AR vs. 2D Studies . . | 314 |
| 4.43 | Participant Experience and Knowledge: AR vs. 2D Setups . . | 316 |
| 4.44 | Participant IUIPC Comparison: AR vs. 2D Studies | 317 |
| 4.45 | The Accurate Data Flow Model of the SH-Setup | 318 |
| 4.46 | Sample Sketches From the Participants | 318 |
| 4.47 | Comparison of Participant Drawings in AR and 2D Studies . . | 320 |
| 4.48 | Model Testing Results | 327 |
| 4.49 | UEQ Comparison Benchmarks Chart | 328 |
| 4.50 | Extended Model of the Dissertation | 341 |
| 5.1 | Extended Model of the Dissertation | 359 |

List of Tables

| | | |
|------|--|-----|
| 3.1 | Interface Design Evaluation | 133 |
| 3.2 | Overall Risk Assessment | 149 |
| 3.3 | NASA-TLX Dimensions | 169 |
| 3.4 | ATI Scales Across All Groups | 189 |
| 3.5 | IUIPC Subscales Across All Groups | 189 |
| 3.6 | Self-Efficacy Across All Groups | 190 |
| 3.7 | Awareness Assessment | 190 |
| 3.8 | Perceived Privacy Protection | 190 |
| 3.9 | Average Number of Checked Checkboxes | 191 |
| | | |
| 4.1 | Locations of Terms in Smart Home Apps | 201 |
| 4.2 | IUIPC Dimensions and Context-Specific Factors | 211 |
| 4.3 | Security Terms Descriptive Statistics | 213 |
| 4.4 | Being Informed and Participants' Behavior Intention | 213 |
| 4.5 | Category of Mistakes and Number of Errors | 215 |
| 4.6 | Health & Fitness and Medical Apps | 225 |
| 4.7 | IUIPC Dimensions and Context-Specific Factors | 257 |
| 4.8 | Correlations among Variables Related to Privacy Concerns | 258 |
| 4.9 | UEQ+ (<i>Linker & Connector</i>) | 258 |
| 4.10 | UEQ+ Paired Samples T-Test | 259 |
| 4.11 | IUIPC Scores and Privacy Concerns by Gender | 261 |
| 4.12 | UEQ+ Subscales by Gender with T-Test (<i>Linker</i>) | 262 |
| 4.13 | UEQ+ Subscales by Gender (<i>Connector</i>) | 263 |
| 4.14 | IUIPC Dimensions and Context-Specific Factors Scores | 289 |
| 4.15 | Results of the Participant Drawings | 291 |
| 4.16 | IMI Questionnaire Results and Paired T-Test Comparisons | 297 |
| 4.17 | Informed Behavior Results and Paired T-Test Comparisons | 297 |
| 4.18 | Cronbach's α Scores | 298 |
| 4.19 | UEQ Results and Paired T-Test Comparisons | 299 |
| 4.20 | IUIPC Dimensions and Context-Specific Factors Scores | 316 |

| | |
|--|-----|
| 4.21 Results of the Participant Drawings | 319 |
| 4.22 IMI Questionnaire Results and Paired T-Test Comparisons . | 324 |
| 4.23 Informed Behavior Results and Paired T-Test Comparisons . | 325 |
| 4.24 Cronbach's α Scores | 325 |
| 4.25 UEQ Results and Paired T-Test Comparisons | 328 |

Acronyms

| | |
|---------------|--|
| AUI | Adaptive User Interface |
| app | application |
| API | Application Programming Interface |
| APK | Android Package |
| AR | Augmented Reality |
| ATI | Affinity for Technology Interaction |
| BAALL | Bremen Ambient Assisted Living Lab |
| CIA | Confidentiality, Integrity, and Availability |
| CLT | Cognitive Load Theory |
| CySESH | Cybersecurity Self-Efficacy in Smart Homes |
| EU | European Union |
| FBM | Fogg Behavior Model |
| GDPR | General Data Protection Regulation |
| HCI | Human-Computer Interaction |
| IMI | Intrinsic Motivation Inventory |
| IoT | Internet of Things |
| IUI | Intelligent User Interface |
| IUIPC | Internet Users' Information Privacy Concerns |
| KPI | Key Performance Indicator |
| SAM | Self-Assessment Manikin |
| SDT | Self-Determination Theory |
| SCT | Social Cognitive Theory |
| SLT | Social Learning Theory |
| SSL | Secure Sockets Layer |

| | |
|-------------|------------------------------------|
| SUS | System Usability Scale |
| TTAT | Technology Threat Avoidance Theory |
| UEQ | User Experience Questionnaire |
| VPN | Virtual Private Network |
| WPS | Wi-Fi Protected Setup |

1

Introduction

We find ourselves amidst a significant technological revolution. Computers and the Internet have fundamentally reshaped our lifestyles and professional landscapes in just a few decades. Technology is now seamlessly integrated into our daily lives, with innovations in communication and internet connectivity fueling transformation across countless domains. For example, smartphones have become essential tools, enabling people to fulfill various needs and stay connected with the world. Technology now enhances productivity, fosters social connections, enables access to information, and much more, establishing itself as an essential part of everyday life (Kushlev et al., 2019).

Data is the foundation of many digital services, including social media platforms like Instagram, e-commerce websites like Amazon, and streaming services like Netflix. This critical resource supports targeted advertising, personalized content, and optimized user experiences. While the type of data is essential, users' perceptions about what to share and how to engage with these platforms play an equally significant role (Kacsmar et al., 2022). Through numerous decisions, users actively shape their interactions with digital services, driving the personalization and experiences these technologies offer. This dynamic relationship between technology, data, and user agency creates a complex and evolving landscape that defines today's digital experience.

1.1 Research Challenge

As users shape their interactions with digital services, the scope and scale of data collection have expanded. With the proliferation of mobile and ubiquitous technologies, data collection has moved beyond desktops and now permeates daily life through smartphones, wearable devices, and smart home systems. These constantly present and adaptive technologies, often considered “lively technologies,” continuously gather user data, frequently without explicit awareness (Lupton, 2017). This data, initially referred to as “small data” when focused on individuals, grows into “Big Data” as it is aggregated, creating extensive datasets that enable highly personalized experiences yet raise complex privacy and security concerns (Lupton, 2018). Personal data is often treated as currency, serving as a form of payment for “free” digital services or product discounts (Malgieri and Custers, 2018). This data encompasses general usage patterns and specific personal information, revealing insights into users’ habits, preferences, and behaviors, which are of substantial value to service providers and advertisers.

Examples of privacy issues illustrate the challenges data collection poses in today’s digital landscape. Social media platforms like Facebook, X (formerly Twitter), Instagram, and LinkedIn highlight these concerns. Facebook has been scrutinized for incidents such as the Cambridge Analytica scandal (Hinds et al., 2020), while X faces issues with fake accounts (Bhattacharya et al., 2023), and Instagram’s influencer marketing raises questions about user data control (Hudders and Lou, 2023). LinkedIn also presents ethical concerns, with some companies posting misleading job advertisements to gather user information (Bhattacharya et al., 2023).

Privacy issues also extend to smart home devices in private spaces. Studies show that many users are uneasy with the data collected by smart home devices, whether through intended collection by manufacturers or remote attacks. For instance, many users are unwilling to share personal data from smart homes due to risks like identity theft (Naeini et al., 2017). Voice assistants add to these concerns, as users worry about data security and the potential repurposing of their data for targeted advertising (Tabassum et al., 2019; Liao et al., 2019; Cheng and Roedig, 2022). Although sophisticated threats to smart home security exist, many users feel they are unlikely targets, which often diminishes their concern or leads them to overlook privacy issues (Zeng et al., 2017; Tabassum et al., 2019).

This cautious attitude toward data sharing highlights the significant influence of user decisions on privacy outcomes. Users’ choices around data-sharing practices, security measures, and consent mechanisms are important

1.1. RESEARCH CHALLENGE

in shaping privacy risks (Torre et al., 2018). Decisions such as enabling device permissions, connecting multiple smart home devices, or opting into data-sharing features determine the type and extent of personal data collected, often including sensitive information such as location, usage patterns, and biometric details. When convenience (or perhaps a lack of knowledge) takes precedence over security, such as by using weak passwords, bypassing two-factor authentication, or neglecting software updates, users expose their personal data to potential breaches (Fagan and Khan, 2016). Additionally, the common practice of accepting privacy policies without thorough review heightens privacy risks, as many policies permit extensive data collection and third-party sharing (Wigand and Soumillion, 2019). These decisions collectively increase vulnerability to cyberattacks and unauthorized surveillance, as weak entry points in the system can be exploited by malicious actors.

The design and functionality of user interfaces in online service providers further shape privacy-related decisions (Acquisti et al., 2017). Interfaces, such as those found in mobile apps or web platforms, are important in guiding user interactions, decision-making processes, and even emotional responses. However, certain design choices, known as dark patterns, may intentionally manipulate users into making choices that prioritize convenience or data sharing over privacy (Luguri and Strahilevitz, 2021). The dark patterns, such as pre-checked consent boxes, can lead users to expose more of their personal data unknowingly. On the other hand, well-designed interfaces can encourage secure behavior, influencing how users retrieve information, select privacy options, or modify their settings. This interplay between interface design, dark patterns, and user decision-making underscores the need for thoughtful design that promotes informed and secure interactions in data-intensive environments like social media and smart homes.

Analyzing user behavior is another key to privacy protection, as it allows researchers to identify patterns that could expose users to privacy risks and aids in developing more effective privacy-preserving strategies (Chung et al., 2021). User behavior analysis involves understanding how individuals interact with digital systems, what data they share, and under what circumstances they may accidentally disclose sensitive information. By recognizing common behaviors and trends, developers can identify which aspects of a system or process tend to be affected by unexpected or unauthorized data exposure.

Psychological theories, particularly Social Cognitive Theory (SCT), offer a robust framework for understanding user behavior (Bandura, 1986). SCT explains that user behavior is shaped by a dynamic interaction between personal factors, environmental cues, and cognitive processes. This concept of reciprocal determinism suggests that a person’s actions, beliefs, and sur-

1.1. RESEARCH CHALLENGE

roundings continuously influence one another (Bandura, 1986). For instance, when deciding whether to disclose personal information online, users weigh perceived risks and rewards, assess their confidence in managing privacy settings, and take cues from their digital environment, like friends sharing similar information.

The concept of self-efficacy in SCT is particularly relevant; it suggests that users with higher confidence in managing privacy controls are more likely to adopt proactive behaviors, such as adjusting settings to restrict data access or employing security measures (Bandura, 1977). Additionally, observational learning influences users as they mimic privacy practices seen in peers or public figures, which can either strengthen or compromise their privacy based on the examples observed (Merrill Warkentin and Shropshire, 2011). SCT thus can provide insight into how personal beliefs, environmental factors, and learned behaviors shape users' privacy management, guiding the design of user-centered, behaviorally-informed privacy tools.

Complementing SCT, the Fogg Behavior Model (FBM) further explains the conditions under which users act on their confidence to engage in behaviors (Fogg, 2009). According to this model, three factors must align for a behavior to occur: motivation, ability, and a trigger. While high self-efficacy increases users' belief in their ability, motivation and a timely trigger are also essential (Fogg, 2009). For example, a highly confident user may still neglect privacy settings unless motivated by a recent data breach and prompted by an in-app reminder to review their privacy options. Together, these models suggest a combined approach, where integrating insights from the Social Cognitive Theory and the Fogg Behavior Model offers a broader understanding of how confidence, motivation, and contextual cues can drive users toward informed and protective actions in digital environments. This integration leads to the central research question explored in this dissertation:

Central RQ

How can integrating psychological principles, including self-efficacy and the Fogg Behavior Model, empower individuals' comprehension and engagement and promote informed decision-making concerning privacy and security tasks in mobile and ubiquitous applications?

This research question examines user behavior through the lens of Social Cognitive Theory, focusing on how individuals' beliefs about their abilities and the expected outcomes of their actions influence their engagement with privacy and security practices. First, it explores ways to enhance user

1.2. CONTRIBUTIONS

motivation, emphasizing that motivation is closely tied to users' self-efficacy and confidence in their ability to perform a task successfully. For example, users who believe that regularly updating their software will reduce malware risk are more motivated to perform this task consistently. Given that, in the context of SCT, self-efficacy plays an essential role in shaping individuals' perceptions of their capabilities, this part of the research question explores strategies to strengthen self-efficacy that can empower users to manage their digital security more effectively. Subsequently, the research question considers strategies to improve user ability, directly linking skill acquisition to self-efficacy. As users gain skills and knowledge, their self-efficacy is reinforced. For instance, users who become proficient in setting strong passwords and understanding the importance of password security feel more confident in their ability to protect their accounts from unauthorized access. Finally, the role of triggers in influencing users' behavior is examined within SCT's framework. Triggers, such as feelings of vulnerability after a privacy breach or notifications prompting software updates, encourage users to initiate and maintain secure behaviors. For instance, users who receive notifications about unusual login attempts may promptly change passwords, driven by the belief that this action will protect their account security.

This integrated approach addresses users' motivations, abilities, and the influence of triggers, which together shape their intentions and actions in managing digital security effectively. By understanding and applying these factors, Human-Computer Interaction (HCI) design can be tailored to better support users in making informed decisions and adopting secure behaviors across diverse mobile and ubiquitous environments.

1.2 Contributions

This dissertation makes significant contributions to the field of user empowerment in digital privacy and security, drawing from 14 studies that explore motivational drivers, individual abilities, behavioral prompts, regulatory implications, and advanced interface applications. Each study highlights how understanding and enhancing user motivation, ability, and responsiveness can foster informed, proactive behavior in managing privacy and security within mobile and ubiquitous environments.

The initial three studies examine motivational drivers by employing gamification, humor, and narrative themes to engage users with digital security education. These studies demonstrate that integrating engaging elements into educational content can increase user motivation, as predicted by Social Cognitive Theory and the Fogg Behavior Model, enhancing comprehension and willingness to adopt security practices.

1.2. CONTRIBUTIONS

The next group of three studies focuses on assessing and enhancing users' abilities to navigate complex privacy and security settings in mobile and smart home environments. Approaches like infographics, interactive permission visualizations, and a mobile security scanner reveal that simplifying technical information and enhancing transparency can effectively improve users' ability to manage their privacy settings. These studies underscore the importance of equipping users with both knowledge and confidence to navigate privacy and security tasks.

The subsequent three studies investigate the impact of behavioral prompts, such as notifications, simplified privacy policies, and strategically timed reminders, on users' engagement with privacy and security actions. Findings indicate that tailored triggers aligned with user motivation and ability levels can significantly influence behavior, guiding users toward more consistent and informed security management.

Furthermore, the next two studies address the regulatory landscape, focusing on the user experience of privacy policy comprehension and transparency in data-sharing practices. Through analyzing user understanding and the presence of dark patterns in privacy policies, these studies highlight the gap between regulatory requirements and user awareness, advocating for clearer, more user-centered privacy information.

Finally, the dissertation explores the role of Augmented Reality (AR) in enhancing user understanding and management of security practices in smart home environments. By overlaying visual indicators, data flow representations, and security cues onto physical devices, two studies illustrate how AR can transform complex security concepts into accessible, interactive experiences. This approach empowers users with procedural knowledge, enabling more confident and secure interactions within their smart home networks. As the final study, a follow-up investigation using a 2D interface, designed to replicate the features of the AR studies on a standard screen, yielded similar results. The results of the studies demonstrate that AR and 2D interactions can effectively support user comprehension and engagement with security practices. The findings also suggest that, while AR offers unique interactive benefits, 2D interfaces can also serve as practical and accessible alternatives for promoting secure behavior in smart home environments.

Collectively, these contributions advance our understanding of how motivational factors, enhanced abilities, tailored triggers, regulatory clarity, and AR technology can be leveraged to empower users in making informed, privacy-protective decisions. This work offers a holistic framework for designing digital interfaces and educational interventions that meet the evolving privacy and security needs of users in mobile and ubiquitous environments.

1.3 Outline

The second chapter establishes the foundation of this dissertation by providing an overview of ubiquitous and mobile computing and examining privacy and security mechanisms. It emphasizes the necessity for interventions that effectively influence user behavior and explores key theoretical frameworks, including Social Cognitive Theory and the Fogg Behavior Model. The chapter discusses how games can facilitate learning and engagement, focusing on the role of conceptual and procedural knowledge in fostering users' self-efficacy. It concludes by integrating user behavior theories with Human-Computer Interaction principles, presenting the research questions, and proposing a theoretical model to guide the dissertation.

The third chapter investigates the factors that shape security behavior based on insights gathered from nine studies conducted as part of this dissertation. It examines motivational drivers such as gamification, humor, and storytelling as strategies to engage users effectively. Additionally, the chapter evaluates users' abilities, focusing on their skills and ease in managing security tasks. It analyzes behavioral prompts to understand how specific triggers can encourage proactive privacy and security practices.

The fourth chapter focuses on empowering users to take control of their security behaviors, drawing on findings from five studies. It advocates for a user-centered design approach, emphasizing the importance of understanding user needs and fostering empowerment through clear communication and informed decision-making. The chapter further explores how augmented reality and 2D interfaces can enhance users' understanding and enable proactive security management in smart home environments.

The fifth chapter brings together the research findings, revisiting the research questions and aligning the results with theoretical frameworks. It discusses the contributions and practical implications of this work, addresses its limitations, and provides recommendations for future research.

The final chapter highlights the key contributions of this dissertation and underscores its impact on advancing privacy and security practices in mobile and ubiquitous computing. It concludes with reflections on the broader significance of the research for both academic and practical contexts.

2

Background

This chapter provides a foundation for the theories, technologies, and design strategies that empower users to make informed privacy and security decisions in ubiquitous and mobile computing. It begins by introducing the context of ubiquitous and mobile computing, then discusses privacy and security mechanisms essential for protecting user data. Next, the chapter delves into the theoretical foundations of user behavior, focusing on the Social Cognitive Theory (SCT) and the Fogg Behavior Model (FBM) to explain how beliefs, motivations, and environmental factors influence user interactions with privacy settings. Building on these theories, it covers conceptual and procedural knowledge, emphasizing their roles in effective privacy management, and examines the integration between games and learning to enhance engagement in privacy education. Further sections address knowledge transfer and building self-efficacy, illustrating how confidence in privacy management can be developed. The chapter concludes by integrating these concepts with Human-Computer Interaction (HCI) approaches to highlight strategies that make privacy and security information more accessible and actionable, providing a framework for empowering users within digital environments.

2.1 Ubiquitous and Mobile Computing

Ubiquitous computing is a concept that envisions the widespread use of computing across all devices, locations, and configurations. Mark Weiser (1991) initially articulated the foundational idea behind the concept of ubiquitous computing. His vision of ubiquitous computing aims to create a world where technology becomes so seamlessly integrated into our environment that it effectively “disappears” from our conscious attention (Weiser, 1991). This invisibility is not only about physical form but also about minimizing the cognitive load of technology, enabling people to interact with their surroundings naturally (Poslad, 2011). Ubiquitous computing’s core objective is to embed computing into everyday objects and spaces, allowing individuals to engage with technology as part of their environment rather than through dedicated devices (Weiser, 1991). This concept, termed “calm technology,” promotes interactions that allow people to remain focused on their tasks without interruption from technology itself (Poslad, 2011).

Fundamental principles support this vision, including *invisibility*, which ensures that technology fades into the background, enhancing usability without becoming a focal point. *Context-awareness* is another critical aspect, allowing systems to adapt their behavior based on the user’s environment, activities, and needs, thus providing relevant, timely assistance. *Distributed computation* furthers this goal by connecting multiple devices seamlessly, enabling them to work collaboratively within a space without the user’s conscious coordination. Lastly, *human-centric design* ensures that technology aligns with human activities and natural interactions while respecting *privacy* and *security*, which are essential in a pervasive environment with continuous data collection (Weiser, 1991; Poslad, 2011).

Whereas ubiquitous computing emphasizes the seamless and invisible integration of technology into everyday environments, *mobile computing* focuses on the use of lightweight, wireless-enabled devices, such as smartphones and laptops, to provide “information at your fingertips anywhere, anytime” (Satyanarayanan, 2011). This capability has become a reality through innovations in wireless technology, energy-efficient hardware, and adaptive software. Mobile computing emphasizes portability and seamless connectivity, allowing devices to maintain interactivity and continuous data exchange even while users move across various environments (Satyanarayanan, 2011). Increasingly, these mobile devices act as rich sensors, capturing complex, contextual data, such as images and location-specific information, enabling real-time responses and personalized interactions. By supporting data-rich applications, mobile computing facilitates diverse functions like location-aware services, real-time

image searches, and crowd-sourced data gathering. This framework empowers users to stay connected and informed, leveraging transient infrastructure like public screens when needed, thus enhancing the flexibility and resilience of mobile computing in dynamic settings (Qi and Gani, 2012).

Although ubiquitous computing technologies offer innovative ways to embed computing into everyday objects, they also raise significant privacy and security challenges. These technologies facilitate extensive data exchange across various environments, raising concerns about safeguarding privacy, ensuring robust security, and upholding ethical data practices (Sheng et al., 2008). Privacy issues in ubiquitous computing arise from the proliferation of advanced technologies, such as interconnected devices and location-aware systems, which significantly increase access to personal data (Langheinrich, 2018). For example, when users enter a shopping mall, personalized notifications about discounts and promotions can be sent to their devices, tailored to their interests and shopping patterns. In order to deliver such personalized experiences, ubiquitous systems often require tracking and compiling users' activities, leveraging both previously collected data and real-time information. Balancing these privacy challenges with the benefits of integrated technology is essential to protect individual privacy while enhancing user experience.

In mobile computing, similar privacy challenges exist due to the general use of portable devices that rely on real-time data for personalized services. Mobile computing applications depend on identifying user characteristics, preferences, and location to customize interactions and enable “anytime, anywhere” connectivity (Mollah et al., 2017). This often involves extensively tracking users' movements and habits to create personalized experiences, such as location-based recommendations or notifications when users are near a favorite store. The reliance on portable devices for storing and sharing personal information increases the risk of unauthorized access and misuse. Addressing these issues is essential to ensure that mobile computing provides convenient, customized services while upholding privacy and data security (Kulkarni and Khanai, 2015).

2.2 Privacy and Security Mechanisms

Gaining insight into the perspectives of essential components in data-driven services within ubiquitous and mobile computing, particularly regarding privacy and security mechanisms, necessitates thoroughly exploring the definitions associated with privacy and security terminology. This imperative is rooted in the natural interconnection between privacy and security mechanisms. *Privacy* can be understood in several ways. It is described as a fluid concept shaped by historical, social, and technological developments, with

2.2. PRIVACY AND SECURITY MECHANISMS

privacy’s meaning varying across eras and cultures (Solove, 2002). While privacy has ancient roots, it only gained legal recognition in the 19th century, when Warren and Brandeis defined privacy as “the right to be let alone,” laying the foundation for modern privacy laws (Warren and Brandeis, 1989). Privacy is closely linked to values like dignity, autonomy, and independence. As technology advances, new legal protections become essential to guard privacy against increasing intrusions. Given its dynamic nature, some scholars advocate for a flexible approach to privacy protection, one that adapts to evolving societal and technological contexts (Bloustein, 1964; Westin, 1968).

Neil Richards (2022) offers that “privacy is the degree to which human information is neither **known** nor **used**”. This definition highlights that privacy fundamentally pertains to information concerning humans. Personal information can be characterized as data or knowledge susceptible to privacy considerations, particularly concerning its acquisition, dissemination, or utilization by other persons or entities (Voigt and Von dem Bussche, 2017). While legal definitions may employ technical jargon, they recommend using “human information” to underscore the association with individuals. It explores the impact of technology on human behavior, encompassing aspects like targeted advertising and manipulation through social media.

According to Neil Richards, the term “known” pertains to the gathering or acquisition of information about an individual, while “used” relates to subsequent processes, including detection, organization, analysis, storage, transmission, and even disclosure. As a result, he emphasizes that addressing concerns regarding human information necessitates contemplating what is gathered or acquired and how that information is managed, utilized, and protected (Richards, 2022). Furthermore, the concept of privacy as a matter of degree underscores that privacy is not merely a binary state of being either “private” or “public.” Instead, it exists along a continuum, with various levels of information sharing (Smith et al., 2011). Privacy and ubiquitous computing are not inherently incompatible but require thoughtful design and adherence to privacy principles. Users should have the ability to exercise control over their data, and systems should be designed to respect their privacy preferences. Striking a balance between the benefits of ubiquitous computing and user privacy is essential (Politou et al., 2022).

The classic definition of *security* equates it with the Confidentiality, Integrity, and Availability (CIA) triad. Confidentiality involves protecting sensitive information from unauthorized access. Integrity, conversely, guarantees the originality of data and detects any unauthorized alterations or tampering. Moreover, availability represents the proportion of time during which a system must remain operational and accessible to its authorized

2.2. PRIVACY AND SECURITY MECHANISMS

users (Samonas and Coss, 2014). Confidentiality, integrity, and availability mark the initial stages in the story of information security within a ubiquitous system (Colella and Colombini, 2012). For instance, a crucial question emerges within ubiquitous computing as a user logs into a device or engages with various interconnected services: How does the system validate the user’s true identity and distinguish them from potential hackers or unauthorized individuals? Furthermore, when users access their specific online banking account in this ubiquitous environment, how can the bank be sure that it is indeed the legitimate account holder and not a hacker attempting to gain unauthorized entry? In this context, security mechanisms become even more critical than traditional computing environments. These mechanisms are essential for protecting user identities and data integrity and ensuring the availability of services, ultimately ensuring a secure and trustworthy experience in this interconnected and data-rich environment (Nissenbaum, 2004). Despite the surface-level similarities of these authentication challenges, a deeper exploration unveils the nuanced and distinct nature of each problem within the context of ubiquitous computing. From this standpoint, developers of ubiquitous systems and services must recognize that the complexities and functionalities of technical solutions and mechanisms must be incorporated through user involvement.

2.2.1 Users’ Perspectives

The integration of ubiquitous and mobile computing technologies into workplaces and homes emphasizes the essential role of user interaction within these systems, placing users at the center of usability and adaptation concerns. Human-Computer Interaction is a multidisciplinary field dedicated to designing, evaluating, and implementing interactive computing systems for human use (Hewett et al., 1992). By focusing on user needs, HCI draws from psychology, sociology, and design to create intuitive and adaptable systems. In ubiquitous computing, HCI addresses challenges unique to interconnected environments, desiring to promote seamless user experiences across various devices and contexts. The goal of HCI in this field is to enable users to interact with technology in ways that are as natural and unobtrusive as possible, often using implicit, context-aware, and multimodal interfaces. This approach minimizes the need for direct user input, allowing technology to adapt to users’ environments automatically (Bashir et al., 2014).

Usability is central to HCI and is defined as the effectiveness, efficiency, and satisfaction that users experience within a specified context (ISO, 2018). These attributes are required for creating intuitive and supportive user experiences across interactive systems. Usability is also a fundamental

2.2. PRIVACY AND SECURITY MECHANISMS

component of broader software quality, as outlined by ISO/IEC 25010:2011, which incorporates usability, security, maintainability, and compatibility as essential quality characteristics in software systems (ISO, 2011). Additionally, ISO 9241-210:2019 emphasizes a human-centered design approach, advocating for continuous user involvement and iterative testing to meet user needs effectively (ISO, 2019). Together, these standards guide HCI in developing systems that not only meet technical requirements but also support a user-centered experience, enhancing trust, safety, and overall satisfaction.

However, the nature of ubiquitous services often introduces new complexities for users. Privacy and security mechanisms may require additional steps, such as verification during online banking. While users expect such security measures for financial data, their approach to privacy can vary in other contexts, such as smart homes. For example, users might resist sharing their Wi-Fi password with guests to avoid security risks, which could be misinterpreted socially as distrust. Additionally, turning off location tracking might prevent a thermostat from automatically adjusting when a user leaves or enters the house, reducing the ease and energy savings that smart technology typically provides. This behavior reflects a need for adaptable privacy and security features that align with user preferences and social contexts (Lederer et al., 2003).

2.2.2 Developers' Perspectives

Developers typically address various software quality factors, such as usability, flexibility, user satisfaction, maintainability, and privacy (Ferre, 2003). These factors are often interconnected; for example, flexibility can improve maintainability, while reliability can enhance user satisfaction (Folmer and Bosch, 2004). However, certain quality attributes can conflict with each other. This is particularly evident in the trade-offs between usability, privacy, and security, where enhancing one aspect can inadvertently weaken another (Naqvi and Seffah, 2019). For instance, in smart home applications (apps), improving usability by allowing easier access to devices or settings might compromise privacy or security if not carefully designed.

Balancing these factors requires a user-centered design approach that gives equal priority to usability and security without compromising either. Two-factor authentication serves as a good example of this challenge. The complexity of encryption and its associated terminology often conflicts with the language and understanding familiar to everyday users, creating barriers to effective adoption. As a result, misconceptions about authentication processes can lead to usability issues. While the basic concept of two-factor authentication, which combines something the user knows, such as a password,

2.2. PRIVACY AND SECURITY MECHANISMS

with something the user has, such as a mobile device, is relatively straightforward, users often struggle to grasp the underlying security principles and the necessity for employing two distinct authentication factors (Dutson et al., 2019). This gap between users' understanding and the technical requirements of privacy and security mechanisms highlights the importance of user-focused solutions to bridge this divide and foster informed, secure user behavior.

Furthermore, privacy and security mechanisms should be crafted to complement the core product seamlessly, for instance, in the case of a corporate environment where employees are required to adhere to a complex and frequently changing password policy. While these policies aim to enhance security, they can result in employees spending excessive time managing passwords instead of focusing on their work tasks (Gerlitz et al., 2021). This scenario highlights the conflict between stringent security measures, which emphasize complex passwords, and employees' production tasks, which prioritize productivity and efficiency. Achieving a balance between these priorities requires collaboration between security experts and workflow managers to design policies that enhance security without undermining productivity. The challenge lies in aligning security requirements with the demands of production tasks and ensuring that security does not hinder users' productivity (Mujeye and Levy, 2013). In order to tackle these issues, developers should also communicate the importance of privacy and security mechanisms to users, ensuring that guidelines are easy to understand and follow. This approach can encourage users to actively participate in maintaining privacy and security standards. Moreover, adherence to legal privacy and security procedures is essential, as violations can result in serious consequences for both users and manufacturers (Carre et al., 2018).

2.2.3 Legislators' Perspectives

Specific regulations have been established to govern data collection and processing. They outline practical responsibilities for data-collecting entities, often referred to as data controllers, to return control of personal data to the individuals they pertain to, known as data subjects. These responsibilities include informing data subjects about the purpose of data usage, obtaining their consent, and providing accessible means for users to access, rectify, and delete their personal information (Tikkinen-Piri et al., 2018).

The European Union (EU) General Data Protection Regulation (GDPR) stands as a prominent model of a regulation that introduced a comprehensive set of legal requirements, effective as of May 25, 2018, governing the processing of personal data for any business operating within or in part with the EU or managing data of EU citizens (Voigt and Von dem Bussche, 2017). Art. 4 No.

2.2. PRIVACY AND SECURITY MECHANISMS

1 GDPR defines personal data as any information related to an identified or identifiable natural person. This legislation aims to establish the utmost transparency and control, striking a balance between those from whom data is collected and those receiving the data.

The advent of GDPR underscores the significance of providing data controllers with necessary information regarding data protection, strengthening the criteria for obtaining legally valid consent from data subjects, and expanding their rights, particularly regarding access to information and disclosure. Following the requirements outlined in Articles 12, 13, 14, and 21 of the GDPR, data controllers are obligated to inform users about the processing of personal data relevant to them and their associated data protection rights. Under GDPR, data subjects are entitled to a spectrum of rights, including access to their data (Art. 15), the rectification of inaccuracies (Art. 16), the right to erasure (Art. 17), the ability to restrict data processing (Art. 18), notification rights (Art. 19), and data portability (Art. 20).

Furthermore, data subjects have the option to lodge complaints with a data protection supervisory authority if they believe their personal data is being processed unlawfully (Art. 77) without prejudice to other legal remedies. Should data processing rely on consent, individuals can withdraw their consent for future data usage at any time (Art. 7), though this does not affect prior processing. It is important to note that specific data may need to be retained for legal compliance, regardless of consent status (Voigt and Von dem Bussche, 2017).

Despite the intended purpose of these regulations to protect users' personal data and their interests, the interfaces and implementations of these sensitive mechanisms within ubiquitous systems often lack user-friendliness (Jensen and Potts, 2004; Luger et al., 2013; Kitkowska et al., 2020b), and most users do not thoroughly read privacy policies. The primary reasons for this low engagement are that the explanations remain excessively long and challenging to comprehend (Wigand and Soumilion, 2019). While there have been positive developments in data protection rights and information inclusion before and after GDPR, this has not necessarily translated into user-friendly policies (Linden et al., 2018). Policies have grown significantly in length, encompassing more syllables, words, and sentences. Since individuals typically use smartphones to interact with ubiquitous services, reading such lengthy texts on small screens may be challenging and inefficient (Raptis et al., 2013). This unaware consenting, often induced by complex and lengthy regulations and the potential use of dark patterns, can contribute to inappropriate behavior and increase the risk of unintentional data disclosure (Clark et al., 2015; Kang et al., 2015; Tabassum et al., 2019).

2.3 Theoretical Foundations of User Behavior

2.3.1 Social Cognitive Theory

Albert Bandura initially introduced the concept of Social Learning Theory (SLT) in 1977 (Bandura and Walters, 1977). He later evolved it into Social Cognitive Theory by 1986. Bandura's pioneering and influential work expresses that learning occurs within a social context and involves a dynamic and reciprocal interaction among *personal factors*, *environmental influences*, and *behavior* (Bandura, 1986). The Social Learning Theory, as the forerunner to the Social Cognitive Theory, suggested that people learn through observation, imitation, and modeling, influenced by psychological factors such as attention, retention (memory), and motivation (Muro and Jeffrey, 2008; Nabavi, 2012).

Bandura's theories are pivotal in understanding that learning is not solely the product of direct reinforcement or conditioning, as proposed by behaviorist theories, but also occurs by observing the actions of others (Fryling et al., 2011). For instance, homeowners may learn to improve their home security by observing a neighbor's use of smart security systems. They notice that the neighbor's home, equipped with surveillance cameras and motion sensors, has never been burglarized, unlike other homes in the area. This observation and the neighbor's positive reinforcement about the system's efficacy motivate the homeowner to adopt similar security measures. Thus, learning about the benefits and operations of smart home security is influenced by cognitive characteristics and the observed positive outcomes of the neighbor's behavior. The Social Cognitive Theory expanded on this by emphasizing the role of cognitive processes in learning from interactions with others and the environment. This integration of behavioral, cognitive, and environmental dimensions made Bandura's theories a significant bridge between behaviorist and cognitive learning theories, explaining a wide array of human behaviors that could not be accounted for by traditional learning theories alone (Muro and Jeffrey, 2008).

The Social Cognitive Theory identifies several key elements that impact behavior. Foremost among these is perceived self-efficacy, which relates to an individual's confidence in their ability to execute a particular action to achieve a targeted result. Another central component of the SCT is outcome expectancy/expectations, which refer to an individual's beliefs about the potential results of their behaviors. Additionally, the SCT encompasses objectives as well as recognized barriers and chances. These elements are depicted in Figure 2.1, demonstrating their dynamic interaction during behavioral modification.

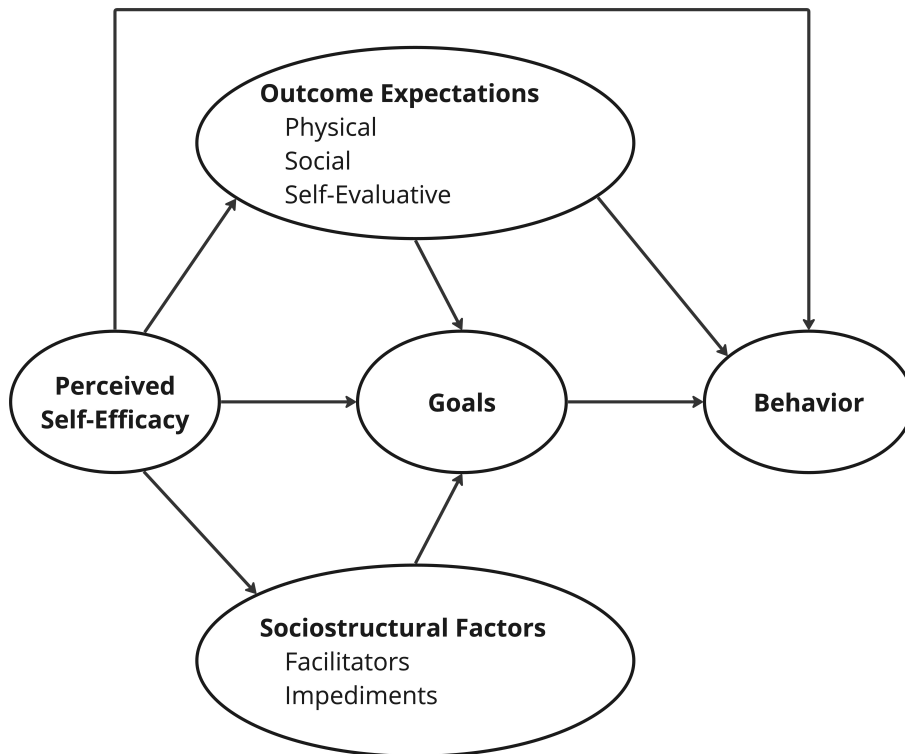


Figure 2.1: Diagram of the Social Cognitive Theory (Bandura, 2012). This illustration captures the pathways of influence where perceived self-efficacy impacts shaping goals, outcome expectations, and the individual’s view of sociostructural facilitators and impediments.

Self-Efficacy

Self-efficacy is a psychological structure that develops and is revised by interpreting information from four primary sources: *mastery experiences*, *vicarious experiences*, *social persuasion*, and *physiological and emotional states* (Bandura, 1977). The most substantial influence typically arises from mastery experiences, where personal success boosts self-efficacy, and repeated failures may diminish it (Bandura, 1977). However, the development of self-efficacy is nuanced; not every easy success necessarily heightens it, nor do all failures lead to a lower sense of efficacy. The effects of failures on self-efficacy are influenced by their timing and the overall pattern of experiences (Bandura, 1977). Similarly, facing difficulties provides valuable opportunities to learn from failures, refine skills, and gain better control over tasks. Turning failure into success by honing one’s abilities further strengthens self-efficacy (Bandura et al., 1999).

2.3. THEORETICAL FOUNDATIONS OF USER BEHAVIOR

Vicarious experience also plays an essential role in developing an individual's self-efficacy, especially when they lack personal experience (Bandura, 1977). This form of learning involves observing others performing similar tasks and making comparisons with one's own perceived capabilities. Individuals often use these observations as benchmarks, assessing their abilities based on the successes or failures of others who are perceived as models (Bandura, 1982). The similarity between the model and the observer significantly influences the effectiveness of this process. For example, the more an observed model shares characteristics with the observer, such as adeptness, perseverance, age, or experience level, the more profound the impact on the observer's self-efficacy (Bandura, 1977).

Social persuasion is the third factor influencing perceived self-efficacy, which involves verbal support and encouragement from essential figures like parents, peers, and teachers (Joët et al., 2011). It is commonly employed to influence human behavior due to its simplicity and accessibility. Social persuasion involves guiding people to believe they can successfully manage previously overwhelmed situations. However, the efficacy expectations generated through such suggestions tend to be less robust than those developed from personal achievements, mainly due to the lack of a solid experiential foundation in social persuasion (Bandura, 1977). When individuals face complex challenges and have a past filled with unsuccessful attempts at handling them, the confidence instilled through suggestion can be rapidly diminished by experiences that counter these induced expectations. Although social persuasion alone has a limited capacity to establish enduring personal efficacy, it can significantly enhance effort and success when combined with practical performance support (Bandura, 1977). Nevertheless, raising competence expectations solely through persuasion, without creating conducive conditions for effective performance, can lead to failures that discredit the persuasion and weaken perceived self-efficacy (Bandura, 1982).

Physiological and emotional states, including emotional arousal, represent the final determinant of perceived self-efficacy. These states, characterized by feelings like anxiety or fatigue encountered during tasks, significantly contribute to shaping an individual's self-efficacy (Bandura, 1977). High emotional arousal, often interpreted in stressful situations as vulnerability, can impair performance. This influence on self-efficacy varies depending on environmental factors and the personal meaning of these emotional states. Individuals typically assess their anxiety and vulnerability to stress based on their physiological state. In scenarios where high arousal is present, it usually hinders performance, leading to expectations of more favorable outcomes when the individual is calm rather than tense (Bandura, 1977).

Outcome Expectations

Perceived self-efficacy significantly influences the perceived potential rewards or consequences of outcome expectations (Bandura, 1977). Essentially, the outcomes that individuals anticipate are deeply rooted in their beliefs about their ability to perform successfully in various situations. They are distinguished from self-efficacy because self-efficacy is the perceived ability to do a behavior. In contrast, outcome expectancies are judgments about the probability of outcomes that flow from behavior (Bandura, 1977, 1986; Bandura et al., 1999). Individuals with a strong sense of self-efficacy expect positive results from their efforts, believing that competent performance will bring favorable outcomes. Conversely, those with low self-efficacy may predict unfavorable results, anticipating their poor performance will lead to negative consequences (Bandura, 1977).

The expected outcomes influenced by an individual's sense of self-efficacy can take various forms, impacting both their internal state and external circumstances (Bandura, 2004). Physical outcome expectations can include practical consequences such as the success or failure of a given project, the quality of interpersonal relationships, or career advancement (Conner and Norman, 2015). Socially, these outcomes may be reflected in recognition or disapproval from peers and community, shaping one's social standing and networks (Conner and Norman, 2015). Internally, self-evaluative outcome expectations manifest through emotional responses like a sense of fulfillment or disappointment, influencing an individual's overall well-being and self-esteem (Conner and Norman, 2015). It is essential to clarify that self-efficacy beliefs are based on individuals' perceptions of their capabilities rather than actual abilities to complete a task (Bandura, 1977).

Goals

In the Social Cognitive Theory, goals are critical in influencing behavior and interacting with other theory elements (Bandura et al., 1999). The level of challenge associated with a goal affects the effort and satisfaction derived from pursuing it. Challenging goals, when accepted and committed to, typically lead to more significant effort and better performance. However, overly complicated or unrealistic goals can be demotivating if they undermine self-efficacy (Bandura et al., 1999). Goals can be long-term (distal) or short-term and immediate (proximal) (Bandura et al., 1999). For instance, a long-term goal in a smart security system might be to achieve a fully secure and automated home environment. In contrast, short-term goals could involve installing specific security devices or setting up automatic alerts for different scenarios. The proximity of goals is also essential (Bandura et al., 1999).

2.3. THEORETICAL FOUNDATIONS OF USER BEHAVIOR

Short-term goals help focus immediate efforts, such as activating nightly alarms or regularly updating security protocols. Conversely, long-term goals, like maintaining a consistently secure home over several years, provide an overarching aim.

Goals in the Social Cognitive Theory frequently exhibit a hierarchical structure, where the attainment of short-term objectives plays a pivotal role in achieving long-term goals (Bandura et al., 1999). In our smart security system example, completing immediate tasks (like setting up a new security feature) contributes to the broader goal of comprehensive home security. However, simply having a goal is insufficient for behavioral change (Bandura et al., 1999). Self-regulatory skills are required, similar to those needed to effectively manage and adjust a smart security system, which includes monitoring system performance and tracking and reviewing security logs, setting specific security objectives, and rewarding oneself for achieving these objectives. The interaction between individuals' belief in their abilities (efficacy beliefs) and goal setting is crucial. These beliefs guide setting realistic goals and commitment to them (Bandura et al., 1999). Achieving challenging goals, like successfully troubleshooting and fixing a complex issue with the security system, can enhance these efficacy beliefs, boosting one's confidence in managing home security.

Sociostructural Factors

The process of goal setting within the framework of the Social Cognitive Theory is influenced by the presence of facilitators and the challenge of overcoming impediments (Bandura et al., 1999; Bandura, 2004). Social factors like online community trends and technological advancements significantly influence behavior and goal setting, particularly in the digital era (Tsai and Bagozzi, 2014). This influence is mainly noticeable in how users adapt to evolving technologies and navigate complex interfaces (Miraz et al., 2021). Facilitators play a crucial role in addressing these challenges in easing the transition. Intuitive software design is one such facilitator, making technology more accessible through user-friendly interfaces and simplified navigation (Issa and Isaias, 2022). Another facilitator is accessible tech education, including online tutorials and mobile learning, which empowers users from diverse backgrounds to engage with technology confidently (Granić and Marangunić, 2019). Moreover, policies aimed at reducing the digital divide, such as government initiatives for affordable internet access and public computer training programs, are also required for creating an inclusive digital environment (West, 2015; Rodriguez-Hevía et al., 2020).

However, challenges exist through barriers like rapid technological changes

2.3. THEORETICAL FOUNDATIONS OF USER BEHAVIOR

and systemic issues, including unequal access to technology and lack of digital literacy (Van Dijk, 2017). These barriers can significantly hinder user engagement and counteract the benefits brought by facilitators (Prior et al., 2016). Therefore, while advances in Adaptive User Interfaces (AUIs) and Intelligent User Interfaces (IUIs) aim to enhance user-machine interactivity, the importance of designing universally usable interfaces becomes paramount (Miraz et al., 2021). Addressing these challenges necessitates a multidisciplinary approach, integrating fields like understanding human behavior, individual modeling, and human-computer interaction to respond effectively to the diverse needs of users. As technology evolves, the interplay between facilitators and barriers will shape how effectively users interact with and benefit from digital tools in an increasingly connected world (Lavie and Meyer, 2010; Miraz et al., 2021).

2.3.2 Fogg Behavior Model

Persuasive technology is a form of design that aims to influence user behavior in a specific way (Fogg, 2002). For instance, a fitness app that sends daily exercise reminders and tracks progress is a persuasive technology designed to motivate users to maintain a regular workout routine. However, applying persuasive technology is not a one-size-fits-all solution that guarantees behavioral change. Instead, it requires a customized approach that resonates with the individual’s unique psychological state and situational context (Fogg, 2002, 2009). The Fogg Behavior Model is a comprehensive framework for understanding behavior change and designing persuasive technology in many domains, such as health, education, and sales (Fogg, 2009). It emphasizes three key factors: *motivation*, *ability*, and *triggers*. These factors must converge for a target behavior to occur. The model is visualized with motivation on the vertical axis and ability on the horizontal axis, highlighting that high motivation and ability are typically required for behavior occurrence (see Figure 2.2). This model balances the interplay between motivation and ability, showcasing a blend of simplicity and effectiveness. These qualities make it an ideal and beneficial tool for understanding and influencing information security behavior (Kießling et al., 2021).

In the Fogg Behavior Model, motivation is a nuanced mix of interrelated elements. It encapsulates the immediate emotional responses of pleasure and pain, the anticipatory forces of hope and fear, and the profound social acceptance and rejection influences (Fogg, 2009). Each element plays an essential role in the calculus of human behavior. For instance, pleasure can instantly incentivize a behavior, while pain may deter it. Hope can propel a person towards a goal-oriented action, while fear may prevent them from

2.3. THEORETICAL FOUNDATIONS OF USER BEHAVIOR

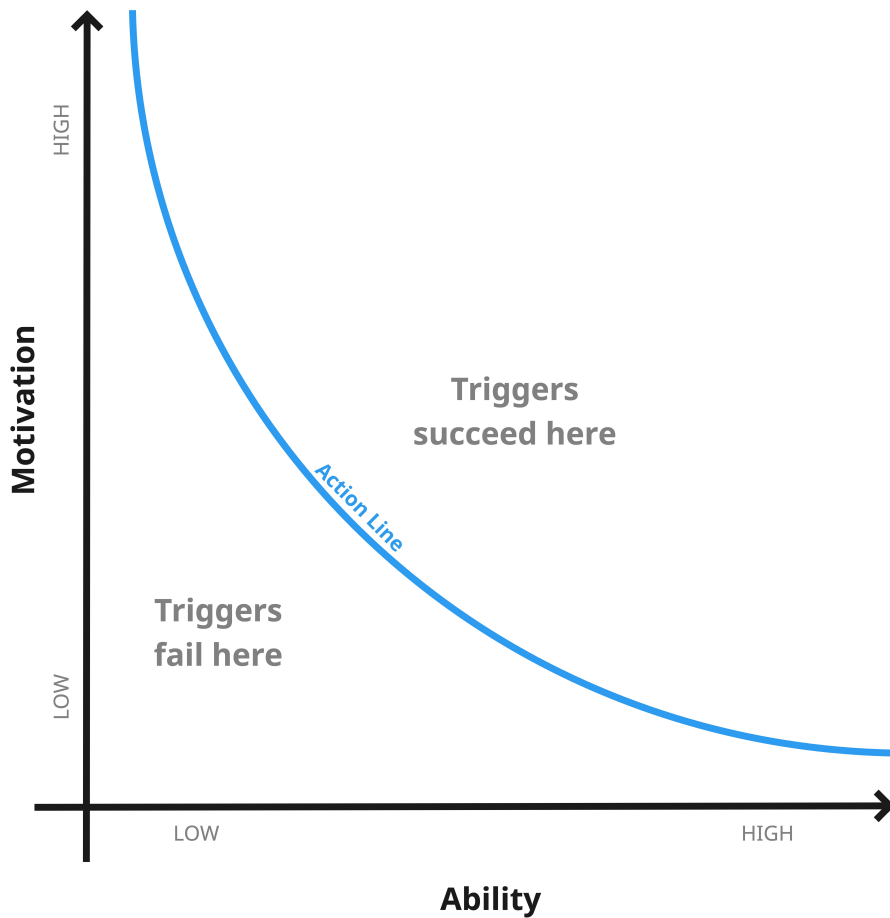


Figure 2.2: Diagram of the Fogg Behavior Model (Fogg, 2009). The Fogg Behavior Model represents the relationship between motivation, ability, and behavior, with the Action Line depicting the threshold at which triggers lead to behavior change.

engaging in potentially harmful behaviors. Social dynamics add another layer, with the desire for acceptance and fear of rejection guiding much of our social conduct. Similarly, the model's take on ability transcends mere physical capacity. It comprises the tangible resources of time and money that can directly enable or impede action (Fogg, 2009). The physical effort ties into the bodily energy required for an activity, while mental effort (brain cycles) relates to the cognitive engagement demanded. Beyond these, social deviance and routine consider the social norms and established patterns that can either ease or complicate the path to action (Fogg, 2009). In practical terms, the FBM suggests that a person's ability to act is contingent upon the simplicity of the action (Fogg, 2009). Simplicity here is multilayered,

2.3. THEORETICAL FOUNDATIONS OF USER BEHAVIOR

involving the time taken to perform an action, the financial cost, the physical and mental exertion required, and whether the action aligns with social norms and established routines. As a result, what may be a straightforward task for one individual could be complex and taxing for another, underlining the importance of context and individual differences in the FBM’s approach to ability (Fogg, 2009).

Triggers constitute the third essential factor in the FBM and are categorized into sparks, facilitators, and signals (Fogg, 2009). Sparks are used when a person lacks motivation for a target behavior. They are designed alongside motivational elements and can take various forms, like text or videos that inspire hope or highlight fear. Facilitators are suitable for users with high motivation but low ability, aiming to make the behavior easier to perform, such as software updates that imply ease with one-click solutions. Signals, the third type, are effective when people have both the ability and the motivation to perform a target behavior and act mainly as reminders. An example is a traffic light signaling when to drive or stop (Fogg, 2009).

In conclusion, technologies designed for behavior change, underpinned by models such as the Fogg Behavior Model, are key influencers of behavior in the digital era. Their success hinges on a deep understanding and application of the fundamental principles of human behavior, like motivation, ability, and triggers. Nevertheless, it is imperative to thoughtfully address the ethical considerations associated with these technologies to ensure their responsible use and to prioritize the interest of users.

2.3.3 Integration of SCT and FBM

Since the 1980s, the field of HCI has incorporated a variety of theories from different disciplines to analyze and predict user performance with computer interfaces and systems. Most of these imported theories are rooted in cognitive, social, and organizational domains (Rogers, 2022). Theories in behavioral studies can be categorized based on their level of generality or specificity (Hekler et al., 2013). *Conceptual frameworks* are one such category, focusing on specific facets of a problem to provide in-depth insights for understanding and analyzing a particular domain. An exemplary conceptual framework is self-efficacy theory, which offers detailed perspectives on how an individual’s belief in their capabilities impacts their behavior (Consolvo et al., 2017). This theory provides targeted strategies and practical applications for behavior research and interventions.

In contrast, *Meta-Models* serve as broad, overarching structures that offer a generalized understanding of behavior. These models are less about detailed specifics and more about setting the stage for various behavioral inquiries.

2.3. THEORETICAL FOUNDATIONS OF USER BEHAVIOR

They deliver a foundational perspective for addressing a problem but often require further details through conceptual frameworks and methodologies like experience sampling to fully flesh out their applications. The Fogg Behavior Model exemplifies a meta-model (Consolvo et al., 2017). It presents a comprehensive organizational structure that facilitates understanding behaviors across various contexts. The FBM's broad applicability makes it a valuable tool in behavior analysis, although it necessitates additional specific insights for thorough application and understanding. The integrations of theories in HCI highlight the significance of theoretical concepts in the field. They offer essential psychological and behavioral insights, which are crucial to creating technological designs that are both user-centered and highly effective (Rogers, 2022). This work outlines a strategic approach to select theories for behavioral research in the privacy and security domain within ubiquitous applications, beginning with integrating meta-models and progressing to applying conceptual frameworks (Consolvo et al., 2017).

The initial phase of this approach is grounded in integrating two prominent meta-models, which were introduced, namely the Fogg Behavior Model and Social Cognitive Theory. The FBM is instrumental in examining how factors like motivation, ability, and triggers influence behaviors, such as a person's decision to use a security feature on their smartphone. Meanwhile, SCT delves into the interplay of personal beliefs, behavioral patterns, and environmental influences. As the work advances, attention shifts to more specific frameworks, notably self-efficacy theory. This shift is motivated by the imperative to explore the nuances of how individuals perceive and navigate privacy and security challenges in behavior change technologies environments. For example, the initial phase might investigate how individuals are motivated to use privacy features (drawing from FBM) and why these motivations influence their behavior (using insights from SCT). This exploration could be further enriched by HCI perspectives, examining how interface design and usability factors influence users' motivation to engage with privacy and security settings effectively.

Subsequently, the work transitions to self-efficacy theory within an HCI context, aiming to explore whether individuals feel confident and capable of independently managing these privacy and security settings. This structured approach evolves from broad meta-models to more targeted conceptual frameworks, ensuring a thorough exploration of motivational factors and self-perceived abilities in interaction with technology. Overall, the benefits of this approach lie in consistently placing the user at the center of the theoretical selection process, ensuring that the chosen theory remains closely aligned with user experiences and requirements (Consolvo et al., 2017).

2.4 Conceptual and Procedural Knowledge

2.4.1 Defining Key Knowledge Types

The previous section provided an understanding of user behavior by integrating relevant theories, highlighting the link between self-efficacy and a person's belief in their ability to learn and successfully perform behaviors over time. Within this framework, the influence of prior knowledge and abilities on self-efficacy are critical factors (Van Dinther et al., 2011). Before delving into how knowledge and abilities influence self-efficacy, it is essential to understand the different types of knowledge involved.

People acquire two fundamental types of knowledge, including conceptual understanding and procedural skills, which are essential for learning and problem-solving (McCormick, 1997). Conceptual knowledge encompasses a person's inherent or stated understanding of the basic principles and relationships among various pieces of knowledge in a specific subject area (Rittle-Johnson et al., 2001). This knowledge is adaptable and not confined to particular problem scenarios, allowing it to be applied across various contexts (Rittle-Johnson et al., 2001). It provides a theoretical framework that helps individuals make sense of complex concepts and phenomena, thereby enhancing their understanding of a subject at a fundamental level (McCormick, 1997). An example of conceptual knowledge in the context of mobile permissions would be understanding why certain apps request access to specific features like location, camera, or contacts. It includes grasping the broader implications of granting these permissions, such as how they can affect personal privacy and data security and the general principles of data management within mobile ecosystems. This kind of knowledge helps users comprehend the potential risks and benefits of permissions, regardless of the specific app or device used.

On the other hand, procedural knowledge pertains to the capability of executing sequences of steps to solve problems (Rittle-Johnson et al., 2001). It is closely tied to the mastery of skills and is often revealed through changes in performance based on prior experience rather than explicit recall (Willingham et al., 1989). Procedural knowledge is usually specific to particular issues and is not as broadly applicable as conceptual knowledge. It involves the practical application of skills and techniques to accomplish tasks and tackle challenges (McCormick, 1997). This knowledge is particularly essential in disciplines and professions where complex and potentially hazardous procedures are common, such as in health, education, science, or technology (McCormick, 1997; Hiebert, 2013; Torrente et al., 2014).

Based on the earlier example in the context of mobile permissions, where

2.4. CONCEPTUAL AND PROCEDURAL KNOWLEDGE

conceptual knowledge involves understanding the privacy implications of app permissions, procedural knowledge is demonstrated by actively managing these permissions on a mobile device. It includes steps such as navigating the smartphone's settings, identifying which apps have been granted specific permissions, and making informed decisions to adjust these settings as needed.

The interplay between these two types of knowledge is required for effective learning and application. Conceptual knowledge lays the groundwork for understanding the “why” behind various phenomena, while procedural knowledge provides the “how-to” for practical application (McCormick, 1997). Together, they enable a comprehensive understanding and competence in a subject, allowing individuals to grasp theoretical concepts and apply them effectively in real-world situations. This integration is especially crucial in fields like technology education, where a balance between theoretical understanding and practical skills is essential for navigating the complexities of the discipline (McCormick, 1997).

2.4.2 Influence on Self-Efficacy and Behavior

The concept of self-efficacy, both in computer use and broader educational settings, is significantly influenced by practical experience and specialized training (Cassidy and Eachus, 2002; Van Dinther et al., 2011). Research has shown that factors such as hands-on computer experience, familiarity with software packages, and targeted computer training are closely correlated with higher levels of self-efficacy (Cassidy and Eachus, 2002). These are aligned with educational research, which emphasizes that enactive mastery experiences, or direct engagement in relevant tasks, are mighty in fostering a strong sense of efficacy. Furthermore, the effectiveness of interventions based on theoretical models like Social Cognitive Theory suggests that structured and theory-informed educational programs can effectively enhance students' belief in their capabilities (Van Dinther et al., 2011).

Individuals enhance their self-efficacy by connecting past and present experiences (Usher and Pajares, 2008; Ineson et al., 2013). This relationship is particularly evident in virtual communities, where knowledge sharing is essential (Hsu et al., 2007). Examples of knowledge sharing in such communities include online forums, where users engage in discussions and exchange ideas on different topics; professional networks and social media groups, where industry news and professional insights are shared; webinars and online courses that offer educational content from experts to a global audience; and blogs and vlogs, where individuals disseminate specialized knowledge and personal experiences. As people acquire more knowledge, their self-efficacy grows, leading to positive behavioral impacts such as

2.5. GAMES AND LEARNING INTERPLAY

increased participation in knowledge-sharing activities. This effect is observed in instances where individuals who have successfully shared knowledge or integrated information from various sources are more inclined to continue such activities (Hsu et al., 2007).

Integrating this comprehension with insights from the computer security domain, it becomes clear that the amalgamation of conceptual and procedural knowledge significantly shapes user behavior against online threats like phishing and malicious attacks (Arachchilage and Love, 2014). Users with a comprehensive knowledge base display notable improvements in circumventing cybersecurity threats (Zwilling et al., 2022). Their enhanced ability to avoid phishing attempts and other malicious activities is closely linked to their increased self-efficacy (Arachchilage and Love, 2014). Improving users' behaviors underscores the critical role of a thorough understanding of computer security principles and practices (Stanton et al., 2005). This understanding is not only foundational for grasping user behavior. Still, it is also crucial in the practical application of self-efficacy theory, particularly in the context of online engagement and information security (Rhee et al., 2009). It highlights how comprehensive knowledge is essential in understanding and effectively influencing user actions in the digital realm.

2.5 Games and Learning Interplay

2.5.1 Developing Knowledge through Gaming

The earlier section explored the influence of learning and knowledge development on shaping self-efficacy and user behavior. This discussion is particularly relevant in the context of rapid technological changes witnessed over the past few decades. Such advancements underscore the importance of continuously expanding and deepening individuals' knowledge and skills, particularly in diverse fields affected by digital transformation (Goulart et al., 2022). For instance, in the field of information technology, the evolving job market now demands not only technical qualifications but also personal development and social skills (Goulart et al., 2022). In order to address such concerns, it is essential to identify and implement effective strategies that enhance people's qualifications and foster a comprehensive understanding of new digital concepts and tools. In this context, games, gamification, serious games, and game-based learning emerge as promising approaches, emphasizing motivation, behavior change, and acquiring knowledge through gaming experiences in various everyday scenarios (Krath et al., 2021).

A game is a structured form of play or activity designed to bring participants enjoyment, challenge, or educational value (Abt, 1987; Aarseth,

2.5. GAMES AND LEARNING INTERPLAY

2014). Governed by a set of rules (Juul, 2011), games create an environment where players engage in a contest or pursuit towards specific objectives. This engagement can manifest in various forms, from competitive to cooperative player interactions (Lim and Reeves, 2010). Central to games is the element of challenge, requiring skill, strategy, or luck to overcome (Greg, 2002; Tekinbas and Zimmerman, 2005). As dynamic and engaging experiences, games evolve during play, demanding adaptability and offering clear outcomes and feedback on performance (Juul, 2011; Barr, 2017). Particularly in digital games, there is often a strong element of representation or simulation, where the game environment mimics aspects of reality or fantasy worlds (Tavinor, 2009). This broad definition encompasses the diverse nature of games, highlighting their role as sources of entertainment and as tools for education, social interaction, and mental stimulation (Ijsselsteijn et al., 2007; Rogers, 2017). Expanding beyond their formal role, engaging and interactive features of games have been adapted into new contexts through gamification, serious games, and game-based learning. Gamification applies the game design elements to non-gaming contexts, transforming tasks in education, health, finance, and other areas into more engaging and rewarding experiences (Detterding et al., 2011). By incorporating game design elements like points, badges, and leaderboards, gamification leverages the innate human desire for achievement and recognition, enhancing participation and motivation in various activities (Alsawaier, 2018).

Simultaneously, gamification shares a close relationship with two other concepts: serious games and game-based learning. Game-based learning represents an innovative educational approach that leverages the engaging and interactive nature of games, where players can learn via experience and solve problems through critical thinking (Chang and Hwang, 2019). Beyond education, serious games are a form of persuasive technology whose primary purpose is not merely entertainment but to influence user behavior and facilitate knowledge transfer (Orji et al., 2017; Adaji and Adisa, 2022). Serious games are crafted with specific cognitive attributes like problem-solving, memory enhancement, and attentional focus, making them exceptionally engaging through interactive and immersive gaming elements (Vlachopoulos and Makri, 2017; Lamb et al., 2018). They effectively utilize these cognitive traits, which enhances their adaptability across various areas. In the health domain, serious games focus on wellness and managing diseases. In the realm of public policy, they facilitate a deeper understanding of governance. They are crucial in honing strategic thinking and communication abilities for strategy and communication. In education, they support diverse learning objectives, while in training and simulation, they offer valuable professional

2.5. GAMES AND LEARNING INTERPLAY

development experiences (Lope and Medina, 2017). This versatility highlights their broad applicability and potential in shaping the future of educational and behavioral interventions.

In educational technology, the differentiation between gamification and game-based learning is characterized by their distinct approaches and impacts on learning outcomes. Research shows that both strategies can effectively enhance learning, though they operate differently (Karagiorgas and Niemann, 2017; Fernández Galeote et al., 2023). Gamification focuses on increasing learner motivation by incorporating game design elements into educational content. However, it often does not consider individual learner preferences (Monterrat et al., 2015) and needs to be personalized to suit the characteristics of each player (Oliveira et al., 2023). On the other hand, game-based learning centers around using games as the primary mode of instruction. It offers a more immersive educational experience and is realized as individuals play games to learn content. Nevertheless, game-based learning faces challenges that encompass accessibility concerns, the transferability of acquired skills to practical situations, and the delicate task of harmonizing engaging gameplay with educational objectives (Al-Azawi et al., 2016; Giannakas et al., 2018). Data security and user privacy also pose substantial concerns, as mobile and ubiquitous game-based learning apps often involve collecting sensitive personal data (Smith et al., 2015; Giannakas et al., 2018). These complexities underscore the critical importance of a thoughtful and inclusive approach to integrating game-based learning within educational settings.

2.5.2 Theoretical Connections to Gamification

Exploring the use of game elements in learning contexts and transferring knowledge reveals a fascinating blend of theories from psychology and education (Krath et al., 2021). In this intricate mix of ideas, two essential concepts, motivation and engagement, emerge as interconnected yet distinct elements that play a crucial role in learning and human behavior (Alsawaier, 2018). Motivation delves into the psychological drivers behind our actions and choices (Sailer et al., 2013). It encompasses various components, including intrinsic motivation, which ignites our innate desires for mastery and curiosity, and extrinsic motivation, which is influenced by external factors such as rewards and grades (Alsawaier, 2018). Conversely, engagement reflects the passion and emotional involvement individuals display when participating in learning activities. It contains observable behaviors, effort, and dedication in performing tasks, emphasizing the enthusiasm and diligence invested in learning (Alsawaier, 2018). Motivation and engagement

2.5. GAMES AND LEARNING INTERPLAY

form the fundamental essence of Self-Determination Theory (SDT) when understanding human motivation. This theory emphasizes three core aspects: *autonomy*, *competence*, and *relatedness* (Ryan and Deci, 2000). In gamification, this translates to giving users choices in how they approach tasks (autonomy), providing progressively challenging levels that match their skillset (competence), and enabling social interaction, like team challenges or leaderboards (relatedness) (Sailer et al., 2013). The influence of SDT on behavior is more distal, indirectly impacting motivation by fostering a more profound, intrinsic desire to participate (Sweet et al., 2012). For instance, in an educational game, allowing students to choose their learning path (autonomy) can increase their intrinsic motivation to learn, as it aligns with their interests or goals.

The alignment between SDT and self-efficacy theory offers valuable insights into the drivers of human behavior. Both theories share a core belief that individuals are agents of their actions but diverge in their views on agency. Self-efficacy theory significantly emphasizes self-efficacy as the key motivator, suggesting that people act when they believe they can achieve their goals. On the other hand, SDT underscores autonomy as a central factor, contending that self-determined motivation plays a pivotal role in influencing behavior (Sweet et al., 2012). Furthermore, these theories differ in how they position competence/self-efficacy, with SDT considering it as a more distal factor linked to motivation and self-efficacy theory considering it a proximal factor with a direct impact on behavior. Understanding the alignment and distinctions between SDT and self-efficacy theory provides a foundation for grasping human motivation and behavior. It ensures that users are engaged due to the immediate confidence boost from overcoming challenges and enjoy a more profound satisfaction from a self-determined desire to learn and connect with others (Sweet et al., 2012).

The study of gamification and its influence on behavior is also anchored in other psychological and sociological theories. Reinforcement Theory (Skinner, 1953) plays a pivotal role in understanding how rewards and incentives in gamified environments can shape behavior, particularly in learning contexts where elements like points and leaderboards act as immediate feedback mechanisms (Richter et al., 2015). The Theory of Reasoned Action (Ajzen, 1980) and the Theory of Planned Behavior (Ajzen, 1991) offer insights into how an individual's attitudes and subjective norms influence their behavioral intentions in educational gamification (Chen, 2018). Similarly, the Technology Acceptance Model (Davis, 1989) is crucial in evaluating how the perceived usefulness and ease of use of gamified systems affect their adoption and ongoing engagement (Bourgonjon et al., 2013). The Trans-

theoretical Model (Prochaska and Velicer, 1997) provides a framework for understanding the stages of behavioral change, which is essential in designing gamified interventions tailored to individuals' readiness for long-term engagement (Hammerschall, 2019). Lastly, Activity Theory (Vygotsky and Cole, 1978) considers the dynamic and complex interplay between individuals, their diverse perspectives, and the socio-cultural context of activities. It highlights the importance of recognizing and leveraging individual differences, understanding the specificity of contexts, and addressing ethical concerns through the lens of agency and transformation, focusing on the transformative power of gamification in educational and other activity systems (Vermeulen et al., 2016). These theoretical frameworks collectively enrich our understanding of how gamification can influence behavior across various domains.

2.6 Knowledge Transfer and Building Self-Efficacy

2.6.1 Gamification Boosting Security Knowledge

Expanding from the theoretical groundwork laid out earlier, the following section transitions into how these foundational principles are practically applied across different HCI methodologies to bolster privacy and security awareness. In recent years, increasing recognition and interest in leveraging digital games and game mechanics to enhance education has grown (Gros, 2007). Implementing gamification in information security training has shown increased engagement and learning retention. Users exhibited heightened awareness of security practices, leading to improved preparedness against cyber threats (Francia et al., 2014). Researchers explored gamification to enhance traditional security awareness and training programs, which are often tedious. Their gamified prototype significantly increased employee engagement and raised knowledge levels by incorporating game mechanics like mastery, progression, and competition (Gjertsen et al., 2017). In a related study on the efficacy of gamification in educating average users about password security, Scholefield and Shepherd (2019) created an Android app called "Role-Playing Quiz". This app presents questions on topics like strong password creation and the avoidance of common passwords. Correct answers diminish the strength of a dark knight character during gameplay, whereas incorrect responses weaken a golden knight. The study's outcomes highlighted that users found the learning process enjoyable through the application and reported comprehensible benefits stemming from the incorporation of gamification techniques.

Baral and Arachchilage (2019) explored enhancing users' self-efficacy to improve their phishing threat avoidance behavior through a gamified

2.6. KNOWLEDGE TRANSFER AND BUILDING SELF-EFFICACY

approach. By integrating social cognitive theory, the study identified that observational, heuristic, and structural knowledge significantly boost self-efficacy. A theoretical framework linked these knowledge attributes with self-efficacy and threat avoidance behavior, culminating in a gaming prototype designed to reinforce these elements and thereby reduce phishing attacks. The findings suggest that incorporating these specific knowledge attributes into a gamified learning tool can effectively enhance users' confidence and motivation to avoid phishing threats. Moreover, studies found that gamified learning significantly improved overall information security knowledge, particularly in password management, Internet use, and information handling. However, this approach did not impact attitudes, compliance intentions, or the willingness of individuals to pursue further education in information security. These findings suggest the necessity of exploring additional methods to engage users effectively (Wu et al., 2021).

Studies emphasize the effectiveness of gamified cybersecurity training for developers to enhance engagement and learning. Given the rising cybersecurity breaches and the shortage of skilled professionals, it is essential to equip developers with comprehensive security knowledge. Boopathi et al. (2015) redesigned traditional training methods into interactive, multi-level games that test various cybersecurity concepts, making learning more effective and engaging. This gamified approach combined theoretical knowledge with practical application, better preparing developers for real-world challenges and enhancing digital security. Results from these implementations show increased learner motivation, a deeper understanding of cybersecurity concepts, and improved practical skills in real-world scenarios. Previous research has explored the effectiveness of gamified applications in enhancing awareness of cybersecurity threats and promoting secure coding practices in JavaScript, particularly among first and second-year undergraduate students (Berisford et al., 2022). Initial results indicate positive engagement outcomes, implying the potential for integrating such approaches into conventional educational frameworks.

As highlighted in the introduction, legislators constitute a critical component in data-driven services. Similar to users and developers, gamified learning methods engage and empower legislators to comprehend complex legal concepts effectively. By integrating game-like elements such as challenges, rewards, and simulations, this approach revolutionizes legal education and makes learning more dynamic and effective (Vargas-Murillo et al., 2023). The gamified learning environment enables legislators to immerse themselves in realistic scenarios, hone their problem-solving skills, collaborate effectively, and receive immediate feedback, which is critical for navigating intricate

laws such as data protection and privacy in today’s mobile and ubiquitous applications (Corrales Compagnucci et al., 2022).

2.6.2 Empower Security Awareness via Visualization

Information visualization is a powerful tool that transforms data into visual representations, effectively communicating complex information or concepts. These visualizations, ranging from quantitative graphs to qualitative diagrams and abstract visual metaphors, enhance understanding and clarity for the audience (Smiciklas, 2012). Moreover, they reduce cognitive effort and improve decision-making accuracy by utilizing visual forms, such as scatterplots for sentiment analysis or visualized risk data (Krum, 2013). The design of visualizations often aims to promote specific behaviors and facilitate faster comprehension, making them integral in fields like cognitive psychology, education, management, marketing, and information science (Eberhard, 2023). Visualization in Human-Computer Interaction can be defined as the process and practice of creating interactive visual representations of data that facilitate a dynamic dialogue between the user and the data interface (Dimara and Perin, 2020). This interaction involves a user performing actions on the data through the visualization system, which in turn provides responsive reactions that the user perceives and interprets. The goal of visualization in HCI is to support a broad spectrum of user intents, ranging from data analysis and exploration to personal engagement and storytelling, by enabling flexible and diverse interaction means. This includes input, processing, mapping, and presentation actions, as well as meta, social, and interface actions. Visualization systems in HCI aim to empower users to manipulate and personalize data representations, fostering deeper understanding and insight through iterative, goal-oriented interaction (Dimara and Perin, 2020).

In terms of data security, researchers underscored the critical role of visualization in both enhancing user experience and protecting sensitive data on mobile platforms. By adapting visual interfaces to user context and needs, there is potential to mitigate security vulnerabilities associated with mobile data access, especially in contexts like healthcare where data privacy is paramount (Muchagata and Ferreira, 2018).

A systematic literature review on cyber threats situational awareness visualizations uncovers a multifaceted landscape marked by significant gaps and promising opportunities (Jiang et al., 2022). The results reveal that while most visualizations are geared towards operational-level staff, there is an apparent lack of tools designed for managers, higher-level decision-makers, and non-expert users, underscoring a critical oversight in catering to diverse stakeholder needs. The review also highlights that threat information

2.6. KNOWLEDGE TRANSFER AND BUILDING SELF-EFFICACY

is predominantly visualized, leaving impact information, response plans, and collaborative data underrepresented. This imbalance suggests that current cyber threat visualizations may not fully support comprehensive risk management and coordinated responses to cyber incidents. Furthermore, the maturity of these visualizations is also questionable, as most evaluations are limited to demonstrations or toy examples rather than rigorous, real-world industrial applications (Jiang et al., 2022).

In contrast to conventional desktop and mobile interfaces, Internet of Things (IoT) and smart devices often lack screens, posing challenges for existing privacy protection methods. Al Muhandar et al. (2023) investigated current web, mobile, and IoT privacy visualization techniques, pinpointing five crucial privacy considerations specific to IoT: data type, usage, storage, retention period, and access. They explored diverse notification approaches, employing icons, text, and colors to represent distinct privacy factors. Icons provided quick insights, with tooltips appearing upon hover for detailed information, and toggle switches enabled interactive adjustment of privacy settings. Labels accompanied by icons and concise text summaries delivered rapid overviews of privacy practices, emphasizing key details through bullet points and bold formatting. Their results demonstrated that integrating these visualization techniques enhanced users' comprehension and management of privacy settings on IoT devices. Users reported improved clarity regarding data handling practices, empowering them to make informed privacy decisions. Interactive elements such as toggle switches and tooltips effectively engaged users and offered actionable insights. At the same time, icons and labels facilitated swift communication of essential information without overwhelming the user.

2.6.3 Self-Efficacy Enhancement with AR Interaction

Augmented Reality (AR) overlays digital information onto the real-world environment in real time, enhancing user perception and interaction. AR devices accurately track and integrate virtual content with the physical world by using sensors, cameras, and computer vision. Key applications include education, where AR models enhance learning; retail, offering product visualization; navigation, providing real-time guidance; entertainment, creating immersive games; and maintenance, aiding in repairs with overlaid instructions. Despite technical and user experience challenges, AR continues to evolve, promising broader adoption and transforming our interaction with everyday environments through advancements in hardware, software, and content creation (Eberhard, 2023). Researchers explored how using AR technology to complete programming tasks affects student academic self-

2.6. KNOWLEDGE TRANSFER AND BUILDING SELF-EFFICACY

efficacy in higher education. They found that cognitive strategies enhance task value and technology characteristics, boosting academic self-efficacy. The study recommends integrating AR into education to enhance engagement and confidence (O'Connor and Mahony, 2023). Similarly, another study underscores AR technology's role in enhancing learning outcomes, self-efficacy, and personal development in language education settings and advocates integrating AR into education to foster engagement, confidence, and broader educational innovations (Khodabandeh and Mombini, 2024). While AR shows its ability to enhance learning, a study on integrating AR, gamification, and serious games in computer science education revealed compelling benefits. Through an educational mobile application, it was found that these technologies enhance learning by making it more interactive and student-centered. Students reported increased motivation, engagement, and enjoyment in learning activities while improving their critical thinking and social skills. The app effectively met users' psychological needs for autonomy and competence, fostering a positive learning environment that enhances cognitive and social-emotional development (Lampropoulos et al., 2023).

Alqahtani and Kavakli-Thorne (2020a) developed an AR game called "CybAR" aimed at increasing cybersecurity awareness. One study focuses on the practical aspects of this initiative, detailing the game's design, which includes interactive tasks and quizzes to educate users about various cybersecurity threats and safe practices. Following their development, they surveyed 91 participants, which showed positive responses, indicating the game's effectiveness in engaging users and enhancing their understanding of cybersecurity concepts. Important results include a majority of participants agreeing that the game made learning cybersecurity concepts more accessible and enjoyable and significantly increased their awareness and motivation to adopt safer online behaviors.

Another study takes a more theoretical approach, utilizing the Technology Threat Avoidance Theory (TTAT) to identify and analyze factors influencing users' cybersecurity behavior. Following their development, they examined individual differences such as demographic factors, personality traits, risk-taking preferences, and decision-making styles, exploring how these variables affect users' motivations and behaviors toward cybersecurity threats (Alqahtani and Kavakli-Thorne, 2020b). This study found significant correlations between these individual differences and users' avoidance motivation and behaviors, providing a deeper understanding of the psychological and behavioral aspects of cybersecurity education. The results suggest that tailoring educational tools to consider these individual differences can enhance the effectiveness of cybersecurity training programs.

2.7 Integrating Theories with HCI Approaches

2.7.1 Research Questions

In an earlier section of this chapter, we introduced the Social Cognitive Theory (Bandura, 1986) and outlined its foundational components. For the purposes of this dissertation, our analysis focuses specifically on the core elements of this theory: self-efficacy, goals, and behavior. We intentionally exclude outcome expectations and sociostructural factors, which are significant aspects of the SCT, but are not central to our current studies. By concentrating on these main components, we aim to examine in depth how self-efficacy beliefs, the process of setting goals, and the resulting behaviors interact within the specific contexts studied in this research. Aligned with Bandura's model (Bandura, 2012), Figure 2.3 illustrates these pathways of influence, emphasizing how perceived self-efficacy plays a crucial role in shaping goals and directly influencing user behavior.

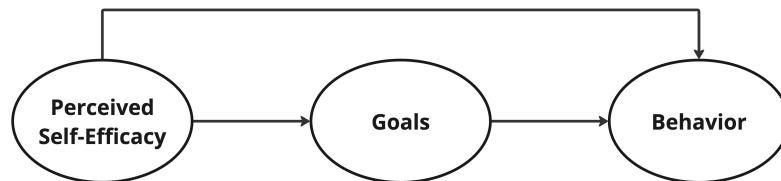


Figure 2.3: This illustration captures the routes of influence where perceived self-efficacy impacts the shaping of goals and directly influences users' behavior.

We mentioned that the Fogg Behavior Model focuses on the interplay of motivation, ability, and triggers to facilitate behavior change effectively. This model is particularly relevant for designing interfaces and applications aimed at altering user behaviors, serving as a meta-model within our approach. By addressing practical considerations in behavioral design, such as simplifying tasks and enhancing motivation through triggers like notifications, the FBM offers a structured framework for creating user-friendly systems that promote desired behaviors.

Our exploration further highlights the integration between the Social Cognitive Theory and the Fogg Behavior Model. While the SCT operates as a conceptual framework, offering insights into the interaction between personal beliefs, goal settings, and behaviors, the FBM translates these insights into actionable design strategies. This combination of models allows us to understand and influence user behavior, particularly within the contexts of privacy and security in mobile and ubiquitous computing applications.

2.7. INTEGRATING THEORIES WITH HCI APPROACHES

Although the Fogg Behavior Model guides the structuring of triggers and task simplification, and the Social Cognitive Theory provides a framework for understanding self-efficacy and behavioral influence, the specific effects of these models on user behavior in the context of privacy and security settings remain uncertain. In order to address this gap, our research aims to answer the following questions, focusing on how psychological models can enhance user interaction with privacy and security tasks.

RQ1

How do game elements and narratives in ubiquitous and mobile applications enhance users' self-efficacy, boost intrinsic motivation, and promote the adoption of informed behaviors?

RQ2

How do visualization techniques in ubiquitous and mobile applications enhance users' ability to manage security settings, interact with their self-efficacy, and promote informed behaviors?

Alongside investigating the influence of motivation and ability, we furthermore seek to explore the role of triggers. Specifically, we will examine how the temporal precision of triggers, including their timing and contextual relevance, influences users' decision-making and actions when configuring privacy and security settings within these technological environments. Therefore, we will investigate the next question.

RQ3

How does the temporal precision of triggers impact users' decision-making and actions when configuring privacy and security settings within ubiquitous and mobile applications?

Through the preceding three questions, we examine the roles of motivation, ability, and triggers within the Fogg Behavior Model and their effectiveness in promoting behavioral change. Nevertheless, developers frequently design apps with a multitude of privacy and security settings in real-world applications, embedding numerous complex terms, options, and configurations that challenge users' understanding and decision-making processes. This complexity can result in scenarios where, despite users' willingness to engage and make proactive choices, they may lack the necessary clarity to navigate

2.7. INTEGRATING THEORIES WITH HCI APPROACHES

these settings effectively or to make informed decisions about their privacy and security due to inaccessible information, ambiguous interfaces, or unclear explanations. Furthermore, the transparency of these mechanisms often varies, with some settings presented while others remain obscured or challenging to interpret. For many users, this lack of clarity creates uncertainty around how their data is used or shared, directly impacting their trust and willingness to engage with these applications. To address these issues, it becomes essential to focus on user empowerment, ensuring that users have the foundational understanding and accessible tools needed to navigate privacy and security settings confidently. The need for empowerment shapes our next research question, which focuses on examining whether users understand core security components and if apps are designed with transparent mechanisms to support informed decision-making.

RQ4

Do users understand the basic components of security, and do apps implement transparent mechanisms to support this understanding?

By addressing the previous questions, we establish the groundwork for understanding the individual elements (motivation, ability, and triggers) that influence user behavior within privacy and security contexts. We explain how game elements and narratives boost users' intrinsic motivation and self-efficacy, how visualization techniques enhance their ability to manage privacy and security settings, and why transparency and clear information in privacy and security mechanisms are essential for fostering informed decision-making. These insights underscore the necessity of empowering users through accessible, comprehensible, and engaging design choices in ubiquitous and mobile applications.

Building on this foundation, we turn to the role of augmented reality as a novel approach to further enhance users' self-efficacy and procedural knowledge. AR creates immersive, hands-on experiences that can simplify complex topics, making them more understandable and actionable. By visualizing privacy and security processes in an intuitive, real-world overlay, AR has the potential to deepen users' understanding, improve their motivation, and enable informed decision-making within these tasks. This leads us to our final question, which explores whether augmented reality can integrate the core elements of the Fogg Behavior Model by enhancing self-efficacy and procedural knowledge, ultimately empowering users in privacy and security settings in ways that 2D interfaces may not.

RQ5

How can augmented reality enhance users' self-efficacy and procedural knowledge to promote motivation, ability, and informed behavior in privacy and security tasks?

Since this question may raise issues regarding the potential effectiveness of 2D interfaces, we include a comparative study at the end of this dissertation to determine if a 2D interface in a replicated study can achieve similar effects. This approach allows us to explore whether the benefits associated with AR are exclusive to immersive environments or if they can also be realized within common 2D interfaces. By examining the 2D interface as a comparative benchmark, we can address concerns about the necessity and uniqueness of AR-specific features. This comparative analysis helps validate the potential of augmented environments and assesses if accessible and straightforward 2D settings can offer comparable advantages. Ultimately, this approach contributes to a well-rounded perspective on interface design choices, clarifying their roles in empowering users within a security context.

2.7.2 Theoretical Model

In addressing these five research questions, this dissertation proposes an extended model that integrates HCI approaches to investigate how acquiring security knowledge influences users' self-efficacy and subsequent behaviors within mobile and ubiquitous applications. Grounded in Bandura's Social Cognitive Theory, this model extends the original framework by positioning knowledge on the left side, illustrating its essential role in bolstering self-efficacy. Here, knowledge is emphasized as a foundational component for users, building their confidence in managing privacy and security tasks effectively. The model seeks to bridge the gap between understanding and action, empowering users to make informed decisions regarding privacy and security features (see Figure 2.4). The behavior component has been refined to focus on informed behavior, highlighting the objective of promoting privacy and security choices rooted in understanding. This modification shifts the focus from general actions to deliberate, security-aware behaviors that align with users' privacy preferences, marking a distinct contribution within this extended SCT-based model. In this framework, self-efficacy is linked to informed behavior through two primary pathways: motivation and ability, as outlined in the Fogg Behavior Model. Motivation represents the user's drive to engage with privacy and security tasks, while ability reflects their competence in managing these tasks effectively.

2.7. INTEGRATING THEORIES WITH HCI APPROACHES

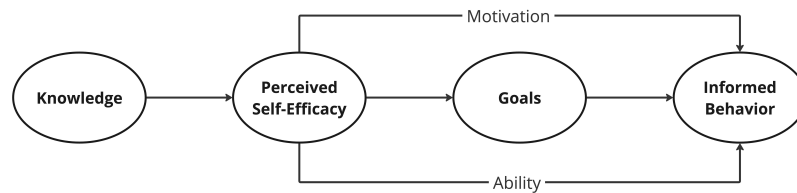


Figure 2.4: This model illustrates how knowledge acquisition influences users' self-efficacy beliefs and behaviors.

This dissertation addresses five research questions that progressively construct and validate a comprehensive model to understand user behavior in privacy and security contexts within mobile and ubiquitous applications. Each question targets a core component of the model, helping to assess the influence of motivation, ability, goals, and knowledge on informed behavior. These components are illustrated in Figure 2.5. The first research question delves into motivation to identify what drives users to engage with privacy and security tasks actively. The second question investigates ability, focusing on users' competence in effectively managing these tasks. The third question examines goals, which are closely linked to triggers defined by the Fogg Behavior Model. These triggers set immediate goals for users, prompting specific actions that align with their privacy and security preferences. The fourth question explores the role of knowledge, highlighting its importance in building users' self-efficacy for managing privacy and security. The fifth and final question validates the entire model, examining how motivation, ability, goals, and knowledge interact to promote informed behaviors. This comprehensive approach enables a deeper understanding of user interactions with privacy and security features in mobile and ubiquitous applications.

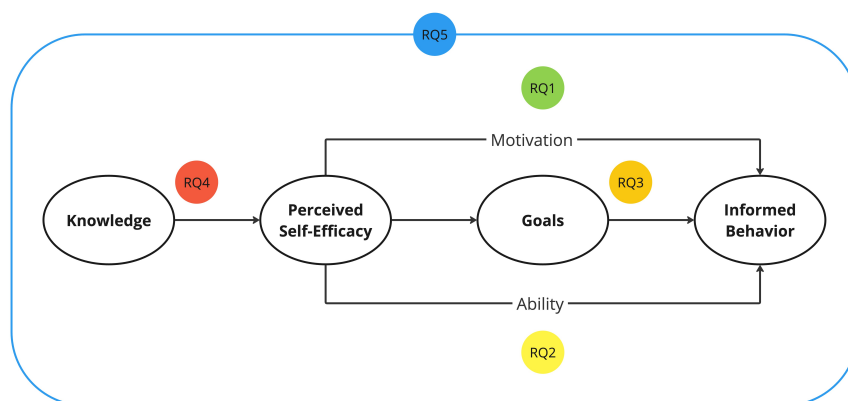


Figure 2.5: Research questions addressing relationships within the model

3

Security Behavior Elements

This chapter explores the dynamics of user behavior in privacy and security settings within mobile and ubiquitous apps, guided by the Fogg Behavior Model. Through multiple studies, the research investigates how the components of the FBM, including motivation, ability, and triggers, can drive user engagement and informed behavior. The initial section examines motivational drivers, focusing on gamification, humor, and narrative premises in educational tools to enhance engagement and effectiveness in security learning. Following this, the chapter assesses users' ability to manage privacy settings through infographics, interactive permission visualizations, and a user-friendly security scanner, simplifying complex privacy controls. Finally, it analyzes the impact of various triggers, including sparks, facilitators, and signals, to encourage proactive security behaviors. Each approach demonstrates how HCI can integrate user-centered design and well-timed prompts, ultimately empowering users to navigate privacy and security challenges confidently and independently across digital platforms.

3.1 Motivational Drivers Analysis

As mentioned earlier, the Fogg Behavior Model suggests that the efficacy of a behavior hinges on an individual's motivation and ability levels before engaging in a task, with triggers serving as intervention mediators. To explore deeper into the impact of gaming on individuals' motivation within the domain of mobile security, we¹ conducted studies encompassing three distinct approaches. The first study delves into gamification, investigating its potential to enhance mobile security awareness among users. By integrating game design elements into the learning process, this research aims to evaluate how such an approach can make understanding mobile security settings more interactive, enjoyable, and effective. The study builds on the premise that engaging users through gamified learning experiences can significantly boost their motivation and comprehension, grounded in the principles of self-determination theory.

Following the theme of engaging educational methods, the second study focuses on humor, explicitly examining its impact within a decision-making game on users' motivation and awareness regarding mobile privacy and security issues. This investigation seeks to understand whether incorporating humor into educational content can make learning about serious topics like privacy and security more appealing and memorable, enhancing educational interventions' effectiveness.

The third study explores the influence of narrative premises, specifically themes of good versus evil, on user engagement and learning outcomes in an educational game centered on smart home security. This research examines whether the narrative context within which educational content is delivered affects users' motivation to learn and their ability to comprehend and apply security recommendations, leveraging standardized measures to assess the game's usability and the motivational impact on its players.

Collectively, these studies offer innovative insights into harnessing gamification, humor, and premise to elevate motivation in digital security education. Their findings underscore the potential of these approaches to engage and inspire users towards improved digital practices, reflecting the Fogg Behavior Model's emphasis on motivation as a pivotal factor in driving behavior change in digital privacy and security.

¹Commencing from this position and continuing through, "we" refers to my collaborative efforts as the author, colleagues, and students involved in conducting multiple studies referenced throughout this dissertation.

3.1.1 Study 1: Gamifying Mobile Security Settings

Introduction and Background

The widespread adoption of mobile devices, such as smartphones and tablets, has profoundly transformed how people engage with technology daily (Wang et al., 2016). They have advanced functionalities and extensive storage capacities, making them indispensable tools central to modern lifestyles. These devices have become integral parts of everyday life, unprecedentedly shaping communication, productivity, and entertainment. However, the proliferation of sensitive data stored on these devices, from personal contacts to financial information, raises significant concerns regarding user privacy and the risk of installing malicious apps (Nauman et al., 2010; Zhou et al., 2012; Egelman et al., 2013; Moonsamy et al., 2014; Wijesekera et al., 2015). In response to these challenges, operating systems like Android have implemented permission mechanisms to regulate the access of apps to sensitive data. Despite these efforts, research indicates a gap in users' understanding and awareness of security implications when granting requested permissions to apps (Felt et al., 2012; Ramachandran et al., 2017). Users often overlook security risks or lack the necessary knowledge to make informed decisions (Krutz et al., 2016). Consequently, instances of permission misuse leading to privacy breaches are prevalent in the mobile ecosystem. For instance, a *Flashlight LED* widget abused permissions, gaining device administrator privileges and surreptitiously harvesting banking credentials (Barker, 2017). Similarly, the official app of the Spanish soccer league, *La Liga*, covertly accessed users' microphones to detect unlicensed broadcasts (Cuthbertson, 2019). These cases highlight the complexity and seriousness of permission misuse, emphasizing the necessity of educating and informing users about such circumstances.

Numerous approaches have been investigated in the literature to tackle privacy and security concerns associated with mobile devices. Some studies have focused on improving the presentation of permissions to users, such as integrating privacy information into the app decision-making process (Kelley et al., 2013) or customizing permission dialogues with personalized examples (Harbach et al., 2014). Others have developed tools to enable users to specify privacy settings for installed apps (Zhou et al., 2011; Liu et al., 2016). Addressing the challenge of raising awareness among users regarding the misuse of Android permissions by malicious apps necessitates exploring alternative methods incorporating personalized intervention techniques. While traditional instructional approaches may require adjustments to the Android framework or visualization techniques, the integration of tailored interventions can significantly enhance effectiveness (Forget et al., 2016).

3.1. MOTIVATIONAL DRIVERS ANALYSIS

Gaming stands out as a particularly promising avenue in this regard, as it has been shown to motivate users and improve learning outcomes in security training (Nagarajan et al., 2012). The decision to adopt a gaming approach for educating users about Android permissions is influenced by several key factors. For instance, research has consistently shown gaming to be significantly more effective in retaining information than traditional instructional methods, highlighting its potential for educational purposes (Annetta, 2010). It is particularly evident in the success of previous games in teaching security-related concepts like phishing avoidance (Sheng et al., 2007; Canova et al., 2014) and cyber security (Le Compte et al., 2015), suggesting their applicability to complex topics such as privacy awareness. Furthermore, incorporating principles such as reinforcement, incentives, customization, contextualization, and feedback provides further validation for using games in educational interventions. Reinforcement utilizes positive or negative stimuli to encourage desired behaviors (Linehan et al., 2011), while incentives align actions with users' desires to motivate them (Bada et al., 2019). Customization enables users to personalize their experience, fostering a sense of ownership and engagement (Charsky, 2010), while contextualization ensures that content remains relevant and grounded in real-world scenarios (Hamari et al., 2014). Lastly, feedback offers learners valuable insights into their performance, aiding in understanding strengths and weaknesses (Johnson et al., 2017). The need for educational tools specifically targeting Android-specific settings presents an opportunity to fill this gap and offer a tailored solution to effectively engage users and elevate their understanding through the integration of gamification techniques.

By adopting a multifaceted approach that integrates intervention techniques tailored to users' needs and preferences, we introduce *Make my phone secure!*, a gamified application to enhance user knowledge of Android security settings. The playful application *Make my phone secure!* was designed to answer our research question: *How can a gamified application help to raise understanding regarding mobile security settings?*

With the development of a gamified application, we aim to achieve a twofold educational objective. First, players shall acquire knowledge regarding the Android permission system in general. Most importantly, the app is designed to teach users what granting permission to any application can entail and what consequences this might involve. Second, we want to improve how users interact with the permission system. By letting them playfully explore the menu structure of a typical Android device, we intend to teach players how to turn on and off specific permissions for apps installed on the device. In a laboratory study involving 18 participants, we compared the efficacy

3.1. MOTIVATIONAL DRIVERS ANALYSIS

of our gamified approach with traditional Android menus and explanatory variants. Results demonstrated significantly heightened awareness among users of *Make my phone secure!*.

Our efforts in developing gamified mobile security solutions contribute to harnessing gamification’s potential to elevate security awareness, effectively engaging users and fostering better understanding.

Prototype Description

Concept Players in this interactive game immerse themselves in IT customer support, taking on the role of a tech specialist. Their mission is to navigate security and privacy challenges posed by digital clientele. The gameplay involves scenarios where virtual customers request assistance modifying app behaviors on their smartphones, such as turning off targeted advertising. Players must navigate the application settings to adjust permissions appropriately. The outcome of these interventions is reflected in the customers’ responses. Successfully identifying and modifying the correct app permissions leads to positive feedback, indicating issue resolution. This positive reinforcement serves as an extrinsic motivator, encouraging players to engage further and strive for accurate problem-solving.

Conversely, failing to address permissions accurately results in customer dissatisfaction, highlighting ongoing issues like unwanted personalized ads due to unchanged microphone permission settings. This negative feedback prompts players to enhance their decision-making skills to avoid future problems. The game’s design leverages this feedback mechanism to boost engagement and learning, motivating players through immediate customer responses and progression through levels. This extrinsic motivation complements the intrinsic enjoyment of the game, making it an effective tool for learning and skill development in a tech support context.

Game Design Each game level follows a clear sequence. The customer describes an issue to the player, who navigates various menu structures to adjust the necessary settings and find a solution. Ultimately, the customer provides feedback, expressing satisfaction or disappointment based on the player’s actions. Each stage is enhanced by interfaces designed in Unity². Upon initiating a level, the game presents the *Introduction* interface, featuring a screen with an avatar representing the customer alongside text detailing the issue (see Figure 3.1). Upon selecting *Let’s start!* located in the bottom right corner, players progress to the next stage.

²<https://unity.com/>

3.1. MOTIVATIONAL DRIVERS ANALYSIS

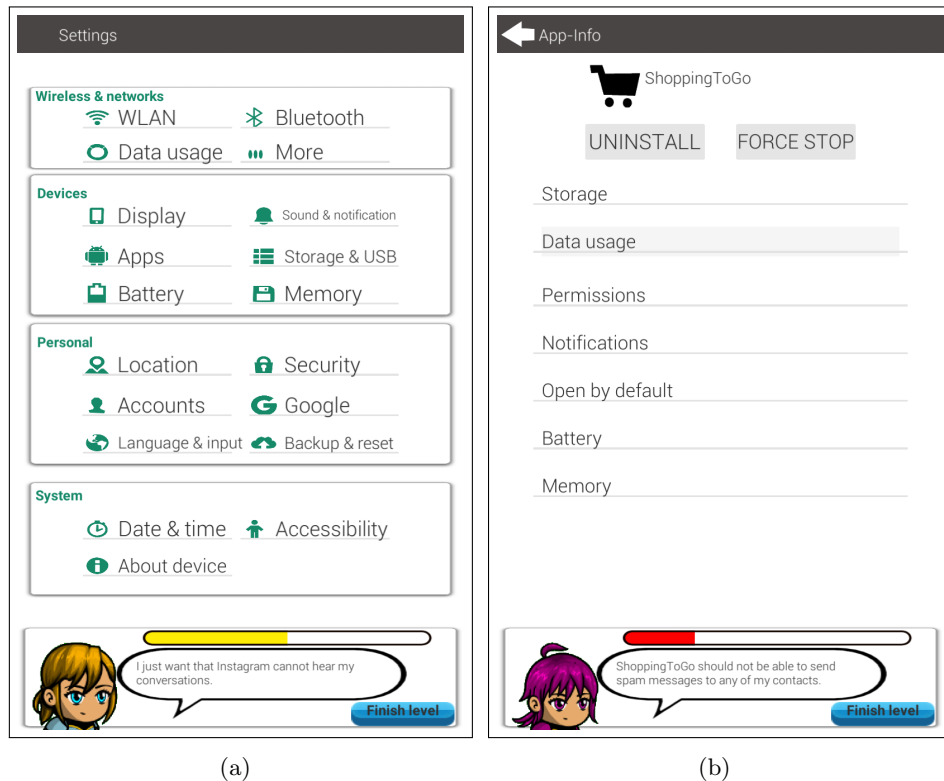


Figure 3.1: Each level of the game features introductory texts that highlight key issues. The first level, *Instagram hears my conversations* (a), raises privacy concerns. The second level, *Flashlight could steal my data* (b), warns about app permissions. The third level, *ShoppingToGo sends spam messages* (c), addresses unwanted communications.

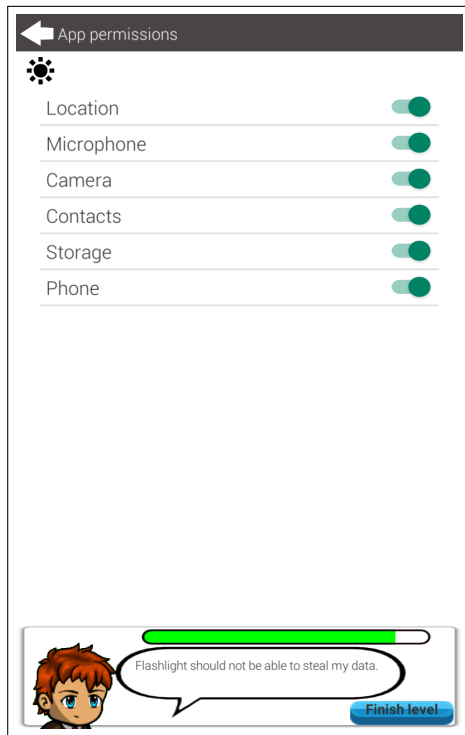
3.1. MOTIVATIONAL DRIVERS ANALYSIS

After completing the *Introduction* level, players progress to the *Progression* stage of the game. In this stage, they are tasked with navigating menu structures that closely resemble those in Android 6. Their objective is to locate and turn off specific permissions associated with various applications. As players engage with these menus, the game provides continual feedback that guides their decisions. This feedback helps players understand whether their actions are effectively advancing them toward the intended goal of managing app permissions. Overall, this immersive experience encourages players to explore the interface enthusiastically while simultaneously learning about app permissions in a practical context.

Feedback mechanisms include dialogue windows and a progress bar at the bottom of the screen, where correct actions fill the bar while incorrect decisions deplete it. Furthermore, customers within the game comment on each step the player takes. They offer either positive or negative feedback. In order to ensure fairness and clarity, criteria were established to define *wrong* actions, which primarily involve altering permissions unrelated to the designated app or adjusting settings for irrelevant applications. Conversely, correct actions involve successfully locating the app within the settings menu and deactivating the corresponding permission, as depicted in Figure 3.2.



3.1. MOTIVATIONAL DRIVERS ANALYSIS



(c)

Figure 3.2: Within the gaming interface, menus are clearly organized: a mimic of Android settings (a), enabling players to customize smartphone preferences; app information (b), which provides details about the specific application; and individual app permissions (c) for managing security settings. Additionally, subtle feedback on player progress is displayed at the bottom, giving a quick overview of achievements and encouraging ongoing engagement with the game.

Players can complete a level during gameplay by selecting the *Finish level* button in the lower right corner. This action triggers a new window, providing feedback on whether their decisions resulted in the intended outcome. Alongside customer feedback, the game also presents a rating determined by the progress bar from the preceding step (see Figure 3.3). For further clarification on the rating, players can click the *Explain* button, which offers a more comprehensive explanation that serves as the final stage of interaction in the game.

Scenarios In order to fully immerse players in the role of an IT support specialist, we focused on developing realistic scenarios within our game design. This dedication to authenticity led us to develop three distinct levels, with each one centered around the functionality of modern and widely used applications found on smartphones, like Android devices. Although the applications referenced (*Instagram*, *Flashlight*, *ShoppingToGo*) were not implemented within the game, they are grounded in real-world app experiences that players encounter daily. This approach allows players to engage with familiar contexts and challenges within the game environment of *Make my phone secure!*.

The initial level is dubbed *Instagram Hears my Conversations*. With

3.1. MOTIVATIONAL DRIVERS ANALYSIS

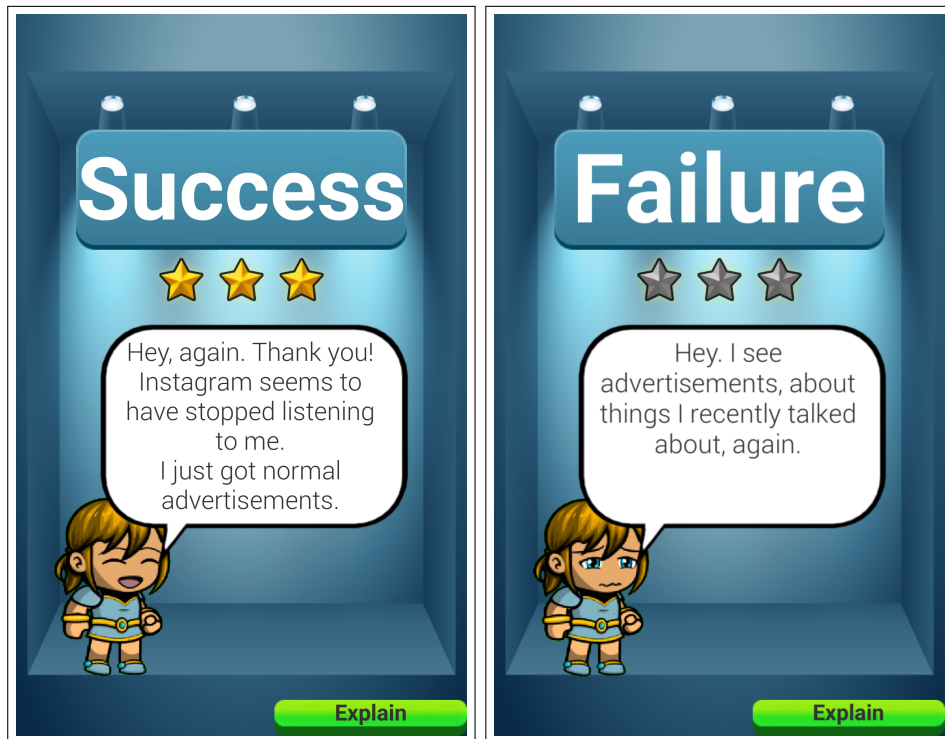


Figure 3.3: Final ratings are displayed at the end of one playthrough, depending on the success (left) or failure (right) of the player.

over one billion users, *Instagram*³ stands as one of the most popular applications on the Google Play Store. The app's free usage is supported by advertisements integrated into the user's feed. Among various permissions, *Instagram* requests access to the device's microphone. In a fictitious scenario presented at a gaming level, a client expresses concern over the app's display of personalized advertisements based on prior conversations. To progress successfully, players must locate and turn off the microphone permission. Subsequently, the client reports that personalized ads no longer appear. Conversely, if players neglect to adjust the permission, the client remains dissatisfied, citing unchanged behavior from *Instagram* (see Figure 3.4). The debate surrounding *Instagram*'s alleged eavesdropping on conversations lacks conclusive evidence, yet this example highlights potential security and privacy concerns associated with popular mobile applications. Despite the potential for misconceptions about *Instagram*, this fictitious scenario aims to evaluate users' comprehension of access rights and their implications within permission-based mobile apps.

³<https://www.instagram.com/>

3.1. MOTIVATIONAL DRIVERS ANALYSIS

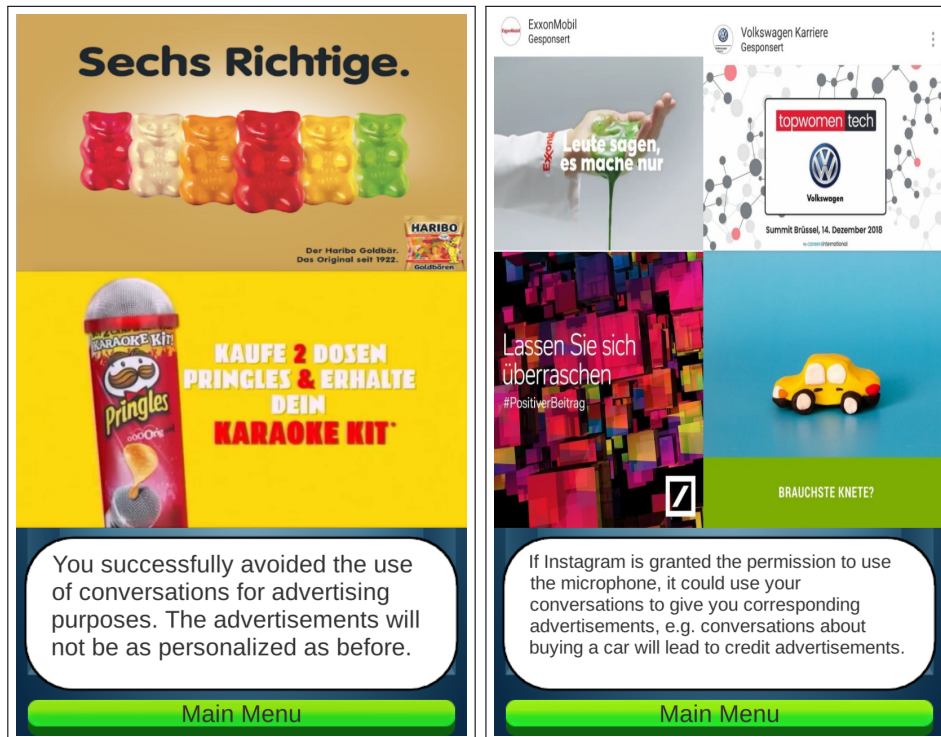


Figure 3.4: After completing the level *Instagram hears my conversations*, a positive or negative message is shown. If the level is successfully completed, the text on the left is unveiled; otherwise, the text on the right is displayed.

In addressing privacy concerns, the subsequent level is labeled *Flashlight could steal my data*. We introduced a widget named *Flashlight*, designed to utilize the camera's flash for illumination continuously. However, this utility necessitates users granting access to the device's storage. Given the prevalence of flashlight apps that seek permissions and data beyond their core functionality, posing potential risks for unauthorized access by malicious entities, it is crucial to raise awareness regarding privacy vulnerabilities on mobile devices. To illustrate this, we present a scenario where the virtual customer expresses apprehension about possible data theft by the *Flashlight* app, questioning the necessity of granting storage permission. Players are tasked with navigating through settings to adjust permissions accordingly. Successfully revoking the permission prompts a reassuring message indicating no data breach, while failure alerts the game about personal data leakage.

ShoppingToGo Sends Spam Messages is the third level that emulates a typical shopping application, enabling users to browse and purchase various products. However, it unexpectedly requests permission to access contact information without disclosing its intentions to the user. This fictitious app

3.1. MOTIVATIONAL DRIVERS ANALYSIS

can abuse this access to profit, potentially facilitating a hacker’s theft of user contacts for resale to advertising networks. This narrative underscores the importance of user privacy when granting contact permissions. Within this fictitious context, the virtual customer notices an uptick in spam messages among their contacts following the app’s installation, a behavior reported in the news as characteristic of *ShoppingToGo*. Consequently, the virtual customer suspects a correlation between app installation and spam messages. The narrative suggests that players should disable the contact permission. Upon completing the game, players are presented with text and images depicting the consequences of their actions. The outcome varies depending on whether players successfully turned off the permission. Success results in the cessation of *ShoppingToGo*-related spam messages to contacts, while failure indicates that the app continues to send messages unabated.

User Evaluation

Study Design The experiment followed a within-subjects design incorporating three conditions, each representing a distinct approach to conveying information about the application permission system. The experiment compared the educational impact of the following variants:

1. *Menu* variant: This prototype emulates the appearance, functionality, and user interface of a traditional Android system, presenting tasks as text and employing the same menu structure as the entire game for navigation. Upon task completion, the prototype displays a message indicating the player’s success or failure.
2. *Menu + Hints* variant: Similar to the first variant, this version includes menus with added hints delivered via small dialogue windows to assist players in achieving their objectives. For instance, a hint might advise the user to adjust settings for each installed application individually (see Figure 3.5).
3. *Gamified App* variant: This variant mirrors the game *Make my phone secure!* with all functionalities described in a prior section.

For the *Menu* and *Menu + Hints* variants, scenarios revolving around the mini-games *Instagram hears my conversations*, *Flashlight could steal my data*, and *ShoppingToGo sends spam messages* were developed. To mitigate confounding errors, a Latin square design (Colbourn and Dinitz, 2006) was employed to generate different orders for the variants and scenarios.

Material We developed a series of questionnaires to investigate the potential educational effects of each experimental variant. For the experimental

3.1. MOTIVATIONAL DRIVERS ANALYSIS

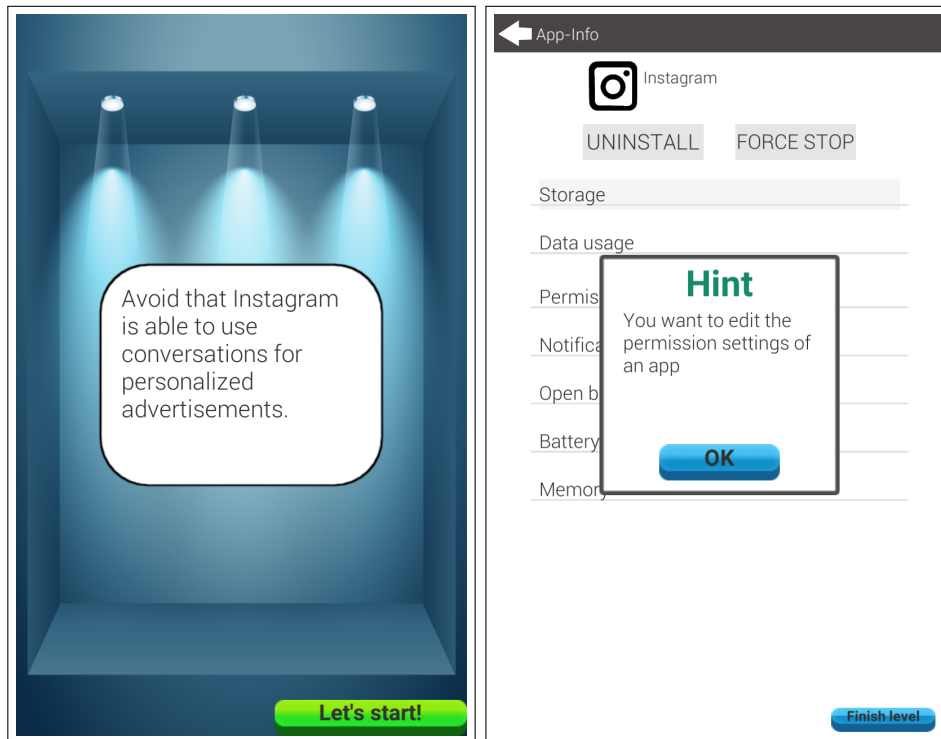


Figure 3.5: The start screen showcases the *Menu* variant on the left. At the same time, on the right, an exemplary hint is depicted from the *Menu + Hints* variant, both specifically designed for the study.

setup, we employed a Lenovo Tab2 A10-30 running Android 6.0.1 to implement the diverse experimental conditions. Initially, before treatment, participants were asked to provide demographic information (such as age and gender) and to share their familiarity with Android permissions, including their understanding of the permissions required by their favorite applications. Following this, we crafted targeted questions to assess participants' baseline knowledge regarding application permissions. These inquiries delved into their perceptions regarding the likelihood of applications using permissions for unauthorized activities, such as recording audio without authorization or sending unsolicited messages to contacts. It is essential to note that we only asked for the relevant level-specific permission in the context of the variant that participants were using or about to use. Therefore, if the microphone permission was not part of their playing level, these questions asked for different permissions (e.g., storage or contacts). Participants used a seven-point Likert scale, from "Very unlikely" to "Very likely", to rate their responses. To simplify statistical analysis, responses from this section were consolidated into a singular variable representing participants' awareness, determined

3.1. MOTIVATIONAL DRIVERS ANALYSIS

as the mean value. The disparity between pre-and post-treatment values was computed, denoted as *Awareness Progression* for statistical assessment. Concluding the questionnaire, participants were prompted to answer two straightforward questions: “How enjoyable was this version?” for *Perceived Fun* and “How informative was this version?” for *Perceived Informative Content*. Responses were recorded on a seven-point Likert scale, ranging from “Very boring” to “Very exciting” (and “I learned nothing” to “I feel enlightened” accordingly).

Procedure The study recruited participants via email distribution and printed notices placed throughout the university campus without disclosing details about the game’s context or the research objectives. The study was conducted in a laboratory setting, with all participants providing informed consent prior to its commencement. Before the intervention, participants completed a pre-test, responding to questions regarding *Awareness Progression*. Subsequently, all three experimental conditions were administered in sessions lasting 30-45 minutes each. After assessing baseline knowledge, participants were exposed to one of the variants (*Menu*, *Menu + Hints*, or *Gamified App*) along with a contextual scenario involving specific permission (microphone, storage, or contact). Following the intervention, participants completed questionnaires assessing *Awareness Progression*, *Perceived Fun*, and *Perceived Informative Content*. This process was repeated until all experimental variants had been tested.

Participants The study comprised 20 participants, all possessing a college degree. Originally intending to include 21 participants, logistical constraints led to excluding the last two for counterbalancing purposes. Hence, the data in this section reflects findings from 18 subjects. Among them, 13 self-identified as male and five as female. Regarding age, participants spanned from 21 to 36 years ($M = 25.27, SD = 4.77$). The participants volunteered for the study and did not receive any monetary compensation.

Ethical Considerations The study design was meticulously crafted in collaboration with data protection experts and well-versed legal advisors to ensure compliance with the General Data Protection Regulation (GDPR). Ethical approval was not required for the studies involving humans because the local ethics board only issues approval if funding agencies demand it. Nonetheless, the studies were conducted in accordance with local legislation and institutional requirements. Participants provided their written informed consent after the study director comprehensively elucidated all aspects of the research, including its objectives, procedures, potential risks, and benefits. Participants were explicitly informed of their right to withdraw from the

3.1. MOTIVATIONAL DRIVERS ANALYSIS

study at any stage without facing any repercussions. This transparent communication process aimed to empower participants to make well-informed decisions regarding their involvement, thereby upholding ethical standards of autonomy and respect for individuals' agency. Extensive measures were deployed throughout the study to prevent inadvertent processing of personal data, with particular emphasis on adhering to the principle of data minimization, thereby ensuring that no participants' personal data were collected or processed. Additionally, every effort was made to minimize any potential harm to the individuals involved (Bailey et al., 2012)⁴.

Empirical Findings

Before engaging with the three conditions, users were asked about their preferences for Android permissions management across different applications, including a social media platform (Instagram), a widget application (Flashlight), and a shopping application. The analysis showed that 9 out of 18 participants prefer to consciously control the permissions they grant to applications, indicating a high level of privacy attention. Conversely, 4 participants always grant permissions, aware of the potential consequences, while 2 are unaware of what Android permissions entail. A cautious approach was evident when examining preferences for granting widget and shopping applications permissions. For the widget application, 6 participants preferred not to grant any permissions, with Location (3 participants) and Location combined with Storage (2 participants) being the most acceptable permissions. Similarly, for shopping applications, 8 participants were comfortable granting no permissions, and Location was deemed acceptable by 6 participants. These findings highlight a dominant preference for limiting app permissions, with Location being the most commonly accepted permission when any permissions are considered acceptable.

We meticulously analyzed every variable using statistical methods to pinpoint potential disparities among the prototypes. The concept of *Awareness Progression* encapsulates the variance in all awareness-related inquiries pre and post-exposure to each condition. By employing dependent t-tests (Student, 1908) for paired samples, we systematically compared the pre and post-conditions for each variant, ensuring comprehensive evaluation. The *Menu* variant exhibits a noteworthy average progression ($M = 0.78$, $SD = 0.99$), demonstrating significant disparities ($t(17) = 3.23$, $p < 0.01$, $Cohen'sd = 0.79$). Equally promising results are observed with the *Menu + Hints* variant ($M = 0.65$, $SD = 0.97$), with a substantial effect ($t(17) = 2.77$, $p < 0.05$,

⁴Our ethical considerations follow a consistent approach across all studies. Additional explanations, if required, are provided in an extra section for clarity in each one.

3.1. MOTIVATIONAL DRIVERS ANALYSIS

$Cohen'sd = 0.67$), and the *Gamified App* variant ($M = 0.61, SD = 0.76$), which also yields significant progress ($t(17) = 3.33, p < 0.01, Cohen'sd = 0.8$) (see Figure 3.6). Notably, the data for all variants was found to be normally distributed. Furthermore, no statistically significant discrepancies were identified upon analyzing *Awareness Progression* across all variants using a one-way ANOVA for repeated measures (Fisher, 1970).

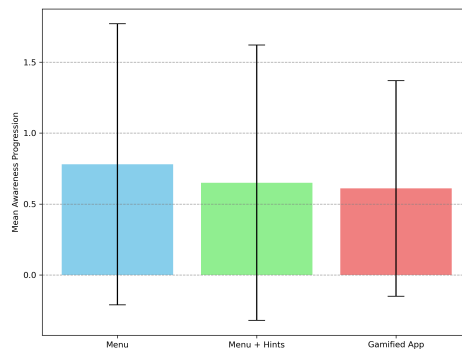


Figure 3.6: The chart displays the mean awareness progression for each variant, with error bars representing standard deviations, highlighting differences between the *Menu*, *Menu + Hints*, and *Gamified App* conditions.

We evaluated *Perceived Fun* using a one-way ANOVA for repeated measures, revealing statistically significant differences among the variants ($F(2) = 5.21, p < 0.05$). Going deeper with post-hoc examinations, we found that participants unequivocally perceived the *Gamified App* condition ($M = 5.78, SD = 1.13$) to be significantly more enjoyable compared to the *Menu* variant ($M = 5.06, SD = 0.91$) ($t(17) = 3.42, p < 0.01$). Similarly, the *Gamified App* was significantly preferred over the *Menu + Hints* ($M = 5.06, SD = 1.39$) ($t(17) = 2.85, p < 0.05$). Notably, no significant differences emerged regarding perceived fun between the *Menu* and *Menu + Hints* conditions ($p > 0.05$) (see Figure 3.7).

Perceived Informative Content is determined based on responses to the last question completed at the conclusion of the study. A one-way ANOVA for repeated measures was conducted, revealing statistically significant differences between the variants ($F(2) = 4.32, p < 0.05$). Post-hoc analyses indicate that participants rated the *Gamified App* condition ($M = 5.33, SD = 1.91$) as significantly more informative than the *Menu* ($M = 4.39, SD = 2.06$) variant ($t(17) = 3.45, p < 0.01$). No significant differences were found between the *Gamified App* and the *Menu + Hints* ($M = 4.78, SD = 2.10$) conditions. Likewise, no significant differences existed between the *Menu* and *Menu + Hints* conditions ($p > 0.05$) (see Figure 3.7).

3.1. MOTIVATIONAL DRIVERS ANALYSIS

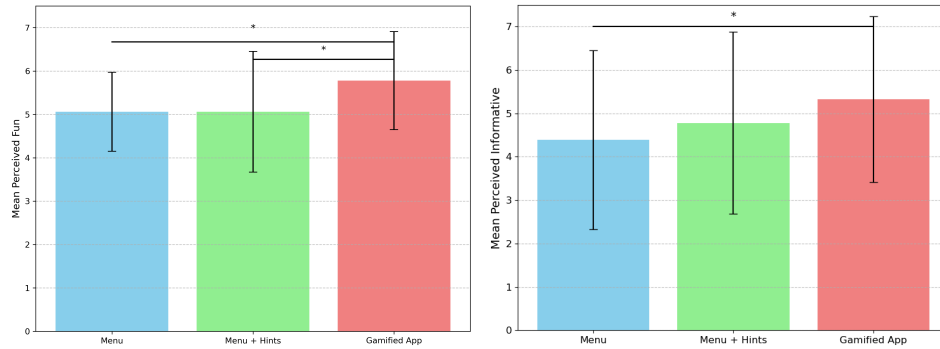


Figure 3.7: The chart on the left illustrates the mean perceived fun, while the right side shows the mean perceived informative content for each variant, with error bars representing standard deviations. Both figures compare the *Menu*, *Menu + Hints*, and *Gamified App* conditions, highlighting differences in participant perceptions across the variants. Asterisks (*) indicate significant differences.

Discussion and Limitations

The exploration of gamification in enhancing mobile security awareness underscores a promising avenue for engaging users in security education (Nagarajan et al., 2012). Our investigation was driven by a desire to thoroughly assess how gamification elements influence awareness and comprehension of mobile security settings within the *Make my phone secure!* application. This initiative stemmed from growing research indicating the effectiveness of gamification in fostering user engagement and guiding behavior toward intended objectives (Von Ahn and Dabbish, 2008). It is also supported by the principles of self-determination theory (Ryan and Deci, 2000), suggesting that gamification can significantly enhance intrinsic motivation by satisfying the psychological needs for autonomy, competence, and relatedness. By juxtaposing the initial findings from the users' preferences questionnaire analysis with the outcomes of the gamified intervention, a nuanced perspective on the effectiveness of gamification emerges, highlighting its significant role in bridging knowledge gaps and boosting user engagement.

Initially, the questionnaire about the users' preferences for Android permissions management across different applications revealed a baseline awareness among users regarding mobile security settings and permissions. This foundational knowledge, albeit varied, underscored an existing level of motivation with privacy and security concerns, particularly among younger users, who demonstrated a relatively high degree of awareness.

Despite this, the post-intervention analysis indicated a marked improvement in awareness and understanding, affirming that gamification could

3.1. MOTIVATIONAL DRIVERS ANALYSIS

further enhance comprehension, even among those with prior knowledge. Consistent with prior findings (Sheng et al., 2007; Canova et al., 2014; Le Compte et al., 2015), our study revealed that incorporating gamification elements significantly elevated users' engagement with mobile security concepts while maintaining the quality of their understanding and application of these concepts. It was particularly evident in the gamified application's ability to make learning more fun and informative than menu-driven structures.

The comparative effectiveness of gamified versus menu-driven interface approaches highlights an essential insight: while gamification stands out for its ability to motivate and engage, traditional methods, including menus with hints, also play a crucial role in raising baseline awareness about mobile security. This finding points to the value of incorporating exercises in everyday security tasks, suggesting that consistent interaction with security settings can enhance users' understanding and vigilance, even without gamification.

The study's findings advocate for a multifaceted approach to mobile security education, integrating both gamified and menu-driven interface learning methods to cater to a wide range of learning preferences and enhance the overall efficacy of security awareness programs. Further analysis of these findings through the lens of the FBM enriches our understanding of how gamification catalyzes behavior change (AlMarshedi et al., 2017). The model's emphasis on motivation, ability, and prompts aligns with the observed outcomes of the gamified intervention. Gamification not only heightened motivation by making the learning process more engaging but also increased users' ability to comprehend complex security settings through simplified, interactive tasks (Bada et al., 2019).

In summary, when contrasted with the post-intervention outcomes, the initial awareness levels captured through the pre-study questionnaire underscore the transformative potential of gamification in mobile security education. This approach enhances intrinsic motivation and comprehension among users with varying degrees of pre-knowledge. It integrates seamlessly with the principles of the Fogg Behavior Model (FBM), offering an innovative framework for fostering proactive engagement with mobile security practices. Through this multifaceted educational strategy, gamified learning emerges as a powerful tool for advancing security awareness and practice among a broad user base, highlighting the need for continued exploration and application of interactive learning methods in the digital age.

The study's representational validity is constrained, primarily due to using a custom questionnaire tailored to assess potential learning effects regarding the permission system. In the absence of established measures for this purpose, we devised our questionnaire, which needs more standardization and should

3.1. MOTIVATIONAL DRIVERS ANALYSIS

be approached with caution when interpreting results. Furthermore, the within-subjects design employed in the study may have introduced sequence effects despite attempts to mitigate them through condition counterbalancing. Participants may have acquired knowledge from one treatment to the next, potentially impacting the awareness ratings derived from the questionnaires. These methodological considerations underscore the need for ongoing research to refine and validate tools for measuring the impact of gamification on learning outcomes.

Acknowledgments

This section is based on the publication:

Mehrdad Bahrini, Georg Volkmar, Jonas Schmutte, Nina Wenig, Karsten Sohr, and Rainer Malaka. 2019. *Make my Phone Secure! Using Gamification for Mobile Security Settings*. In *Proceedings of Mensch und Computer 2019 (MuC '19)*. Association for Computing Machinery. DOI: 10.1145/3340764.3340775

My contribution to this work: Conceptualization, data curation, formal analysis, investigation, methodology, project administration, resources, part of software development, supervision, validation, visualization, and contribution to all parts of the manuscript.

3.1.2 Study 2: Humorous Decision-Making Game on Mobile Security

Introduction and Background

In our previous study, it was evident that users exhibit a keen interest in the security settings of their smartphones, particularly concerning permissions requested by installed applications. However, our findings revealed a lack of awareness regarding the potential ramifications of granting these permissions. By implementing gamified security settings, we successfully demonstrated an approach that informed users and fostered engagement by making the process enjoyable. Building upon our previous effort, we employ a humorous approach to the subsequent study to enrich learning experiences further and effectively communicate the consequences of users' decisions about smartphone security in a gaming environment. Humor in video games has been extensively documented, evident through amusing characters, narratives, gameplay mechanics, and events that improve the gaming experience (Hookham and Meany, 2014). Recognized as a potent tool for motivating individuals towards specific learning objectives, humor within video games enhances players' intrinsic involvement and delivers an enjoyable experience (Dormann et al., 2006; Lombardi, 2012). Beyond mere entertainment, humor influences social, emotional, and cognitive behavior, offering valuable insights for game design to support specific gameplay experiences and outcomes (Dormann and Biddle, 2009). Its potential as an educational tool is underscored by its ability to significantly enhance effective learning and intrinsic motivation (Dormann and Biddle, 2006). Furthermore, the literature highlights humor's capacity to facilitate learning by making it more enjoyable and reducing associated stress (Barral et al., 2017).

Prior research has delved into the integration of humor within educational materials, particularly within computer security, emphasizing the intricate balance between technical content, game mechanics, and humor integration (Denning et al., 2013). It explored how the creators navigated various design constraints to create an engaging and educational experience. Notably, incorporating humor through puns and popular culture references emerges as a distinctive feature to enhance player enjoyment while maintaining thematic coherence. Similarly, researchers investigated the impact of humor in interactive comics for security education (Leah Zhang-Kennedy and Biddle, 2016). Their findings reveal that integrating humor into the narratives makes learning enjoyable and facilitates better information retention. Humorous characters and engaging storylines capture users' interest and motivate them to delve deeper into the material. Their study suggests that humor is a

3.1. MOTIVATIONAL DRIVERS ANALYSIS

powerful tool for simplifying complex concepts, making them more accessible and memorable. Moreover, humor can prompt behavioral changes, as users are likelier to adopt positive security practices when presented with entertaining content. In this work, we present *What Could Go Wrong*, a humorous decision-making desktop game designed to prompt users to make informed decisions regarding smartphone privacy and security settings. Players encounter various scenarios throughout the game, and their decisions trigger informative feedback illustrating the consequences of their choices (see Figure 3.8).

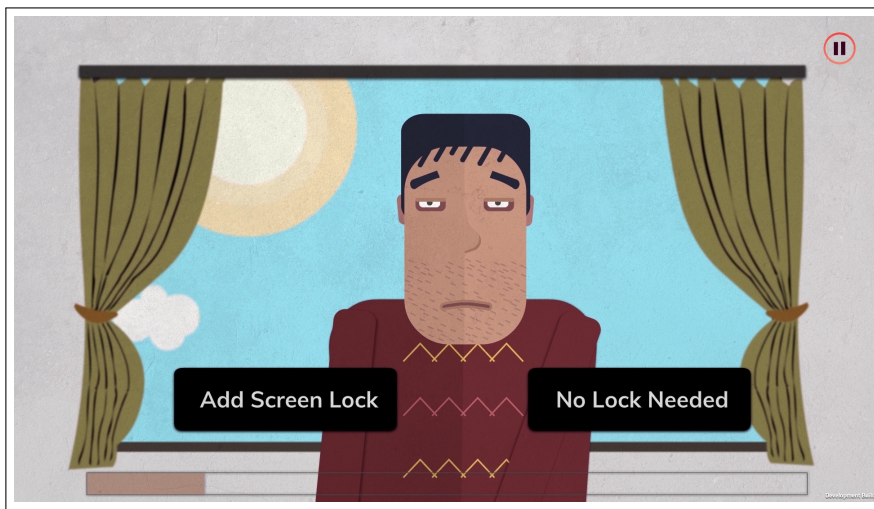


Figure 3.8: *What Could Go Wrong*: A humorous decision-making game that helps users understand the consequences of applying security changes on a mobile.

We conducted a preliminary study involving 21 participants, featuring two additional scenarios to evaluate the effectiveness of our game within contemporary content-sharing environments, such as online videos. In the first scenario, participants are exposed to a serious animated video that earnestly visualizes various actions on a mobile screen, highlighting pertinent issues related to privacy and security. Conversely, the second scenario introduces a different tone with a humorous animated video. This video adopts the same animated style used in the game, offering a lighter approach to the subject matter while addressing the importance of mobile privacy and security (see Figure 3.9).

Our study aims to explore how our approach influences user interest and motivation towards mobile privacy and security and its impact on user awareness of these crucial issues. We pose two research questions: 1) *To what extent does a humorous decision-making game influence user motivation to*

3.1. MOTIVATIONAL DRIVERS ANALYSIS

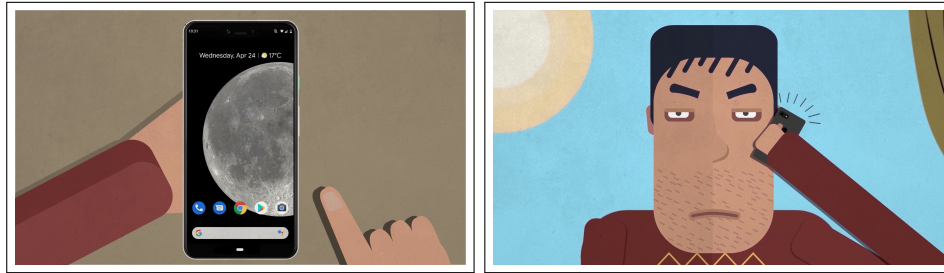


Figure 3.9: Additional video scenarios: On the left is a serious animated video on mobile privacy and security that visualizes actions on a mobile screen. On the right is a humorous animated video mirroring the style of the game.

engage with mobile privacy and security? 2) What are the potential effects of a humorous decision-making game on user awareness of mobile privacy and security issues? This study contributes to raising awareness of mobile device security settings among users, offering a novel learning approach to enhance understanding of the consequences of security and privacy decisions.

Prototype Description

Concept In *What Could Go Wrong*, players engage in a dynamic dialogue between two characters, navigating decision-making scenarios in the contemporary era. This adventure revolves around an animated character named “Michael” and his new smartphone. Acting as a trusted advisor, players interact with Michael and a humorous narrator, guiding them through various privacy and security dilemmas prompted by the smartphone’s features. With a blend of humor and seriousness, the game presents humorous conversations and animations, injecting a comedic essence into the experience. The game aims to raise awareness of common concerns in mobile device usage, targeted at smartphone users and those interested in privacy and security. Through its engaging narrative, “What Could Go Wrong” educates players on the potential threats of everyday activities with smartphones, delivering entertainment and insights simultaneously in an informal manner.

Game Design In the unfolding narrative of *What Could Go Wrong*, Michael embarks on a digital odyssey by receiving a new smartphone, only to find himself reluctantly recruited by the narrator to undertake various tasks. As a character, Michael’s grumpy demeanor colors his reception of these responsibilities, setting the stage for discord. However, the narrator, assuming the role of a knowledgeable guide, interjects with crucial insights into privacy and security concerns inherent in smartphone usage, such as screen locks, phishing attacks, dangerous Android Packages (APKs), and

3.1. MOTIVATIONAL DRIVERS ANALYSIS

app permissions. This clash of attitudes between Michael and the narrator introduces uncertainty, ultimately empowering the player to navigate through the divergent viewpoints, make pivotal decisions, and shape the course of Michael's journey, blurring the lines between humor, instruction, and choice.

In our game, players are empowered to navigate through various decision points, each influencing the duration and outcome of their gameplay. These decisions carry distinct consequences, yet regardless of the chosen path, all players will encounter equivalent security and privacy-related scenarios, ultimately concluding the game in identical states. Central to our game's appeal is its infusion of humor and entertainment. We ensure engagement by immersing players in relatable scenarios reflective of everyday smartphone usage. Information dissemination adopts an accessible approach, avoiding deep technical jargon for comprehension by the average smartphone user. In *What Could Go Wrong*, player interaction is streamlined, primarily reliant on the computer mouse or an equivalent pointing device (see Figure 3.10).

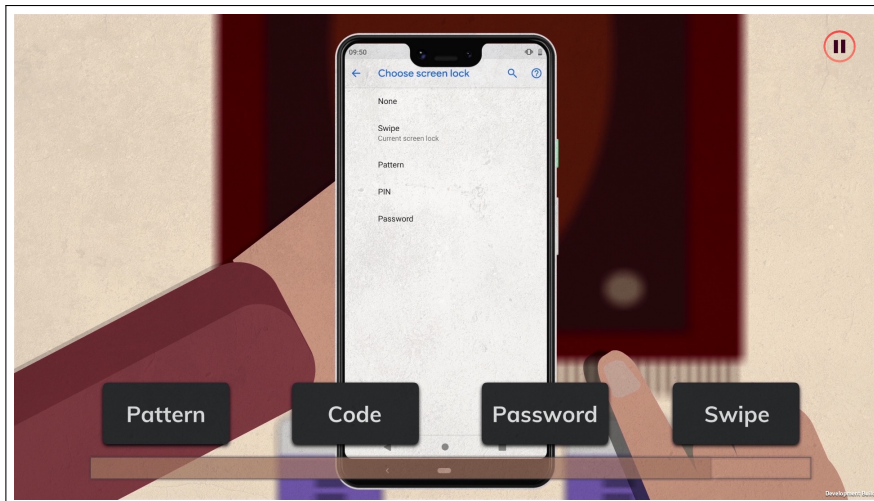


Figure 3.10: *What Could Go Wrong*: Players can choose from different screen-lock settings, influencing their gameplay experience and outcomes.

Certain decisions may expose the character's smartphone to hacking attempts, depicted through an immersive interface (see Figure 3.11). In such instances, players can use the time machine feature to rewind and reconsider their choices (see Figure 3.11), changing the course of events. By leveraging this innovative capability, players can meticulously explore alternative paths, strategically maneuvering through the challenges to thwart potential security breaches. This mechanism empowers players to shape the storyline actively, exerting control over the unfolding events and protecting Michael's privacy.

3.1. MOTIVATIONAL DRIVERS ANALYSIS

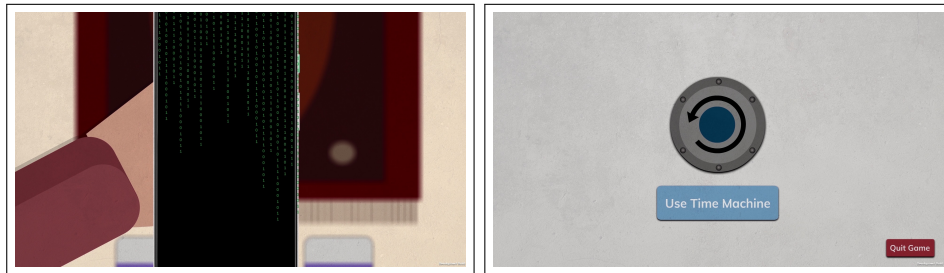


Figure 3.11: On the left, within *What Could Go Wrong*, certain decisions may result in the character’s mobile phone being hacked. On the right, players can utilize the time machine to revisit their last decision and make corrections.

User Evaluation

Study Design In order to assess the effectiveness and efficiency of our game in enhancing awareness and motivation regarding privacy and security concerns on mobile devices, we conducted a preliminary laboratory study employing a between-subjects design. The study comprised three distinct conditions, each requiring approximately 20 to 30 minutes. In the initial scenario, participants watched a short, serious, and informative animation lasting 4 minutes and 30 seconds. Subsequently, in the second scenario, participants viewed a longer informative animation lasting 7 minutes and 40 seconds, incorporating humor elements within the content. Finally, the third scenario involved participants actively engaging with the game. Across all scenarios, participants were presented with identical information concerning privacy and security on mobile devices.

Materials In this study, participants interacted with video content or a game displayed on a laptop with a 15.6-inch screen. Afterward, tasks were carried out using a smartphone featuring a 6-inch display and a 1440 x 2880 pixels resolution. Before each test session, experiment directors configured the smartphone in various ways. Specifically, they turned off the screen-lock feature, connected it to an unsecured Wi-Fi network that required no passwords, paired it with an unknown device via Bluetooth, enabled USB debugging, downloaded multiple unidentified apps and APKs, enabled device location services, and ensured that the device lacked the latest security update. These steps aimed to replicate real-world usage conditions and evaluate user interactions within a potentially compromised digital setting.

Procedure Participants were recruited through online platforms, universities, communities, word of mouth, and professional networks. Upon arrival, they were briefed on the study’s objectives and provided informed consent.

3.1. MOTIVATIONAL DRIVERS ANALYSIS

The study director then collected demographic information and introduced the study, and correspondingly, participants responded to multiple-choice questions about their approach to security concerns. Following this, participants completed the initial phase, which involved either viewing the serious or humorous animation or playing the game. Subsequently, participants were assigned three tasks to perform on an Android device running Android version 8.1.0, catering primarily to Android users. Participants unfamiliar with the Android operating system received instructions and assistance as needed. The first task involved installing a flashlight application using an unknown APK, while the second task required participants to elucidate the purposes of the permissions granted for the flashlight application. Lastly, participants were tasked with identifying potential privacy and security risks on the provided mobile device. For this task, nine possible privacy and security-related actions were considered as follows:

1. Setting a Screen-Lock: Secure the device with a pattern, code, or password to prevent unauthorized access.
2. Checking App Permissions: Review and manage the permissions granted to an installed flashlight application to control access to sensitive data and device functions.
3. Verifying USB Debugging and Developer Settings: Ensure that USB debugging mode and developer settings are disabled to prevent potential security vulnerabilities and unauthorized access.
4. Removing Unknown APK and Installed Apps: Delete any unfamiliar or suspicious APK files and applications installed on the device to mitigate the risk of malware or unauthorized access.
5. Examining the Wi-Fi Connection Status: Check the Wi-Fi connection status to identify potential security risks, such as unsecured networks or suspicious activity.
6. Inspecting the Bluetooth Connections: Verify the Bluetooth connections to detect unknown paired devices.
7. Reviewing Location Settings: Review and adjust location settings to ensure location data is shared securely and only with trusted applications.
8. Ensuring the Performance of Security Updates: Ensure that the device's operating system is up to date to address known vulnerabilities and protect against potential threats.

3.1. MOTIVATIONAL DRIVERS ANALYSIS

9. Accessing the Security Settings of the Smartphone: Navigate to the device’s security settings to configure additional security features.

While the first four actions were addressed in the videos or game content, the remaining actions were not mentioned. Participant performance in identifying these security-related actions was evaluated on a scale of 0 to 9, with higher scores indicating superior performance. Participants were not informed of the grading system for this task.

Participants In our study design, we engaged 21 participants (7 females, 13 males, and 1 individual who preferred not to disclose gender) with ages ranging from 20 to 45 years ($M = 28.76$, $SD = 5.29$) and did not receive any monetary compensation. They spanned educational backgrounds from bachelor’s degrees to PhDs or higher, and all reported ownership of a smartphone, utilizing their dominant hand during the test. A multiple-choice survey revealed that 80.9% of participants rely on websites and forums to address privacy and security concerns, while 38% utilize online videos and 19% consult friends for assistance. Notably, 47% of participants had previously encountered privacy and security-related videos. Furthermore, 24% admitted to never reading about mobile privacy and security, 57% rarely engaged in such reading, and 19% reported frequent engagement with the topic.

Empirical Findings

Our research findings highlight a significant increase in motivation and engagement regarding the topic within the game condition compared to alternative experimental setups. In the post-test questionnaire, participants were asked about their preference to view similar videos or participate in analogous games concerning mobile privacy and security and the frequency of such activities. Among those in the serious video group, 2 out of 7 individuals indicated they would not consume similar content, four would do so occasionally, and one would engage frequently. Within the humorous video group, 2 participants would abstain from similar videos, while five would view them sporadically. Conversely, in the game group, 4 participants expressed a willingness to play similar games occasionally, and three indicated they would do so frequently (see Figure 3.12).

Notable differences were observed between the game group and the other two cohorts in the task performance phase. The serious video viewers achieved an average score of 1.57 ($SD = 0.72$) per participant, while the humorous video group attained an average of 2.28 ($SD = 1.66$). In stark contrast, the game group significantly outperformed both, with participants scoring an average of 4.71 ($SD = 2.24$) (see Figure 3.12). Participants were also

3.1. MOTIVATIONAL DRIVERS ANALYSIS

instructed to install a flashlight app via an APK. In the serious video group, 6 participants chose APK installation, while one opted for Google Play. Similarly, in the humorous video group, five individuals installed the app via APK; one acknowledged associated risks, and another chose Google Play. Among the game group, 2 participants installed the app through APK, three acknowledged risks, and two opted for Google Play. The qualitative analysis involved scrutinizing participant comments and behaviors. In both the humorous video and game groups, all participants smiled at least once during viewing or gameplay, often remarking phrases such as “This is hilarious” or “It’s pretty funny, seems like me and my brother discussing.” Conversely, in the serious video group, 3 participants exhibited impatience towards the video’s conclusion, with comments like “It’s getting boring” or “How many minutes are left?” Interestingly, such behavior was absent in the game group. Moreover, two game group participants expressed a desire to replay the game to explore alternative outcomes, while none of the video groups expressed interest in revisiting the content.

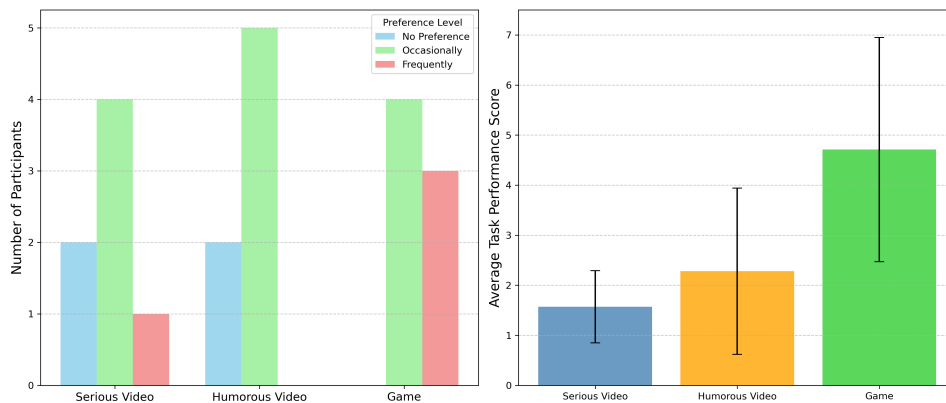


Figure 3.12: On the left, the chart shows engagement and re-engagement preferences, and on the right, it shows the task performance scores of three scenarios.

Discussion and Limitations

The objectives of our study were centered around two pivotal research questions: 1) To what extent does a humorous decision-making game influence user motivation to engage with mobile privacy and security? Moreover, 2) What are the potential effects of a humorous decision-making game on user awareness of mobile privacy and security issues? The findings from our analysis provide insightful answers to both questions, supported by quantitative data and qualitative feedback.

The engagement levels and willingness to re-engage with similar content,

3.1. MOTIVATIONAL DRIVERS ANALYSIS

particularly highlighted in the game group, suggest a positive influence of the humorous decision-making game on user motivation to engage with mobile privacy and security topics (Leah Zhang-Kennedy and Biddle, 2016). Participants in the game condition demonstrated a markedly higher inclination to engage with the subject matter, as evidenced by a substantial portion expressing a desire to play similar games often in the future. This enthusiasm was less evident among participants exposed to serious or humorous video content, indicating a unique motivational pull of interactive, game-based learning when infused with humor (Dormann et al., 2006; Lombardi, 2012).

The task performance scores further illuminate the potential effects of the humorous decision-making game on user awareness of mobile privacy and security issues. Participants in the game group outperformed those in the video groups, suggesting higher engagement and an enhanced understanding and awareness of the subject matter. This is a critical finding, indicating that the game effectively conveyed important privacy and security concepts, thereby raising participants' awareness. Moreover, the qualitative feedback underscores the role of humor in creating an enjoyable and memorable learning experience, which likely contributed to the observed increase in awareness, albeit with the necessary consideration of humor's cultural specificity (Denning et al., 2013).

Moreover, humor is arguably a highly complex cognitive activity, and processing even a simple joke can require language skills, theory of mind, symbolism, abstract thinking, and social perception (Polimeni and Reiss, 2006). Humor and assessing what is "funny" tend to be highly subjective, with interpretations varying across individuals. Due to its interdisciplinary nature, exploring different domains and areas is essential to understanding the underlying reasons behind why something is perceived as humorous. In our game, humor primarily relied on language-based elements. We incorporated unconventional and amusing comments to catch players off guard and enhance their enjoyment. However, such humor often hinges on specific cultural contexts, utilizing puns and cultural references. Consequently, there is a risk that jokes may not resonate or may even appear inappropriate to individuals lacking the necessary cultural background (Olsen and Mateas, 2009).

Despite these promising findings, it is crucial to acknowledge the study's limitations, including the small sample size, which may affect the generalizability of the results. Future research should aim to explore these questions with a larger and more diverse participant pool, further investigating the nuances of how humor influences engagement and awareness in educational content across different cultural contexts.

Acknowledgments

This section is based on the publication:

Nima Zargham, Mehrdad Bahrini, Georg Volkmar, Dirk Wenig, Karsten Sohr, and Rainer Malaka. 2019. *What Could Go Wrong? Raising Mobile Privacy and Security Awareness Through a Decision-Making Game*. In *In Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts (CHI PLAY '19 Extended Abstracts)*. Association for Computing Machinery. DOI: 10.1145/3341215.33562735

My contribution to this work: Conceptualization, data curation, formal analysis, investigation, methodology, project administration, resources, part of software development, validation, visualization, and contribution to all parts of the manuscript.

3.1.3 Study 3: Game Premise in Smart Home Security

Introduction and Background

In recent years, the widespread adoption of smart home technologies has transformed how people interact with and perceive their living spaces, particularly in terms of compatibility, ease of use, and usefulness (Shin et al., 2018). However, alongside the convenience and connectivity offered by these devices comes an escalating concern regarding privacy and security within smart home ecosystems (Lin and Bergmann, 2016; Mocrii et al., 2018). Many users overlook these issues, trusting in their preventive measures or believing they are not targets for cyber threats. Nevertheless, the significant risks identified by security experts, such as vulnerable devices and invasive data collection, are often underestimated by the average user, revealing a gap in awareness (Zeng et al., 2017). When choosing smart home devices, individuals frequently prioritize cost and interoperability over security, highlighting a need for better education on the importance of privacy and security measures. Enhancing user awareness about the risks associated with smart homes and encouraging informed decision-making can help mitigate these concerns, ensuring users can enjoy the benefits of smart technology without compromising their privacy and security (Zeng et al., 2017; Tabassum et al., 2019).

As stated in the previous sections, literature has explored strategies to address privacy and security concerns and lack of understanding. Educational games stand out for embedding incentives within engaging environments, offering potent educational tools that motivate and engage individuals. These games leverage entertainment to teach complex topics, fostering immersive learning experiences where users apply critical thinking skills (Hamari et al., 2016). The formal components of a game, such as its objectives, procedures, and mechanics, define the boundaries within which players can operate, effectively guiding and limiting their actions. This structural framework is essential for establishing the rules and goals of the game (Fullerton, 2014). However, beyond these formal elements, digital games are also deeply emotional experiences (Bopp et al., 2016). They engage players not just on a mechanical level but emotionally, challenging them to achieve their objectives while immersing them in the game's narrative and world (Oliver et al., 2016). Dramatic elements such as the game's premise, characters, and unfolding story enrich the gaming journey. They transform the game from a mere set of rules and objectives into a compelling narrative that captivates the player. This dual focus on the game's structure and emotional resonance ensures a more profound and engaging experience (Fullerton, 2014).

Premises and storytelling have been employed in various games to inves-

3.1. MOTIVATIONAL DRIVERS ANALYSIS

tigate their influence on player experience and behavior. Previous research has delved into different premises, including positive, negative, and neutral, each presenting unique narratives and objectives for players (Grudpan et al., 2019). Through experiments involving player experience surveys, game logs, observations, and interviews, these investigations have demonstrated that game premise significantly shapes player engagement and cooperative behavior. Negative premises, in particular, elicit more robust emotional responses and foster more cooperative actions among players. Similarly, researchers explored the effectiveness of serious games in math education, comparing different modes of gameplay in a math video game among students (Garneli et al., 2017). Divided into groups, students engaged with the game with storytelling, without storytelling, or by modifying it, while a control group used traditional paper-based methods. Although minor differences in learning performance were noted, significant variations in student attitudes towards learning through the video game were observed. Interestingly, the presence of storytelling did not affect performance. Moreover, students without storytelling preferred replaying the game using paper-based methods, suggesting that the effectiveness of storytelling may depend on its continuous evolution and might have a negative influence on the repetition of the practice.

To investigate game premises further, this study explores the impact of contrasting game narratives, good versus evil premises, on player motivation and learning outcomes within an educational game focused on smart home security. The core research question posed is: *Is there a measurable difference in motivation and learning outcomes between opposing game premises?* To address this question, we have developed a mobile game that offers two contrasting narratives: *Save My Home* and *Hacker War*. In *Save My Home*, players support the game character in securing his smart home against vulnerabilities, promoting the idea of protecting one's privacy. In *Hacker War*, players assist an anonymous hacker in exploiting smart home weaknesses for personal gain. We conducted a study employing a between-subjects design with 30 participants. Our analysis, grounded in responses from standardized questionnaires and performance metrics, yields preliminary findings that suggest no significant differences in either motivation or learning outcomes between the good and the evil game premises. This outcome indicates that, within the context of our educational game, the thematic framing of the narrative, whether aligned with good or evil, does not distinctly affect the educational impact on players. Despite the varying premises of the game, participants exhibited a keen interest in engaging with it. Both versions proved highly successful in motivating users to play and effectively educating them about the intricacies of smart home security.

Prototype Description

Concept The mobile game is meticulously crafted for diverse narratives, presenting players with two distinct and opposing premises: *Save My Home* and *Hacker War* (as depicted in Figure 3.13). In *Save My Home*, players engage with “Luca,” a character fraught with worry regarding the security of his smart home devices. Through an interactive narrative, players are tasked with aiding Luca by locating vulnerable devices and providing solutions to security challenges, embodying the good game premise of protecting one’s home and privacy. Conversely, *Hacker War* introduces players to an anonymous hacker lurking in the virtual streets, whose motives are driven by monetary gain and mischief. This nefarious character solicits the player’s assistance in orchestrating cyber-intrusions into neighboring homes, leveraging vulnerabilities in smart home devices for personal profit. Here, players face ethical dilemmas as they navigate the morally ambiguous terrain of cybercrime, blurring the lines between right and wrong. To enhance player immersion and narrative coherence, we meticulously tailored the background music and sound effects to complement the thematic essence of each premise. Despite the inherent contrast in narrative premises, both versions of the game adhere to a unified set of game procedures and mechanics.

Question Scenarios Players must answer ten questions about different smart devices in both game premises. We carefully selected these devices based on several factors. Firstly, we included a router as it forms the backbone of home networks. Secondly, considering the widespread use of smartphones for smart home settings, we deemed it necessary to feature them as smart devices. Additionally, we included six commonly encountered smart home devices, namely, a Smart TV, an IP Camera, a Smart Speaker, a Smart Thermostat, a Smart Lamp, and a Smart Plug. To add an element of intrigue, we introduced the last two devices: a Smart Home Firewall and a Smart Mowing Robot. Moreover, the questions selected for each device draw from privacy and security concerns outlined in recent research and articles (Zeng et al., 2017; Schiefer, 2015). Based on their recommendations, we selected ten questions that resonate with users’ everyday experiences. Following is an overview of each device and its corresponding question.

Router: Setting up routers can be difficult for non-tech-savvy users, and manuals often fail to provide enough information about the security risks of improper settings. Users struggle with configuring aspects like setting a secure admin password, choosing encryption protocols, and utilizing technologies such as Wi-Fi Protected Setup (WPS) (Kaaz et al., 2017). The question about routers addresses which setup can ensure a secure router.

3.1. MOTIVATIONAL DRIVERS ANALYSIS



Figure 3.13: The game consists of two opposing premises, the good (*Save My Home*) on the left and the evil (*Hacker War*) on the right.

Smartphone: Smartphones are ubiquitous and convenient for accessing and controlling smart home devices. Nevertheless, downloading fake, unofficial, or outdated applications can pose security risks to users' data and smart home devices (Sivaraman et al., 2016). Therefore, we ask players how an application could compromise the security of smart devices.

Smart TV: Modern TVs integrate operating systems and internet connections, offering enhanced services to users. However, this integration raises security concerns such as webcam hacking, tracking issues, and outdated software, which threaten user privacy (Bachy et al., 2019). Players are prompted to explore their understanding of such privacy and security issues in the question about smart TVs.

IP Camera: IP cameras facilitate rapid property monitoring, empowering users with instant oversight from any location. Nevertheless, their ease of setup and remote access via applications make them attractive targets for

3.1. MOTIVATIONAL DRIVERS ANALYSIS

hackers. Various security attacks pose serious threats to the video stream from IP cameras (Costin, 2016). Therefore, users are advised to implement security measures such as camera passwords, up-to-date applications, and video encryption to protect against these threats. This question investigates whether users understand the basic settings of a secured IP camera.

Smart Speaker: Smart assistants serve as the central hub of smart home systems, enabling users to control various devices. Nevertheless, recent discoveries reveal vulnerabilities that allow hackers to communicate with users' devices covertly, potentially leading to unauthorized actions (Carlini et al., 2016). Players are prompted to understand and protect against such attacks on their voice assistants within this question.

Smart Thermostat: Smart thermostats, controlled via smartphone apps, offer remote temperature adjustments but may compromise privacy due to their ability to learn users' habits. Hackers could exploit vulnerable thermostats to gather information about users' absence and plan break-ins (Fu et al., 2017). This question aims to raise awareness about the risks associated with smart thermostat usage.

Smart Lamp: Connecting smart lamps to home networks enables users to control them conveniently through various devices like smartphones or voice assistants. Nevertheless, this convenience comes with the risk of security vulnerabilities, which, if exploited by attackers, could lead to different adverse consequences. These may include health risks, such as disruptions to medical environments, and financial risks, like revenue loss in commercial settings due to compromised lighting systems (Morgner et al., 2016). This question provides users with recommendations to make informed decisions about purchasing secure smart lamps.

Smart Plug: Smart plugs enable remote monitoring and control of household appliances but may suffer from insecure communication protocols and lack of device authentication (Ling et al., 2017). Within this question, players are prompted to understand the importance of user profile creation and device authentication for smart plug security.

Smart Home Firewall: Smart home applications automate household tasks by connecting devices to the Internet, raising concerns about security vulnerabilities. Firewalls are crucial in protecting home networks from malicious attacks (Rehman and Gruhn, 2018). This question encourages players to familiarize themselves with firewalls and their role in smart home security.

Smart Mowing Robot: Advanced mowing robots use GPS and internet connectivity for efficient operation. This question explores the benefits of employing a VPN when a user is outside the home and seeks to connect

3.1. MOTIVATIONAL DRIVERS ANALYSIS

to the home network through a public Wi-Fi hotspot to manage a smart mowing robot (Molina et al., 2019).

Game Design The game addresses our research question by immersing users in a simulated smart home environment with the following core elements:

Introduction: Players are greeted by either the homeowner or an anonymous hacker avatar at the beginning of each session, both expressing their respective objectives through speech bubbles. These avatars also provide an overview of the game’s mechanics, with players initiating gameplay by tapping the doorbell in *Save My Home* or touching a window in *Hacker War*.

Finding of Devices: Players navigate through different rooms, each equipped with smart devices, and interact with them to answer security-related questions. The backyard serves as the final room in this exploration.

Progression: As players advance, they encounter ten questions related to the premises per play-through. Advancement within each room is contingent upon answering two questions. In *Save My Home*, correct answers enhance the security of Luca’s home, visually depicted by the transition of three red locks to green ones after each set of three correct answers. Similarly, in *Hacker War*, players face the same questions, albeit with different phrasing originating from the hacker, and earn a golden dollar sign after every three correct answers. Tapping on smart devices reveals the question screen, where all questions are presented as multiple-choice (see Figure 3.14).

Request to Support: Users can tap into supplementary knowledge resources within the game interface to grasp vulnerabilities and solutions for each device. Additionally, they can navigate general game controls via avatar buttons on the question screen. Tapping the information icon guides players to help screens with infographics, employing symbolic representations to convey concepts effectively (as depicted in Figure 3.15). In the design of the infographics, consistency is maintained across both versions. Each question includes distinct supporting knowledge isolated from other questions. Various symbols are strategically incorporated to convey concepts to players and enhance engagement. For instance, a unique caption corresponding to the associated device is assigned to each infographic. Additionally, symbols representing fundamental concepts about device configuration or physical forms are tailored for every device. To illustrate the concepts of security and insecurity, closed or open lock icons are consistently positioned alongside titles or symbols throughout all infographics.

Feedback of Answers: Players receive instant feedback based on their responses, confirming correct answers and offering informative explanations for incorrect ones. Players are ultimately acknowledged for their contributions

3.1. MOTIVATIONAL DRIVERS ANALYSIS

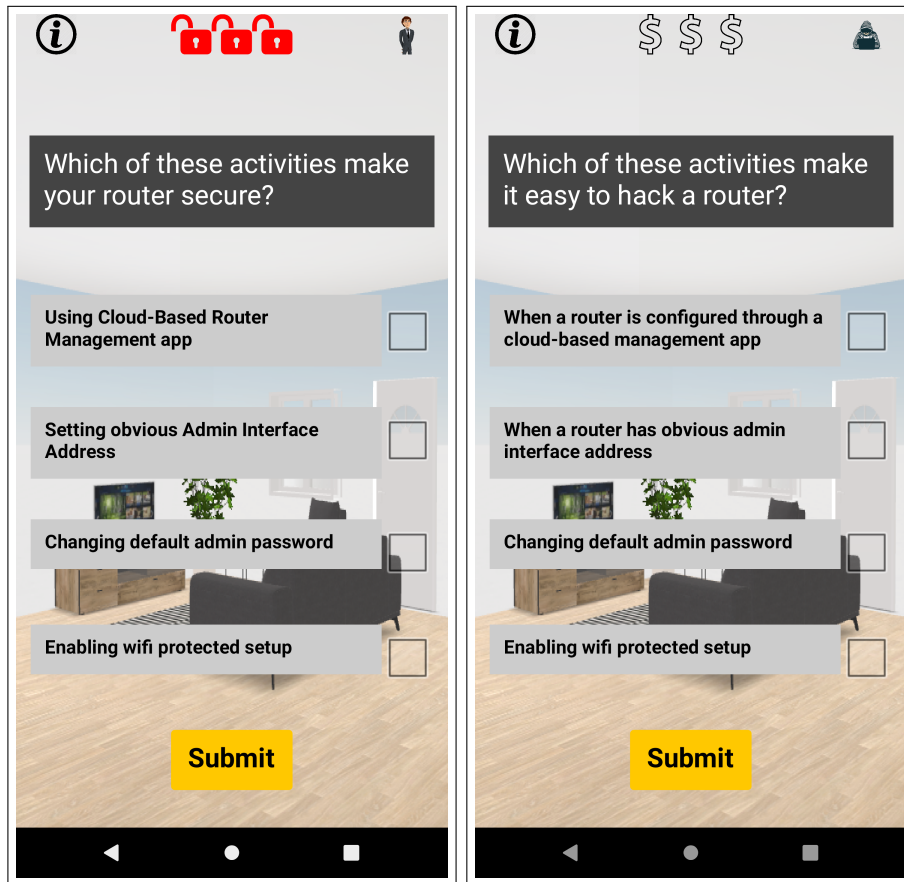


Figure 3.14: Touching the router reveals a corresponding question, with *Save My Home* featured on the left and *Hacker War* on the right.

based on the number of correct answers they provide by the end of the game.

User Evaluation

Study Design We used a between-subjects design to investigate the impact of contrasting game premises on player experiences. Thirty participants were equally divided into two groups, each exposed to either the *Save My Home* or *Hacker War* narrative. This setup enabled direct comparison while minimizing potential biases. The study was carried out in a laboratory environment on the university campus, ensuring consistency across sessions.

Materials In our evaluation, we utilized two prominent questionnaires to comprehensively assess the usability and player motivation within the game environment. Firstly, the System Usability Scale (SUS) (Brooke, 1996) was utilized to evaluate the game's usability, offering significant insights into user experience and interface efficacy. This questionnaire is widely recognized

3.1. MOTIVATIONAL DRIVERS ANALYSIS

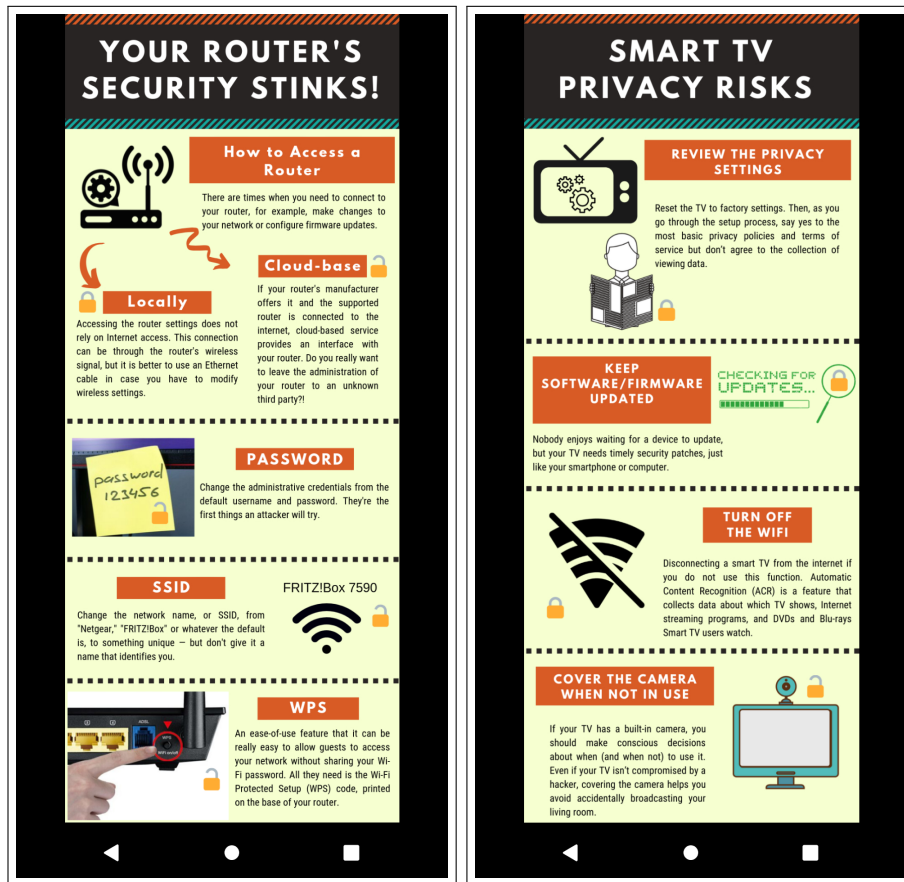


Figure 3.15: The information screens display infographics about smart home devices. The Router is featured on the left, while the Smart TV is on the right.

for its effectiveness in assessing perceived usability, regardless of whether it is utilized in a lab setting or a survey (Sauro and Lewis, 2016). It consists of ten items with varying tones, ranging from positive to negative, where respondents rate their agreement on a scale from “Strongly Disagree” to “Strongly Agree.” Secondly, the Intrinsic Motivation Inventory (IMI) (Ryan, 1982) was utilized to delve into the motivational aspects of players engaging with the game. The IMI, widely recognized in intrinsic motivation and self-regulation research (Tyack and Mekler, 2020), facilitated the examination of critical dimensions such as *Interest-Enjoyment*, *Perceived Competence* and *Effort-Importance*, thereby offering a nuanced understanding of the underlying motivational dynamics shaping player engagement.

We provided a Google Pixel 2 XL with a 6-inch display as a mobile device, ensuring consistent screen size and resolution for all participants. Prior to the study, this device was configured with standardized settings

3.1. MOTIVATIONAL DRIVERS ANALYSIS

to minimize variability in user experience. Participants interacted with the game application installed on this device, specifically optimized for mobile platforms, thereby enhancing the ecological validity of the study.

Procedure Participants were sourced via online platforms, universities, communities, word of mouth, social networks, and email. Upon arrival, they were briefed on the study’s objectives and provided informed consent. The study director delivered an introduction to the game and smart home security concerns. Participants then engaged in gameplay on the provided smartphone device, with play duration monitored by the interviewer. After completing gameplay, participants completed questionnaires covering demographic information and their experience with smart home devices. Additionally, they completed questionnaires to evaluate game usability and player motivation.

Participants The study included 30 participants, comprising 14 individuals with a college degree and 16 who completed high school. Among the participants, 15 identified as male and 15 as female. The age of participants ranged from 21 to 44 years, with an average age of 30.6 ($SD = 6.38$). They volunteered for the study and did not receive any monetary compensation.

Empirical Findings

Our study assessed the usability and intrinsic motivation of the games *Save My Home* and *Hacker War* among 30 participants divided equally into two groups. We utilized the System Usability Scale and the Intrinsic Motivation Inventory for our analysis, along with performance measures, including correct answers per session and playtime duration.

The SUS scores indicated high usability for both game versions. *Save My Home* achieved a mean SUS score of 84.2 ($SD = 8.99$), while *Hacker War* scored higher with a mean of 87.5 ($SD = 4.90$). An independent t-test revealed no significant difference in usability between the two games ($t(28) = 1.260$, $p = 0.218$, $Cohen'sd = 0.46$), indicating that both games were comparably user-friendly (see Figure 3.16).

Both groups consistently rated high across all sub-scales of the IMI Questionnaire. In the context of *Save My Home*, the *Interest-Enjoyment* sub-scale attained a score of 5.84 ($SD = 0.76$), *Perceived Competence* scored 5.67 ($SD = 0.4$), and *Effort-Importance* scored 5.3 ($SD = 0.70$). Conversely, *Hacker War* exhibited slightly higher ratings, with the *Interest-Enjoyment* sub-scale reaching 6.08 ($SD = 0.51$), *Perceived Competence* at 5.91 ($SD = 0.34$), and *Effort-Importance* at 5.8 ($SD = 0.92$). Statistical analysis revealed non-significant differences ($p > 0.05$ for all comparisons), suggesting that both games equally motivated players (see Figure 3.16).

3.1. MOTIVATIONAL DRIVERS ANALYSIS

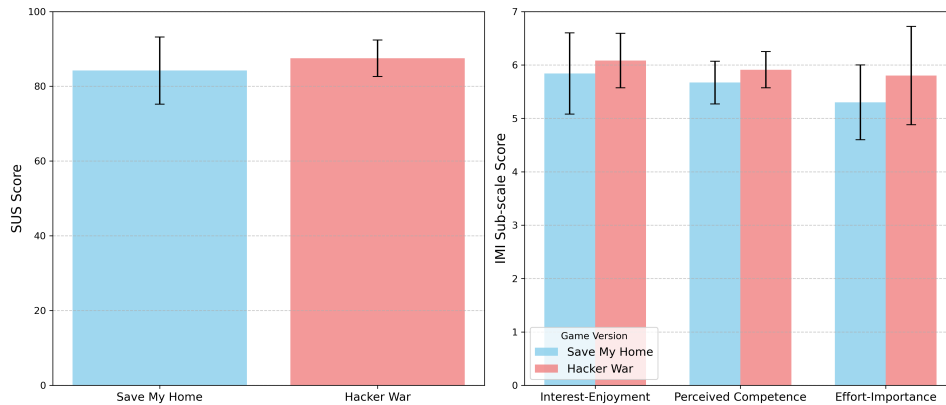


Figure 3.16: On the left are the SUS scores, and on the right are the IMI sub-scales scores of the opposite game premises.

Performance, measured by the number of correct answers per session, was nearly identical between the games, with *Save My Home* players averaging 6.9 ($SD = 0.13$) correct answers and *Hacker War* players averaging 7.1 ($SD = 0.17$) correct answers. The t-test indicated no significant difference in performance ($t(28) = -0.60$, $p = 0.555$, $Cohen'sd = -0.22$). The average playtime was also similar, with *Save My Home* at 14.6 minutes ($SD = 3.38$) and *Hacker War* at 14.93 minutes ($SD = 2.42$). Furthermore, the difference was not statistically significant ($t(28) = 0.31$, $p = 0.758$, $Cohen'sd = 0.11$).

Discussion and Limitations

The investigation into the impact of contrasting game premises on motivation, performance, and usability in an educational game about smart home security has yielded insightful findings. Our analysis, grounded in the responses from standardized questionnaires (SUS and IMI) and performance metrics, indicates that the game premise, whether oriented around themes of good or evil, does not significantly influence the motivational levels or learning outcomes of participants. This conclusion aligns with the usability and engagement metrics observed, suggesting a nuanced interplay between game design elements and educational effectiveness that transcends premise themes.

The absence of significant differences in motivational and performance outcomes between game premises prompts a reevaluation of the premise's role within educational games. Drawing upon Self-Determination Theory and Cognitive Load Theory (CLT) (Sweller, 1988), one might anticipate premise elements to significantly impact motivation and learning by fostering a sense of autonomy and minimizing extraneous cognitive load. However, our findings suggest that integrating educational content and game mechanics

3.1. MOTIVATIONAL DRIVERS ANALYSIS

may play a more substantial role in engaging users and facilitating learning outcomes, echoing the sentiments of previous works on the importance of game design in educational contexts (Gee, 2003; Prensky, 2003). The high usability ratings observed across both game versions further support the notion that effective game design, rather than premise complexity, contributes to a seamless and engaging user experience (Kortum and Peres, 2014). This perspective is reinforced by the IMI scores, particularly within the Effort-Importance sub-scale, which reflect a high level of enjoyment (Mekler et al., 2014) and commitment from players across game premises. These findings underscore the potential of well-designed educational games to foster learning and motivation independent of their premise context (Garneli et al., 2017). Moreover, positive ratings across all IMI sub-scales reinforce the idea that the educational content and interactive experience were well-received. Building upon these insights, the nuanced analysis of performance metrics and playtime data reveals a deeper insight into the player experience. Participants answered correctly approximately 70% of the time across both versions, and the similar amount of time spent playing each version suggests a well-balanced challenge-to-skill ratio. This equilibrium aligns with the flow framework, which posits that when a game’s challenges match the player’s abilities, the experience becomes more enjoyable and engaging (Sweetser and Wyeth, 2005).

While our study suggests that this kind of premise may not be the primary driver of learning outcomes in educational games, it does not diminish the potential value of dramatic elements in enhancing user engagement or supporting educational content. The literature on premise-based learning (Fullerton, 2014; Grudpan et al., 2019) highlights the capacity of stories to scaffold learning and anchor abstract concepts in meaningful contexts. Future research should thus explore the optimal integration of premise with game mechanics and educational content to maximize learning outcomes and player engagement.

Although there was a distinct contrast between the themes of good and evil in both versions, players assumed the role of a helpful character in both iterations. This sense of helpfulness could potentially convey a positive undertone regardless of the game version. Additionally, the distribution of game premises was randomized among participants. While the findings indicate equal playability for both versions, different premise versions may likely have varying effects on different player types. Given the insights gleaned from this preliminary study, exploring the relationship between player types and adaptive game premises within security education is necessary. Furthermore, employing an iterative design approach would be beneficial to ensure that players engage effectively with the narrative (Chen et al., 2019).

3.1. MOTIVATIONAL DRIVERS ANALYSIS

The interpretive framework of this study is greatly influenced by recognizing its inherent limitations, which affect the extent to which our findings can be broadly applied or generalized. This research engaged a relatively small and homogeneous participant pool within the specific educational domain of smart home security. Such specificity, while providing deep insights into this niche, inherently limits the breadth of applicability of our conclusions to broader educational contexts or diverse demographic and cultural groups. Therefore, it raises questions about the universal applicability of our findings, especially considering the diverse nature of educational game audiences.

In summary, our study contributes to the evolving discourse on the role of premise in educational games, suggesting a nuanced perspective where game design and educational integration play pivotal roles in shaping learning outcomes and player motivation. This insight challenges conventional beliefs about the primacy of premises and opens new avenues for research and development in educational game design.

Acknowledgments

This section is based on the publication:

Mehrdad Bahrini, Nima Zargham, Johannes Pfau, Stella Lemke, Karsten Sohr, and Rainer Malaka. 2020. *Good vs. Evil: Investigating the Effect of Game Premise in a Smart Home Security Educational Game*. In *Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play (CHI PLAY '20)*. Association for Computing Machinery. DOI: 10.1145/3383668.3419887

My contribution to this work: Conceptualization, data curation, formal analysis, investigation, methodology, project administration, resources, part of software development, supervision, validation, visualization, and contribution to all parts of the manuscript.

3.1.4 Key Insights of Motivational Drivers

Study 1: Gamified Android Security Settings

The integration of gamification in mobile security education significantly enhanced user engagement and comprehension, as demonstrated in Study 1. From the perspective of the FBM, gamified elements increased motivation by making the learning process more enjoyable and interactive. This heightened engagement aligns with SDT, which posits that intrinsic motivation is fostered when psychological needs for autonomy, competence, and relatedness are satisfied. By providing users with control over their learning and opportunities to master security tasks, the gamified application fulfilled these needs. The interactive and simplified tasks within the gamified application increased users' ability to comprehend complex security settings, aligning with FBM's focus on enhancing ability. Furthermore, the post-intervention improvement in users' awareness and understanding of mobile security settings could reflect an increase in self-efficacy. Successfully navigating gamified tasks boosted users' confidence in their ability to manage mobile security, reinforcing their competence and ability, as emphasized by SDT and FBM.

The study's initial questionnaire revealed a baseline awareness among users regarding mobile security settings and permissions, with younger users demonstrating higher initial knowledge. Despite this, the post-intervention analysis indicated a marked improvement in awareness and understanding, affirming that gamification could enhance comprehension even among those with prior knowledge. This supports the idea that gamified learning can significantly elevate users' engagement and understanding of security concepts by satisfying psychological needs and enhancing self-efficacy.

Study 2: Humorous Decision-Making Game on Mobile Security

This study explored the impact of humor on user engagement with mobile privacy and security topics. The humorous decision-making game served as a powerful intrinsic motivator, symbolized by both FBM and SDT. Humor made the learning process enjoyable, satisfying the need for relatedness by providing a shared, entertaining experience. The decision-making aspect of the game allowed users to exercise autonomy and competence, further enhancing intrinsic motivation. The task performance scores and qualitative feedback indicated that participants in the humorous game group demonstrated higher engagement and understanding of the subject matter. This performance improvement could be remembered as an empowerment of self-efficacy, as participants felt more capable of understanding and addressing mobile privacy and security issues. Moreover, humor in the game contributed

3.1. MOTIVATIONAL DRIVERS ANALYSIS

to creating a memorable and enjoyable learning experience, which likely enhanced participants' motivation and ability to retain and apply security concepts. The study also highlighted the cultural specificity of humor, noting that humor relying on language-based elements and cultural references might not resonate universally. This underscores the need for culturally sensitive content in educational games to ensure broad applicability and effectiveness.

Study 3: Game Premise in Smart Home Security

In this study, we investigated the impact of game premises on motivation, performance, and usability in an educational game related to smart home security. The findings revealed that the thematic premise (good vs. evil) did not significantly influence motivation or learning outcomes. Instead, the design elements of the game played a more critical role in maintaining user engagement and facilitating learning. This result aligns with the FBM, which emphasizes the importance of balancing motivation, ability, and prompts. High usability ratings and consistent performance metrics suggest that effective game design, which incorporates a balanced challenge-to-skill ratio, can enhance user motivation and ability, leading to better learning outcomes.

According to SDT, the study showed that well-designed educational games could satisfy users' needs for autonomy and competence, thereby fostering intrinsic motivation. The high usability ratings and positive IMI scores across both game versions indicate that the games met users' psychological needs, contributing to heightened enjoyment and commitment. The consistent performance across different game premises could also be interpreted as empowerment of self-efficacy, as participants felt confident in their ability to handle security tasks regardless of the game's narrative context. The study's nuanced analysis of performance metrics and playtime data revealed that participants answered approximately 70% of the time correctly across both versions, suggesting a well-balanced challenge-to-skill ratio. This equilibrium aligns with the flow framework, positing that when a game's challenges match the player's abilities, the experience becomes more enjoyable and engaging. While the premise did not significantly impact motivation, the study suggests that integrating educational content with effective game mechanics can substantially engage users and facilitate learning outcomes.

Integration of Theories and Findings

In conclusion, the findings from the three studies collectively underscore the importance of interactive, engaging, and well-designed educational tools. When effectively integrated into educational content, gamification can significantly enhance users' self-efficacy and intrinsic motivation, leading to an

3.1. MOTIVATIONAL DRIVERS ANALYSIS

informed behavior change and proactive engagement with mobile security practices and providing robust evidence to answer our first research question in this dissertation.

RQ1

How do game elements and narratives in ubiquitous and mobile applications enhance users' self-efficacy, boost intrinsic motivation, and promote the adoption of informed behaviors?

By addressing Research Question 1, we explore the pathway from self-efficacy to informed behavior through motivation within the model (see Figure 3.17). This question investigates how users' intrinsic motivation influences their engagement with privacy and security tasks. Through HCI approaches such as gamification, narrative elements, and humor-based interactions, we aimed to make security learning more engaging and appealing. This pathway highlights that fostering motivation can encourage proactive behaviors and support users in making informed decisions in privacy and security contexts.

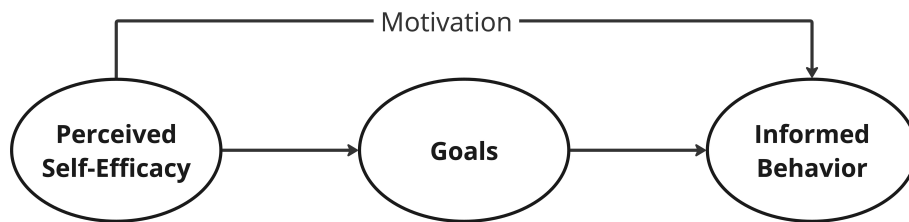


Figure 3.17: Pathway from self-efficacy to informed behavior via motivation

3.2 Individual Abilities Assessment

The second component in the Fogg Behavior Model is “ability.” This aspect assesses a person’s capacity to perform the behavior in question. Ability encompasses a variety of factors, including the individual’s skills, resources, knowledge, and any necessary conditions that facilitate or hinder their ability to carry out the behavior. It is not just about whether someone can physically or mentally execute the behavior but also about the ease or difficulty involved. Factors such as time, money, physical effort, and access to tools or information all play into determining the ability of an individual to perform a behavior. In the domain of mobile and ubiquitous applications, particularly concerning privacy and security tasks, “ability” encompasses more than mere technical proficiency. It includes the readiness and resources essential for successfully performing specific tasks, extending beyond time considerations or financial constraints. Emphasizing simplicity, transparency, and supportive decision-making processes becomes essential in empowering users to navigate security measures confidently and effectively. Meanwhile, mastery experience derived from self-efficacy significantly influences users’ ability to perform tasks, fostering a sense of capability and confidence in managing security challenges. We employed three distinct approaches to explore users’ abilities in mobile security, focusing on their capacity to perform behaviors within the context of privacy and security tasks in ubiquitous applications. In the first study, we investigate how infographics enhance users’ ability to comprehend and apply security measures in smart home settings. An educational game simulates real-world scenarios where players guide a virtual homeowner in protecting smart devices. Our findings underscored the role of infographics in simplifying complex concepts, thus enhancing users’ readiness to engage with smart home security effectively. The second study aims to boost users’ ability to grasp and manage permissions within mobile applications. Central to our approach is the development of “HappyPermi,” an interactive tool that visualizes data flows resulting from app permissions. The study highlights how enhancing transparency and usability in privacy tools strengthens users’ ability to navigate and control app permissions confidently. The third study introduces a user-friendly mobile security scanner to effectively enhance users’ ability to assess app permissions and privacy policies, which was built upon our previous research. Our approach integrates advanced static analysis capabilities from tools like MobSF while prioritizing simplicity and clarity in presenting actionable insights. In conclusion, these three studies underscore the importance of enhancing users’ abilities to navigate privacy and security challenges within mobile and ubiquitous applications.

3.2.1 Study 4: Infographics Enhance Game-Based Learning

Introduction and Background

As mentioned in the previous study, educational games have emerged as powerful tools for teaching, fostering engagement, creativity, and genuine learning experiences (Cone et al., 2007; Karoui et al., 2017; Dixon et al., 2019). They immerse players in simulated scenarios, prompting experiential learning and problem-solving via critical thinking (Chang and Hwang, 2019). In educational games, feedback provides players with essential information for their learning journey. In-game feedback aims to guide learners in enhancing their performance and boosting motivation and learning outcomes by furnishing them with insights into the accuracy of their responses (Shute, 2008). Johnson et al. (2017) classify feedback messages into two categories. *Outcome-oriented* feedback informs players about their progress or the accuracy of their responses (e.g., identifying correct answers and their explanation). *Process-oriented* feedback offers learning guidance and supporting knowledge regarding the processes and strategies employed to achieve the correct answers or actions in a game. Examples of process-oriented feedback include prompts and hints guiding learners toward the correct solutions. Many video games employ supporting knowledge to inform players about objectives and guide them through gameplay. Leveraging this form of process-oriented feedback could enhance the efficacy of educational games (Plass, 2020).

Players can receive supporting knowledge through multiple mediums like text, images, audio, and video, offering clear guidance during their interaction with the game (Johnson et al., 2017). Among these, infographics stand out as techniques that visually enrich individuals' understanding and interpretation of information (Krum, 2013) and comprise a blend of text, images, charts, and icons (Haan et al., 2018). Infographics represent a dynamic tool for distilling complex information into a visual narrative and constitute an effective way of communicating data to decision-makers who need high-quality information in a bite-sized and easily accessible form (Lankow et al., 2012). Studies underscore the inclusivity of infographics, blending various modes of communication to reach a wider audience, irrespective of their learning abilities. Through combinations of text, illustrations, and images, infographics stimulate readers to absorb and retain information more effectively (Bateman et al., 2010; Lyra et al., 2016).

In this study, we employ infographics to convey security information to players in a smart home educational game designed to empower users with a deeper understanding of security issues and emerging risks. Players tackle a dynamic learning journey by guiding a virtual homeowner in protecting his

3.2. INDIVIDUAL ABILITIES ASSESSMENT

smart home devices against potential threats. They explore various rooms, identifying potential smart home devices and engaging with questions about each device’s security features. Throughout the game, players can access security-supporting knowledge for each device, presented in two versions: either text-based or infographics. In our study, we employ a between-subjects design to compare both approaches and address the research question: *To what extent can infographics enrich the learning experience and efficacy of an educational game centered on smart home security?* Our findings illuminate a significant amount of correct responses and the perceived competence of players who got the infographics during playtime. This study contributes to educational serious games by demonstrating their ability to enhance learning outcomes and encourage self-education among players.

Prototype Description

Concept The structures and mechanisms of this mobile game are replicated from the *Save My Home* prototype used in study 3. The game was designed for mobile platforms and featured a narrative centered around an ordinary person named “Luca.” At the outset, the player encounters Luca outside his home, expressing concern about the security of his smart home devices due to his limited understanding of their configuration. Luca requests the player’s assistance searching for devices and answering related questions. Upon ringing the doorbell, the player enters Luca’s home, which comprises five rooms, each housing two smart devices. As the player moves through the rooms, a mellow background music accompanies their exploration. Tapping on each device reveals a question, with an additional hint button available to provide supporting knowledge for answering. Following each answer submission, the game evaluates the response and provides feedback via a notification. Finally, the player receives awards based on the number of correct answers at the game’s conclusion.

Design The smart home devices and associated questions in the current prototype are identical to those in study 3, specifically the *Save My Home* prototype. Its core components consist of the following building blocks:

Introduction: The Luca avatar welcomes players at the start of each session and communicates his respective objective through a speech bubble. Luca also provides an overview of the game’s mechanics, with players initiating gameplay by tapping the doorbell in *Save My Home*.

Finding of Devices: Players navigate through various rooms containing smart devices and interact with them to respond to security-related questions. The backyard serves as the final room in this exploration.

Progression: As players progress, they meet ten questions. Advancement

3.2. INDIVIDUAL ABILITIES ASSESSMENT

within each room is based on answering two questions. Correct answers enhance the security of Luca's home, visually represented by the transition of three red locks to green ones after each set of three correct answers. Tapping on smart devices reveals the question screen, where all questions are presented as multiple-choice.

Supporting Knowledge: When the player clicks on the information icon, they are directed to the supporting knowledge screen. Text or infographics are displayed to evaluate the impact of text versus infographics on player motivation and performance (see Figure 3.18). The content provided for supporting knowledge remains consistent across both versions, with each question accompanied by unique supporting knowledge. Infographics incorporate various symbols to convey concepts and captivate player attention. A tailored caption is chosen for each infographic based on the associated device, complemented by symbols designed to illustrate basic concepts about device configuration or physical attributes. Closed or open lock icons are employed alongside titles or symbols to denote security status, ensuring uniformity across all infographics.

Answer Feedback: Players receive immediate feedback based on their responses, with correct answers confirmed and informative explanations provided for incorrect ones. Ultimately, players are recognized for their contributions based on the number of correct answers provided by the end of the game.

User Evaluation

Study Design The study aimed to evaluate how infographics, employed as supporting knowledge, could enhance the learning experience of users within an educational game focused on smart home security. We conducted a between-subjects user study involving 60 participants, assessing the effectiveness of different presentation formats, including text-based and infographic-based approaches. In the *Text-Group*, participants received descriptive textual background information in the supporting knowledge screen, resembling conventional security news or updates. Conversely, participants in the *Infographics-Group* were provided with visualized information using infographics, incorporating text, images, charts, and icons.

Materials The study comprised a series of questionnaires administered to participants post-game completion. Firstly, demographic data, including age and gender. Secondly, the System Usability Scale (SUS) (Brooke, 1996) was employed to evaluate the game's usability. Additionally, participants' motivation levels were assessed using the Intrinsic Motivation Inventory (IMI) (Ryan, 1982) on a 7-point Likert scale, encompassing dimensions

3.2. INDIVIDUAL ABILITIES ASSESSMENT

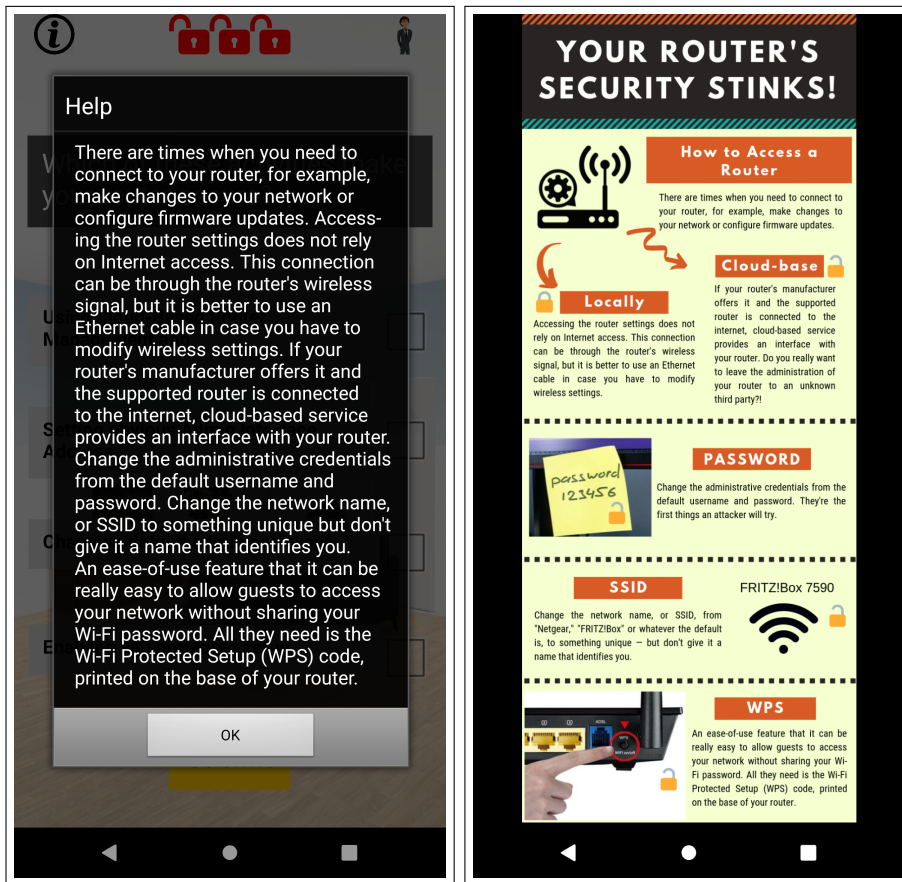


Figure 3.18: The information screens present security information about smart home devices in two formats: text-based (shown on the left) for one group of players and infographics (displayed on the right) for another.

such as Interest-Enjoyment, Perceived Competence, and Effort-Importance. Finally, we asked participants to elicit insights into whether they possessed smart home devices and, if so, what types they owned. We conducted laboratory study sessions on the university campus, with one participant per session and a duration of 30 to 45 minutes. Each group was provided a Google Pixel 2 XL mobile device featuring a 6-inch display to experience the game version.

Procedure The study began with obtaining consent from participants, followed by an introductory briefing by the interviewer regarding the game mechanics and security aspects of smart home devices. Subsequently, participants engaged with the game, navigating through rooms and answering related questions while their play duration was recorded. Upon completing the game, participants proceeded to complete the questionnaires.

3.2. INDIVIDUAL ABILITIES ASSESSMENT

Participants We employed a quota sampling approach to recruit participants, leveraging mailing lists, social networks, and word-of-mouth, specifically targeting smart home users. Participation was voluntary and uncompensated. The *Text-Group* comprised 30 participants, with educational backgrounds reflecting nine individuals holding college degrees and 21 completing high school. Gender distribution was balanced, with 15 participants identifying as male and 15 as female. Age diversity was captured, from 18 to 54 years, with an average age of 28.9 ($SD = 10.25$). The *Infographics-Group*, consisting of 30 participants, mirrored the educational and gender distribution of the first group, with 14 participants holding college degrees and 16 completing high school, and an equal split of 15 males and 15 females. The age range varied from 21 to 44 years, with an average age of 30.6 ($SD = 6.38$).

Empirical Findings

Text-Group After playing the game, all participants in the *Text-Group* reported owning at least one smart device in their homes, with smartphones being universally possessed among them. The most commonly owned devices in this group were Smart TVs (25), followed by Smart Lamps (12) and Smart Speakers (9). Additionally, participants in the *Text-Group* reported ownership of Smart Plugs (3), IP Cameras (2), and Smart Thermostats (2). However, no participants in this group owned Smart Mowing Robots or Smart Firewalls.

The calculated mean value of the SUS score for the *Text-Group* was 89.9 ($SD = 14.70$). The IMI score of *Interest-Enjoyment* was rated 6.2 ($SD = 0.78$), *Perceived Competence* score was rated 3.4 ($SD = 0.1$), and *Effort-Importance* score was rated 5.6 ($SD = 0.97$). The average of correct answers was 2.4 ($SD = 0.17$), and the average playtime was 9.27 minutes ($SD = 1.36$) (see Figure 3.19).

Infographics-Group In the *Infographics-Group*, participants were also surveyed regarding their ownership of smart home devices. The findings revealed that all participants in this group possessed at least one smart device in their homes, with smartphones being universally owned among them. Upon further examination, it was observed that the most commonly owned devices in this group were Smart TVs (29), closely followed by Smart Lamps (10) and Smart Speakers (10). Additionally, smaller numbers of participants reported owning Smart Plugs (2), IP Cameras (3), and Smart Thermostats (1). Interestingly, no participants in the *Infographics-Group* reported owning Smart Mowing Robots or Smart Firewalls.

This group exhibited a mean SUS score of 84.0 ($SD = 7.32$). The IMI score of *Interest-Enjoyment* was rated 6.0 ($SD = 0.65$), *Perceived Competence*

3.2. INDIVIDUAL ABILITIES ASSESSMENT

score was rated 5.8 ($SD = 0.39$), and *Effort-Importance* score was rated 5.6 ($SD = 0.84$). The average of correct answers was 7.3 ($SD = 0.15$), and the average play time was 14.77 minutes ($SD = 2.89$) (see Figure 3.19).

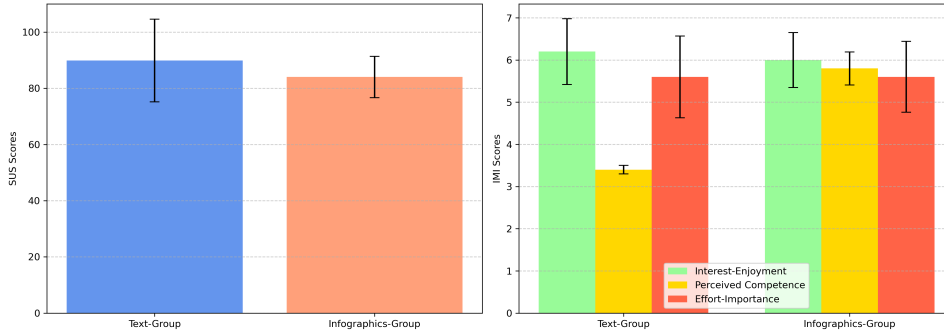


Figure 3.19: On the left are the SUS scores, and on the right are the IMI sub-scales scores of two groups.

Comparisons The independent t-test results indicated significant differences between the groups. Participants in the *Infographics-Group* ($M = 7.3$, $SD = 1.15$), who received supporting knowledge in the form of infographics, demonstrated significantly better average correct answers ($t(58) = 11.734$, $p < .001$, Cohen's $d = 3.030$) compared to participants in the *Text-Group* ($M = 2.4$, $SD = 1.70$). Moreover, the *Infographics-Group* exhibited a significantly higher average playing time ($M = 14.77$, $SD = 2.89$) than the *Text-Group* ($M = 9.27$, $SD = 1.36$) ($t(58) = 9.441$, $p < .001$, Cohen's $d = 2.438$). Regarding IMI *Perceived Competence* scores, the *Infographics-Group* ($M = 5.8$, $SD = 0.39$) significantly outperformed the *Text-Group* ($M = 3.4$, $SD = 0.1$) ($t(58) = 12.456$, $p < .001$, Cohen's $d = 3.216$) (see Figure 3.20).

However, no significant differences were observed in *Interest-Enjoyment* ($t(58) = 1.317$, $p = 0.193$) and *Effort-Importance* ($t(58) = 0.237$, $p = 0.814$) scores between the two groups. Similarly, no significant differences in SUS scores were found between the *Infographics-Group* and the *Text-Group* ($t(58) = 1.364$, $p = 0.178$).

Discussion and Limitations

This study aimed to investigate how *Process-oriented* feedback presented in the form of infographics influences the performance of players in an educational game focused on smart home security. Results from the user study indicate that the game has a distinct usability and players enjoyed playing it, regardless of the difference in supporting knowledge. Furthermore, our findings showed high intrinsic motivation and engagement with the topic

3.2. INDIVIDUAL ABILITIES ASSESSMENT

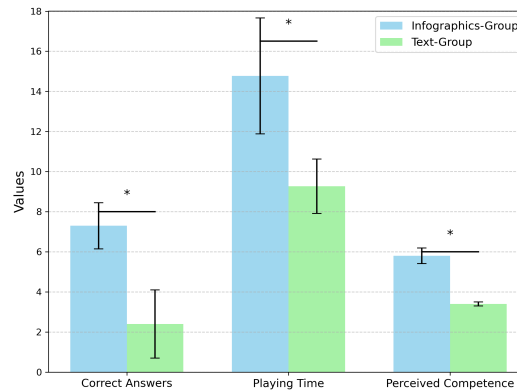


Figure 3.20: The chart illustrates significant differences between the *Infographics-Group* and *Text-Group* regarding Correct Answers, Playing Time, and *Perceived Competence*. The *Infographics-Group* shows higher performance in all three measures.

among the people who played the game. Participants were eager to spend time playing the game in both groups. Players who received infographics as supporting knowledge demonstrated significantly higher performance in correctly answering questions compared to those who received textual feedback. This finding aligns with previous research suggesting that infographics can enhance awareness and retention of complex information by providing visual aids alongside textual content (Krum, 2013; Lyra et al., 2016). The dynamic nature of infographics, blending text, images, and charts, appears to facilitate a deeper understanding of the subject matter, particularly in scenarios where the topic is inherently intricate (Haan et al., 2018). Moreover, the observed increase in players' *Perceived Competence* following exposure to infographics underscores the motivational benefits associated with this form of feedback. As noted by Johnson et al. (2017), feedback in educational games serves not only to inform players of their progress but also to bolster their motivation and learning outcomes. Infographics, with their visually engaging format, seem to instill a sense of mastery and empowerment among individuals, encouraging them to further engage with the learning content and tackle challenges with confidence (Alrwele, 2017). Additionally, the IMI (*Effort-Importance*) scores indicate that players made efforts to answer questions in both groups. However, they achieved significantly lower performance in the *Text-Group*. Despite participants' willingness to engage with questions in both game versions, infographics yielded better results. This suggests that an increase in correct answers may not solely be attributed to differences in motivation but could also indicate an actual improvement in technical understanding.

3.2. INDIVIDUAL ABILITIES ASSESSMENT

While these findings mark progress in exploring the use of infographics as supporting knowledge in smart home security, some limitations remain to address. The experiment assessed performance in an educational game environment under two feedback interventions. Future research should explore alternative instructional support types and assess timing effects, like near real-time or delayed feedback, to fully understand the impact of different approaches in game-based learning. Despite significant performance differences between conditions, there was no direct measurement of long-term learning post-training. Moreover, individual differences such as gaming experience, learning style, and background knowledge could have influenced players' performance. Although the question criteria were carefully calibrated, they were limited to 10 items, potentially lacking specificity. It is important to note that the comprehension of question wording and sentences could influence results. From player performances and post-experiment evaluations, we observed varying perceptions of question difficulty among participants. Hence, we recommend designing questions and structuring levels based on the complexity and difficulty of the topics. Finally, the game was classified as a straightforward quiz-genre type. It would be advantageous to investigate alternative game genres to enhance the comprehensiveness of the findings.

Acknowledgments

This section is based on the publication:

Mehrdad Bahrini, Nima Zargham, Johannes Pfau, Stella Lemke, Karsten Sohr, and Rainer Malaka. 2020. *Enhancing Game-Based Learning Through Infographics in the Context of Smart Home Security*. In *Entertainment Computing – ICEC (ICEC 2020)*. Springer, Cham. DOI: 10.1007/978-3-030-65736-9_2

My contribution to this work: Conceptualization, data curation, formal analysis, investigation, methodology, project administration, resources, part of software development, supervision, validation, visualization, and contribution to all parts of the manuscript.

3.2.2 Study 5: Critical Data Flows in Mobile Applications

Introduction and Background

We have employed gaming in our recent studies as a powerful intervention technique to bolster users' motivation and foster active learning and engagement with crucial privacy and security concepts about mobile devices and smart homes. This approach is particularly helpful for users to comprehend and practice security measures prior to selecting and installing applications. For instance, within a simulated game environment, users can interact with gamified features to comprehend how granting specific permissions could potentially allow apps to access unauthorized data (Bahrini et al., 2019a).

Additionally, researchers investigated a different approach, focusing on supporting users in managing their privacy and security settings for apps already installed on their devices to improve mobile users' privacy awareness and knowledge (Gerber et al., 2018). While maintaining game elements, they developed an Android-based application called "FoxIT" that offers an initial analysis of smartphone settings and app permissions upon first use, categorizing apps based on their permission requests to highlight potential privacy threats swiftly. Users can access detailed information about each app's permissions, including total requests and criticality categorization, with direct access to permission management settings. The FoxIT app also features comprehensive lessons across various courses covering privacy laws, online service settings, encryption, and passwords, with quizzes for knowledge assessment. Field studies were conducted with participants using the FoxIT app on their own smartphones. The results indicated that the app led to higher knowledge about privacy-related topics and increased privacy awareness among participants. They reported improvements in privacy conditions on their smartphones and actively sought privacy information, prompting others to protect their data. Furthermore, one week after the study ended, participants' knowledge of privacy increased, suggesting the potential for long-term effects (Gerber et al., 2018).

While such approaches show promise, they require a deeper understanding of mobile application behavior. Existing literature has explored technical methodologies to address the concerns surrounding unauthorized access or misuse of personal and device data via smartphone permission mechanisms. They have focused on detecting malware and preventing data leaks, typically categorized into static, dynamic, or hybrid analysis, which combines static and dynamic methods (Tam et al., 2017). Static analysis involves reverse engineering an application to analyze its code or binary code for malicious habits. Examples of static analysis methods include examining code struc-

3.2. INDIVIDUAL ABILITIES ASSESSMENT

tures, data flows, function calls, and patterns for vulnerabilities (Pan et al., 2020). Conversely, dynamic analysis entails executing the application in a controlled environment, such as an emulator or a real device, to observe its behavior. This method aims to trace the application’s actions and interactions during runtime to identify malicious behavior or suspicious activities (Tam et al., 2017). Several dynamic approaches have been introduced for malware detection, focusing on monitoring system calls, network traffic, and other runtime behaviors indicative of malicious intent (Gajrani et al., 2020).

Addressing users’ concerns about privacy on smartphones, Balebako et al. (2013) designed and evaluated the “Privacy Leaks” Android-based application, informing users about data sharing by smartphone applications. The goal was to enhance users’ awareness of privacy leakages and provide them with control over their data sharing. The study comprised a lab-based evaluation conducted in three parts. Initially, participants played two smartphone games and evaluated them for recommendation to a friend or family member. Subsequently, they engaged in questioning regarding their comprehension of data sharing. In the subsequent phase, participants played the same games with Privacy Leaks installed, accessing visualizations of data sharing and reassessing their recommendations. Their understanding of data leakages was evaluated accordingly. Finally, participants were interviewed regarding their desire to control data sharing and their perceptions of Privacy Leaks’ usability. Utilizing static analysis methods via the TaintDroid platform (Enck et al., 2014), the Privacy Leaks app detected data-sharing instances and provided users with real-time notifications. Results revealed a significant increase in participants’ awareness of data sharing post-Privacy Leaks usage, with visualizations facilitating comprehension of data sharing frequency and destinations. Participants expressed a desire for more control over data sharing, particularly in specific contexts. The study underscores the importance of transparency and user control in addressing smartphone privacy concerns, suggesting avenues for further research and improvement of the Privacy Leaks application.

Similarly, researchers employed technical methodologies such as static analysis and network traffic monitoring to investigate the efficacy of conveying data collection activities for privacy-related decisions, focusing on the selection and installation of smartphone applications (Van Kleek et al., 2017). They explored whether contextualizing these activities against other apps and presenting indicators, including Sankey diagrams, would influence decisions during the app choice process. Their thorough analysis revealed that providing more varied information, including detailed indicators such as the types of data collected, the organizations involved, and the purposes for

3.2. INDIVIDUAL ABILITIES ASSESSMENT

data usage, influenced decision-making strategies. Users considered factors such as the number of data destinations and the reputation of organizations involved when making their choices. The findings suggest that such communication, backed by rigorous technical analysis and enriched with detailed indicators, significantly impacts decision-making processes, potentially resulting in different outcomes compared to situations where such information is unavailable.

Building upon these insights, this work focuses on enhancing user understanding and control within the Android application permission system by introducing *HappyPermi*, an intuitive application designed to visualize smartphone data flows resulting from a static analysis. Through leveraging users' private information, *HappyPermi* aims to foster greater user vigilance when granting permissions, offering streamlined features that simplify the often complex permission landscape. Our development journey was guided by two pivotal research questions: 1) *How can interactive tools assist users in comprehending the implications of permission requests on their private data?* and 2) *To what extent are users aware of the destinations of their data transmissions?*

We conducted a laboratory study employing a between-subjects design involving 20 participants. Our findings suggest that *HappyPermi* has the potential to elevate user awareness of Android permissions, prompting users to scrutinize permission requests more discerningly. This increased awareness empowers users to make informed decisions about the installation or usage of applications. Our work contributes to the field by striking a balance between usability and security within the Android permission framework and promoting a user-centered approach that prioritizes users' motivation to engage in security and privacy-related tasks.

Prototype Description

Concept *HappyPermi* is an innovative Android application designed to empower users with comprehensive insights into the permissions and data flows of installed applications on a smartphone. At its core, the concept of *HappyPermi* revolves around providing users with the means to analyze the permissions granted to various applications on devices, thereby allowing them to understand the destination and purpose of personal data. By visualizing data flows and presenting detailed information about each permission, *HappyPermi* aims to guide users in making informed decisions about granting permissions, ultimately enhancing their privacy and security on Android devices.

3.2. INDIVIDUAL ABILITIES ASSESSMENT

Design Within the design of *HappyPermi*, we have carefully crafted two distinct versions: *HappyPermi* and *HappyPermi+Flow*, each offering unique functionalities to empower individuals to manage app permissions effectively. Both versions share a common workflow, initiated by a user selecting the “AnalyzeApp” button, triggering an in-depth examination of all installed applications on a smartphone (see Figure 3.21). This action prompts *HappyPermi* to compile a comprehensive list of applications, presenting the user with essential details such as icons, names, and installation dates for each app (refer to Figure 3.21).

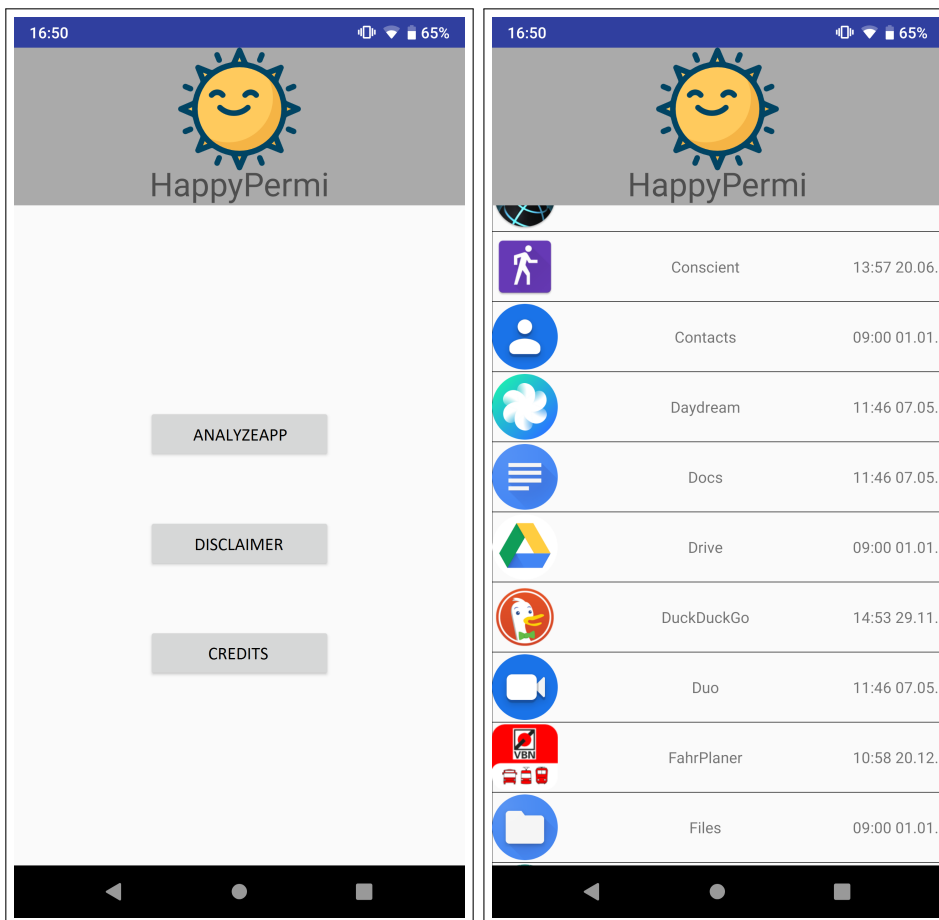


Figure 3.21: On the left is the *HappyPermi* start screen. After pushing the “AnalyzeApp” button, on the right, it presents a list of all installed applications with the icon, name, and installation date. This screen is the main feature in both versions. (The *HappyPermi* icon is credited to Dimitry Mirolubov on www.flaticon.com)

Upon selecting a specific application from the list, the individual seamlessly transitions to a detailed view where granted permissions are visually

3.2. INDIVIDUAL ABILITIES ASSESSMENT

represented (see Figure 3.22). For instance, the “Read Contacts” permission exposes relevant details about a contact’s name, associated phone number, and storage location on the phone or cloud. Conversely, “Read External Storage” reveals a private image stored on the smartphone. Additionally, if the “Access Location” permission is granted, the current location of the smartphone will be displayed.

Notably, our design emphasizes evaluating the FahrPlaner⁵ application, a prime example illustrating the significance of various permissions. The FahrPlaner app is a well-known mobile application assisting passengers in public transportation and individual travel throughout Germany. It offers features such as route planning, schedules, and stop information to assist users in efficiently planning their journeys. This app utilizes location and contacts permissions for route planning and camera and storage permissions for image customization, highlighting the real-world implications of permission management within *HappyPermi*.

After engaging with the visual presentation of permissions in the initial version of *HappyPermi*, the user is guided to FahrPlaner’s permissions settings within the Android operating system, facilitating informed customization based on individual preferences. Conversely, the *HappyPermi+Flow* version enriches the user experience by incorporating insights from an external analysis tool called MobSF⁶ to alert the user about potential data transmission risks via destination URLs as depicted in Figure 3.22.

MobSF, short for Mobile Security Framework, is a universal security research platform tailored for mobile applications. Its functionalities extend across diverse use cases, encompassing mobile application security, penetration testing, malware analysis, and privacy examination. We employed MobSF on a PC to perform a static analysis of FahrPlaner, identifying all destination URLs utilized by the application. These URLs are then integrated into the *HappyPermi+Flow* version, enriching its capabilities. This improved transparency approach to data privacy management helps ensure that users are equipped with comprehensive information to make informed decisions (Liccardi et al., 2014). Like the previous version, by clicking “Continue”, the user is directed to the permissions settings in the Android operating system.

⁵<https://www.vbn.de/service/fahrplaner-app>

⁶<https://github.com/MobSF/Mobile-Security-Framework-MobSF>

3.2. INDIVIDUAL ABILITIES ASSESSMENT

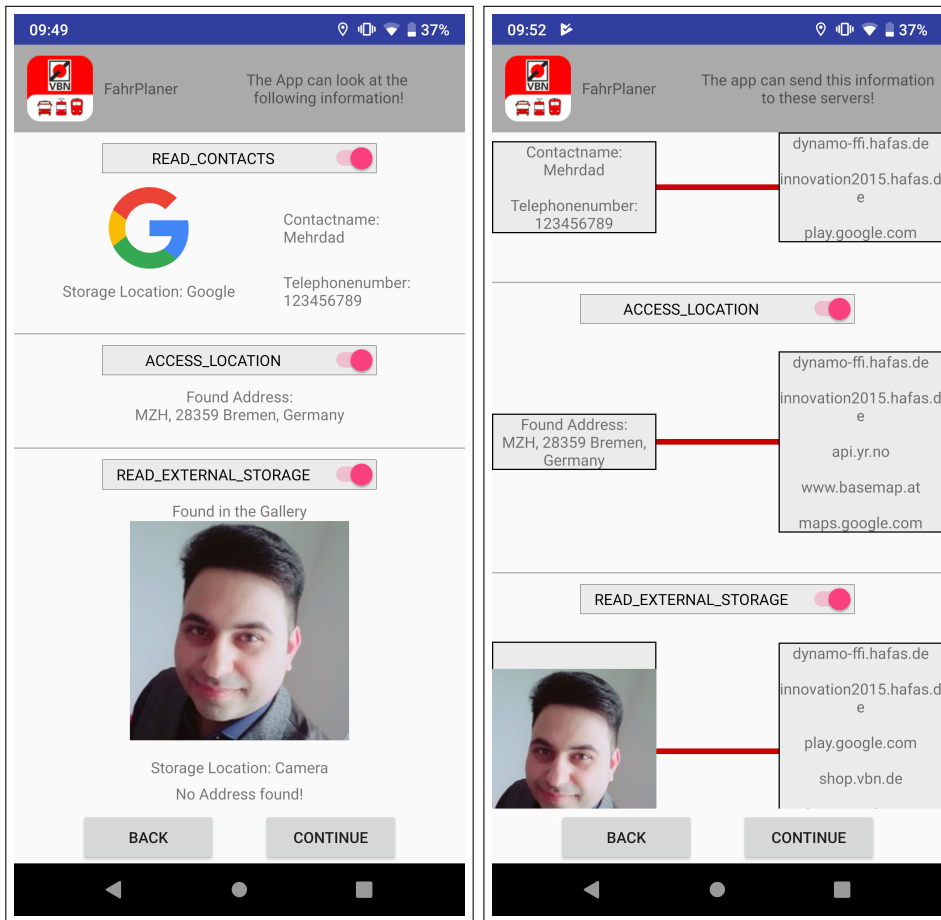


Figure 3.22: On the left, the *HappyPermi* Permission Screen provides visual insights into permissions granted to the *FahrPlaner* application, illuminating potential access to user data. This essential feature is central to both versions. On the right, *HappyPermi+Flow* offers a deeper dive, showcasing user data accessible through permissions and presenting accessible user data alongside corresponding URLs. This screen is exclusive to the *HappyPermi+Flow* version.

User Evaluation

Study Design We conducted our study in a laboratory environment, employing a between-subjects design to evaluate the effectiveness of two iterations of *HappyPermi*. A total of 20 participants, evenly distributed into two groups of 10 each, took part in the study.

Materials In our study design, we incorporate the System Usability Scale (SUS) and the Self-Assessment Manikin (SAM) questionnaires to comprehensively gather user feedback across different dimensions of experience tailored for each participant group. The SUS provides a reliable, quick assess-

3.2. INDIVIDUAL ABILITIES ASSESSMENT

ment of the usability aspects of the design. In contrast, the Self-Assessment Manikin is a nine-point scale evaluation method designed to measure three distinct emotional domains: Pleasure, Arousal, and Dominance (Bradley and Lang, 1994). This innovative tool aids users in accurately describing their emotions by using five distinct images for each domain, enhancing the clarity of their responses. For the domain of Pleasure, the SAM utilizes imagery ranging from a smiling, happy figure to a frowning, unhappy figure, effectively capturing the spectrum of user satisfaction and enjoyment, as shown in Figure 3.23.

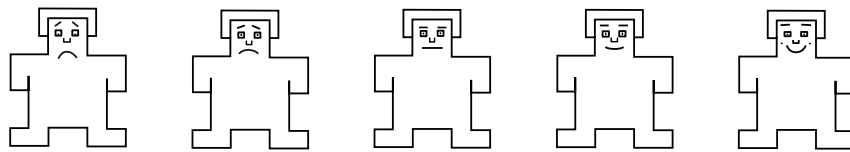


Figure 3.23: The Pleasure dimension of the SAM questionnaire depicts the progression from displeasure to pleasure. Figures range from an unhappy figure on the left to a happy figure on the right.

In assessing Arousal, the SAM spans from an image of a figure appearing sleepy with eyes closed, signifying low Arousal, to a figure with eyes wide open, indicating high excitement or alertness (see Figure 3.24).

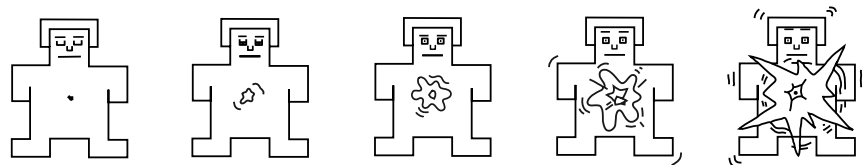


Figure 3.24: The Arousal dimension of the SAM questionnaire illustrates the progression from low to high arousal. The figures range from a calm, relaxed figure on the left to a highly excited and energized figure on the right.

The Dominance dimension employs imagery varying from a very small figure, symbolizing feelings of being controlled or submissive, to a significantly larger figure, denoting feelings of being in control or possessing a powerful presence (see Figure 3.25). Since its inception, SAM has been extensively employed in numerous psychophysiological studies, proving its effectiveness and reliability in capturing nuanced emotional responses in diverse research settings (Morris, 1995).

Moreover, we proposed targeted questions to gauge participants' understanding and management of mobile application permissions, particularly concerning the FahrPlaner app. These questions explored various facets of

3.2. INDIVIDUAL ABILITIES ASSESSMENT

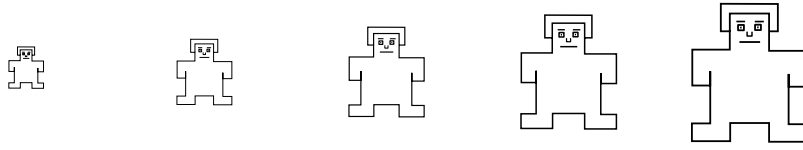


Figure 3.25: The Dominance dimension of the SAM questionnaire illustrates a progression from submission to control. The figures range from a small figure on the left, representing feelings of submission, to a larger figure on the right, signifying control and power.

user interaction with app permissions, including whether participants modified permissions and their rationale for such changes, their prior knowledge of the app’s access to their data, and their perceptions of the necessity and appropriateness of these permissions. Further, we queried the participants on their experience with *HappyPermi*, seeking to determine its impact on their awareness and management practices. The questions also delved into users’ likelihood of continuing to use *HappyPermi*, their overall comprehension of app permissions following its use, any observed changes in their behavior regarding permission vigilance, and their subjective feedback on the tool’s features and areas for improvement. This structured questionnaire was instrumental in determining the participants’ privacy concerns, their desire for transparency, and the potential educational value of permission management tools in enhancing digital literacy.

Procedure Participants were recruited through various channels such as online platforms, communities, word of mouth, social networks, and email invitations. Upon arrival, participants were delivered with detailed information regarding the study’s objectives and were required to provide informed consent before proceeding. Each participant spent approximately 10 minutes interacting with the dedicated version. Subsequently, they were instructed to install the *FahrPlaner* applications on their mobile devices from the Google Play Store if they still need to be installed. We employed the Thinking Aloud method to determine the underlying motivations guiding participants’ decisions throughout the evaluation process (Nielsen et al., 2002). Participants were tasked with analyzing *FahrPlaner* and adjusting permissions as necessary, with no specific instructions on how to use *HappyPermi*, allowing them to explore the application freely.

Participants The participant pool comprised individuals with varied educational backgrounds, including ten with a computer science degree, one high school graduate, and nine holding advanced degrees. In the *HappyPermi*

3.2. INDIVIDUAL ABILITIES ASSESSMENT

group, all ten participants were male, with an average age of 24.1 years ($SD = 2.27$). Conversely, the *HappyPermi+Flow* group consisted of one female and nine males, with an average age of 22.6 years ($SD = 2.08$). The study relied on voluntary participation, and the participants received no financial compensation.

Ethical Considerations In alignment with the ethical principles upheld throughout this dissertation, we prioritized participants' privacy and security when deploying study applications on their devices. The *HappyPermi* app exemplified ethical standards by minimizing data collection, obtaining explicit consent, and keeping all data strictly local. Additionally, we enforced secure communication and employed safe inter-app communication methods, which enhanced user trust and device integrity. These measures ensured that the app maintained the highest privacy and security standards, fostering an environment conducive to ethical research practices. Furthermore, we adhered to ethical guidelines by minimizing third-party data usage, informing users of potential risks during consent, and managing data to maximize benefits while minimizing the risk of disclosure to unauthorized parties.

Empirical Findings

In this study, we evaluated the usability and user perceptions of two application groups (*HappyPermi* and *HappyPermi+Flow*) using the System Usability Scale and the Self-Assessment Manikin questionnaire. The SUS scores suggested that the *HappyPermi+Flow* group achieved a high usability level with an average score of 80.75 ($SD = 20.58$). In contrast, the *HappyPermi* group also demonstrated good usability, albeit lower, with an average score of 72.5 ($SD = 14.62$). Despite these differences, independent t-tests revealed no statistically significant difference in SUS scores between the groups, indicating comparably high usability levels across both applications. Similarly, the SAM questionnaire results, which assessed emotional responses such as Pleasure, Arousal, and Dominance, showed no significant differences between the two groups, suggesting that both applications elicited similar emotional reactions from users ($p > 0.05$ for all comparisons). In the case of the *HappyPermi* group, the mean rating for Pleasure was 5.3 ($SD = 1.2$), for Arousal, it was 3.7 ($SD = 1.9$), and for Dominance, it was 5.9 ($SD = 2.2$). Conversely, for the *HappyPermi+Flow* group, the mean scores were 3.4 ($SD = 2.0$) for Pleasure, 4.7 ($SD = 2.7$) for Arousal, and 6.3 ($SD = 2.1$) for Dominance (see Figure 3.26).

In addition to the findings above, the target questions in the study also explored user interactions with Android permissions, shedding light on significant concerns among participants regarding the access permissions of the

3.2. INDIVIDUAL ABILITIES ASSESSMENT

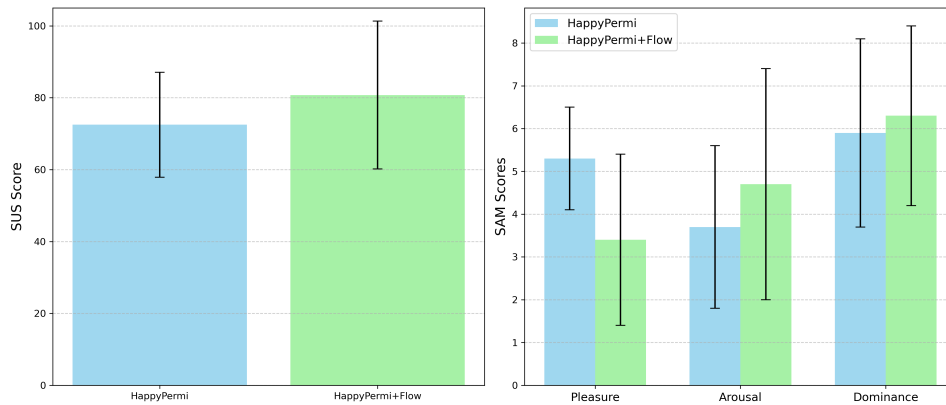


Figure 3.26: On the left are the SUS scores, and on the right are the SAM sub-scales scores of two application groups.

FahrPlaner application. A substantial 69% of participants opted to turn off the contact permission, indicating a widespread unease and lack of understanding regarding the app’s access to personal data. This sentiment was further elucidated by participants such as *P07*, who emphasized the necessity for greater transparency and justification for such permissions, questioning the relevance of granting access to sensitive data like contact details and the device camera. These concerns resonated throughout the responses, with users consistently expressing a desire for more information regarding the utilization and sharing of their data. For instance, *P05* commended the comprehensive insights provided by *HappyPermi* regarding application permissions. At the same time, *P12* underscored the profound impact of witnessing firsthand how personal information could be disseminated to various applications without explicit consent. In line with these sentiments, 11 participants indicated an interest in continuing to use *HappyPermi* as a supplementary informational resource, suggesting a recognition of its value in enhancing awareness and transparency surrounding app permissions. Conversely, nine respondents expressed reservations, reflecting a nuanced attitude toward the utility of such tools in empowering users to make informed decisions about their privacy.

Discussion and Limitations

In this study, we focused on two research questions to investigate the effectiveness of the *HappyPermi* app in enhancing user understanding of Android permissions. The first question explores how interactive tools can assist users in comprehending the implications of permission requests on their private data. The second question delves into the extent of users’ awareness about the destinations of their data transmissions, assessing their understanding of

3.2. INDIVIDUAL ABILITIES ASSESSMENT

where their data is sent after permissions are granted. Our study shows that the *HappyPermi* app impacts user comprehension of permission requests by effectively visualizing where users' data is sent and the implications of granting permissions. This clarity provided by *HappyPermi* and similar tools sheds light on the typically unclear processes through which apps handle user data, enhancing transparency vital for effective privacy management (Gerber et al., 2018). This finding is aligned with existing research emphasizing the importance of understanding and actively practicing privacy and security settings on mobile devices to boost security awareness and user knowledge (Breitinger et al., 2020). *HappyPermi* simplifies this process through a user-friendly interface that demystifies the complexities associated with Android permissions. The SUS usability scores reveal that both versions maintain good levels of usability, which is essential for ensuring that users are aware of the permissions they authorize and fully grasp the associated consequences. This correlation between high usability and effective user engagement and the subject being learned is well-supported by existing research (Vlachogianni and Tselios, 2022).

The finding that 69% of users opted to turn off the contact permission underscores a practical understanding of the potential risks associated with unnecessary data access. This significant proportion of users altering permissions highlights their awareness and proactive management of their privacy, reflecting their discomfort with potential risks and the real-world implications of permission settings. This action indicates that users are prepared to take concrete steps to protect their privacy based on understanding where their data might be sent and how it could be used. It reinforces the importance of tools that educate and empower users to make informed decisions regarding their personal data (Turland et al., 2015).

The SAM questionnaire results further enrich this analysis by revealing no significant emotional differences between users of *HappyPermi* and *HappyPermi+Flow*. This finding indicates that the emotional impact of using these tools is neutral, suggesting that users' decisions to manage permissions are likely based on cognitive understanding rather than emotional responses. However, it is possible that in specific situations, individuals' emotional dispositions could influence their choices, like a trade-off between functionality and privacy (Cao et al., 2021). Participants did not exhibit heightened emotional distress or excessive pleasure, which implies a rational and informed decision-making process. Feedback from participants like *P07* and *P12*, who expressed a desire for greater transparency and control, aligns with these findings, demonstrating a keen interest in understanding and managing how apps use their data.

3.2. INDIVIDUAL ABILITIES ASSESSMENT

While our findings are encouraging, they come with several limitations. The small number of participants limits the generalizability of the results, making it difficult to draw broad conclusions about the applications' efficacy. Future research should involve a more extensive and diverse group of participants to confirm these findings and examine differences across various demographics. Additionally, potential biases in the study design related to participants' tech familiarity might have influenced usability ratings and perceived effectiveness. Enhancing privacy tools with more comprehensive feedback mechanisms could provide users with personalized data usage insights, increasing tool effectiveness.

Acknowledgments

This section is based on the publication:

Mehrdad Bahrini, Nina Wenig, Marcel Meissner, Karsten Sohr, and Rainer Malaka. 2019. *HappyPermi: Presenting Critical Data Flows in Mobile Application to Raise User Security Awareness*. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems (CHI EA '19)*. Association for Computing Machinery. DOI: 10.1145/3290607.3312914

My contribution to this work: Conceptualization, data curation, formal analysis, investigation, methodology, project administration, resources, part of software development, supervision, validation, visualization, and contribution to all parts of the manuscript.

3.2.3 Study 6: Informed Decisions via Mobile App Analyzers

Introduction and Background

In our previous study, the HappyPermi app analyzer substantially impacted users' understanding of permission requests by effectively visualizing where their data would go and the consequences of granting permissions. This clarity enhances transparency, vital for practical privacy management (Bahrini et al., 2019b). We integrated MobSF into our methodology due to its open-source nature, thorough documentation, and widespread adoption across academia and industry for static and dynamic analysis of mobile apps. It is tailored for penetration testing, malware analysis, and security evaluations of mobile apps on Android, iOS, and Windows platforms.

In addition to MobSF, numerous other tools have been developed to analyze mobile apps (Senanayake et al., 2023). Noteworthy among these is *FlowDroid*, which excels in statically computing data flows, providing comprehensive insights into how data moves through an Android app (Arzt et al., 2014). *COVERT* offers compositional analysis for inter-app vulnerabilities, making it a crucial tool for understanding how different apps can interact and potentially compromise each other's security (Bagheri et al., 2015). *HornDroid* (Calzavara et al., 2016) and *DIALDroid* (Bosu et al., 2017) focus on privilege escalations and information flow analysis, respectively, helping to identify and mitigate risks associated with unauthorized access and data leakage. *MalloDroid* specializes in detecting broken Secure Sockets Layer (SSL) certification validations, ensuring that communications are properly secured (Fahl et al., 2012). *JAADAS*⁷ tackles a broad range of issues, including Application Programming Interface (API) misuse, intent crashes, and local denial-of-service attacks, making it a versatile tool for application security. Tools like *DevKnox*⁸ and *AndroBugs Framework*⁹ are geared towards industrial use, providing developers with real-time solutions for detecting and resolving security issues as they write code, thus integrating security directly into the development process. *MARVIN* employs machine learning techniques to assess the maliciousness of unknown apps, creating accurate snapshots of malware behavior to assess associated risks (Lindorfer et al., 2015). Lastly, *QARK*¹⁰ and *FixDroid* (Nguyen et al., 2017) offer robust capabilities for detecting security vulnerabilities and providing actionable security fixes, contributing significantly to the enhancement of app security.

⁷<https://github.com/flankerhq/JAADAS>

⁸<https://devknox.io>

⁹https://github.com/AndroBugs/AndroBugs_Framework

¹⁰<https://github.com/linkedin/qark>

3.2. INDIVIDUAL ABILITIES ASSESSMENT

These tools have been developed and continue to evolve because mobile apps handle sensitive personal data, making it crucial for enterprises to implement clear data handling practices, ensuring secure and transparent user information management. In the European Union, any organization that stores or processes the personal data of European Union (EU) citizens within EU borders must adhere to GDPR regulations, regardless of their physical location. A privacy policy is essential in this context, serving as a critical document that specifies how user data is gathered, utilized, stored, and disclosed. Failure to implement an accurate privacy policy can result in significant fines. Therefore, privacy policies are indispensable components of applications, requiring users' consent before they can start using the app. Due to the specific language used in privacy policies (Fabian et al., 2017), various privacy policy analysis tools have been developed to enhance their readability and comprehension. *Polisis* uses artificial intelligence to simplify and visualize privacy policies, making them more accessible to users (Harkous et al., 2018). *MAPS (Mobile App Privacy System)* utilizes supervised machine learning to assess app privacy policies and highlight potential conflicts (Zimmeck et al., 2019). *PrivacyCheck* summarizes privacy policies using machine learning, providing user control and GDPR compliance scores (Zaeem et al., 2018). Other tools, such as *PolicyLint* (Andow et al., 2019), which identifies contradictions in privacy policies using ontology generation and natural language processing; *PrivacySpy*¹¹, which summarizes and rates privacy policies on a ten-point scale; and *Privee* (Zimmeck and Bellovin, 2014), a browser extension that simplifies privacy policies using crowd-sourced and automated analysis, provide various methods for summarizing, rating, and identifying contradictions in privacy policies.

Despite the availability of these powerful tools, a significant gap remains in their usability for the average user. Many of these tools are designed with researchers and developers in mind, requiring extensive knowledge of Android reverse engineering and security practices. The complexity and technical nature of these tools make them less accessible to regular smartphone users who need straightforward, user-friendly solutions to understand and manage app permissions and privacy policies.

Continuing our previous study, we developed a Mobile Android Security Scanner (MASS) to address these usability challenges. The MASS app aims to provide a user-friendly interface that simplifies the process of analyzing app permissions and privacy policies. Unlike existing tools that often overwhelm users with technical details, MASS focuses on delivering clear, concise, and

¹¹<https://privacyspy.org/>

3.2. INDIVIDUAL ABILITIES ASSESSMENT

actionable information. It integrates static analysis capabilities, leveraging the strengths of tools like MobSF, and presents the results in an intuitive, easy-to-understand format. Additionally, it incorporates features inspired by tools like Polisis to improve the accessibility and comprehension of privacy policies. The design of MASS follows established usability principles to ensure that it meets the needs of average users. Shneiderman’s eight golden rules and Nielsen’s heuristics were foundational in the development process, emphasizing consistency, feedback, error prevention, and user control (Wong, 2023; Nielsen, 1994). Hence, the central research question shaping this study is: *To what extent can static analysis of Android, together with a privacy analysis tool, enhance user awareness and inform decision-making regarding Android application permissions and privacy policies?*

This study contributes significantly in several ways. It examines user awareness and behavior concerning Android app permissions and privacy policies, assessing the impact of user-friendly analyzers like MASS in enhancing user comprehension and decision-making. It also provides valuable insights into designing more effective privacy tools that empower users to manage smartphone security proactively. By focusing on bridging the gap between technical security measures and user-friendly design, this research aims to equip users with better tools to safeguard their personal data in today’s digital landscape.

Prototype Description

Concept We developed an Android app named MASS (Mobile Android Security Scanner) to address our research question. The primary objective of MASS is to empower users to make informed decisions regarding Android apps while protecting their private data. The app adheres to established design guidelines and incorporates MobSF, to scan the apps installed on a user’s smartphone. Furthermore, to clarify the rationale behind the permissions requested by various apps, MASS integrates privacy policies summarized using Polisis (Harkous et al., 2018), a deep learning-based tool designed to interpret and condense privacy policies.

The development process began with creating a prototype to visualize the potential user interface. This prototype served as the foundation for the actual implementation, during which the concept evolved significantly, resulting in the app’s current, more comprehensive functionality. MASS was explicitly designed for the Redmi Note 8 Pro, running Android version 10. The implementation utilized a combination of Ionic 5 and Capacitor 2.0 technologies. Ionic¹², an open-source mobile user interface toolkit, enables

¹²<https://ionic.io/>

3.2. INDIVIDUAL ABILITIES ASSESSMENT

the creation of cross-platform native and web app experiences. Capacitor¹³ facilitates the migration of the app to various app stores and mobile web platforms upon completion, acting as a cross-platform API and code execution layer that allows web code to invoke native software development kits (SDKs).

Analyzer Applications Before prototyping, extensive research was conducted in the Google Play Store to ensure our app provides unique functionalities beyond a redesigned user interface. This research aimed to evaluate the capabilities and usability of existing Android scanning apps, adhering to the eight golden interface design rules (Wong, 2023). The investigation, conducted in March 2021, focused exclusively on free and non-root apps to maintain a structured approach. The evaluation process simulated typical use cases for scanning apps, such as analyzing installed apps on a smartphone. Beyond assessing the functionality and range of scanning features, the analysis emphasized usability, particularly the presentation of elements and information during user interaction. The search terms “permission analyzer,” “APK analyzer,” “APK information,” and “app analyzer” were utilized to identify relevant apps. Despite yielding numerous results, the analysis was confined to apps with a low number of downloads to ensure a detailed evaluation. Finally, we singled out three apps with notable qualities or features that set them apart. Insights gained from this research were instrumental in developing the MASS app.

The first app is *APK-Info* (see Figure 3.27) and comprises two main pages: an app listing page and a corresponding details page. Upon the first launch, the app displays all installed applications on the smartphone. Users can change the language on this page; a search field and sorting method are also available. The scan results are presented on the details page using a simple card design, making the app user-friendly. Running an initial scan is straightforward. However, the design is minimalistic, focusing only on essential features. On the app listing page, users can filter between “user apps” and “all apps,” though the term “all apps” could be ambiguous. A clearer distinction between “installed apps” and “system apps” would be preferable. The scan results are categorized into sections such as “Basic Information,” “Permissions,” and “Requested features.” Other categories include “Installation” and “Certificate,” but the purpose of this information is not explained, potentially leaving users uncertain about its relevance.

The second application, called *App Inspector* (shown in Figure 3.28), boasts the highest number of downloads. Upon its initial launch, users are immediately directed to a page displaying all installed apps without

¹³<https://capacitorjs.com/>

3.2. INDIVIDUAL ABILITIES ASSESSMENT

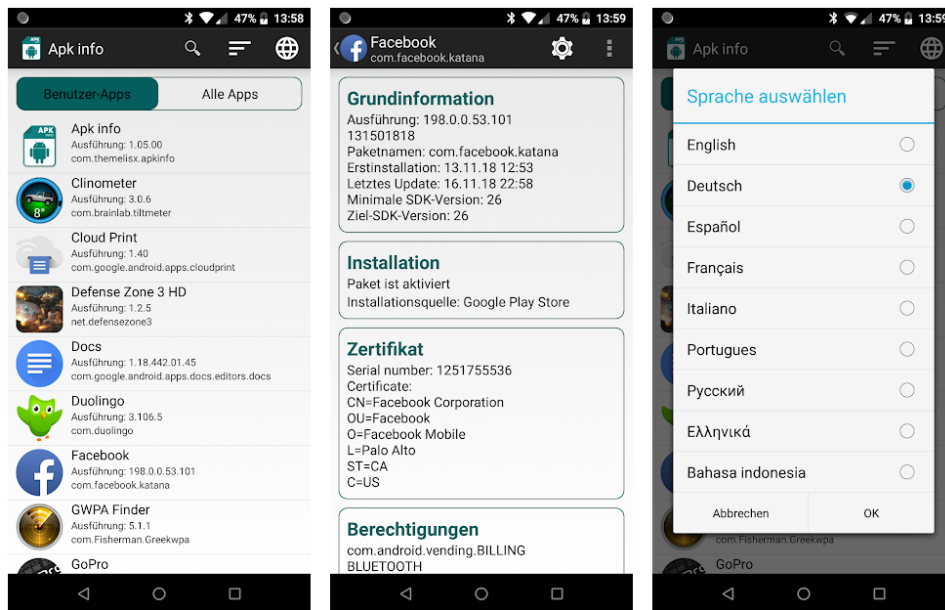


Figure 3.27: The *APK-Info* screenshots from 2021

any search or sorting options available. Each app is listed individually, with no additional functionalities provided on this page. When an app is selected, users are redirected to a details page that offers only the most essential information. However, the design of this page is rudimentary, lacking organization and clarity. Instead of neatly grouped APK information, the details are presented in a confusing list format, comprising only the app's name, package name, version code, target SDK, class name, source directory, and data directory. Such limited and unorganized information may prove inadequate for users seeking comprehensive insights from a scanning app.

The third app is *Apk Analyzer* (see Figure 3.29). It stands out as the sole app among the three that requests access to camera and memory permissions. Upon launching the app, users are presented with a familiar listing of installed apps akin to the previous two applications. However, *Apk Analyzer* introduces a novel feature, which is a menu navigation system on the listing page. This menu allows users to navigate to pages such as “Applications,” “Statistics,” “Permissions,” “Settings,” and “About.”

The “Statistics” page offers users comprehensive insights into their installed apps, summarizing data such as average app size and presenting app distribution in a diagram format. Information is displayed in an accordion style, enhancing clarity and readability. The “Permissions” page lists all utilized permissions, accompanied by the number of apps employing each

3.2. INDIVIDUAL ABILITIES ASSESSMENT

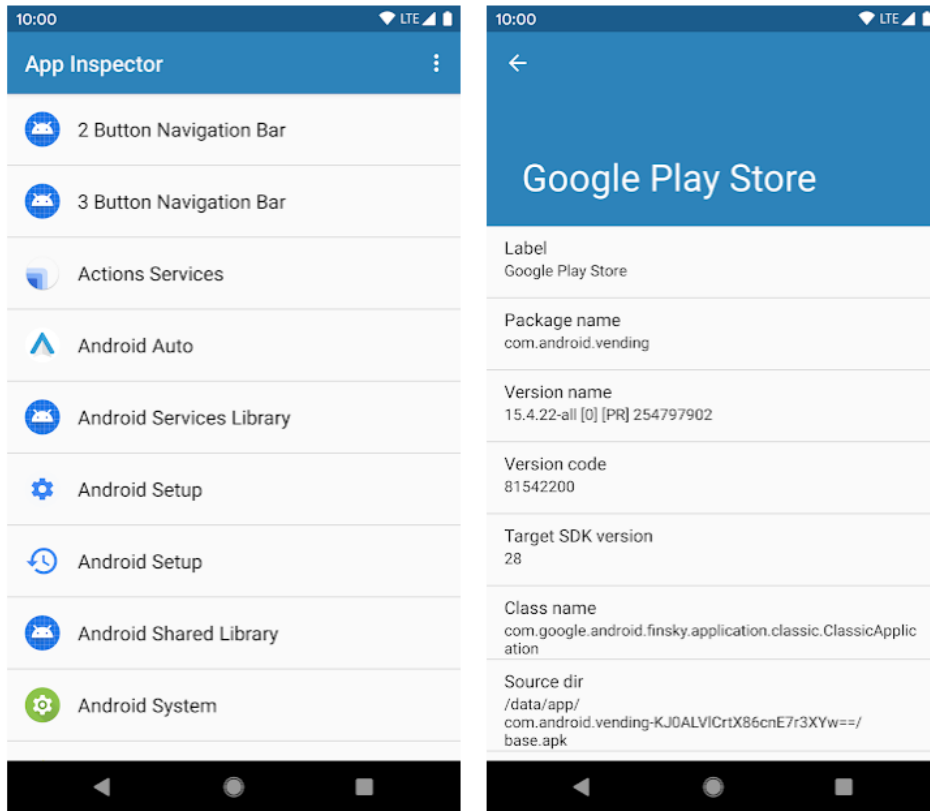


Figure 3.28: The *App Inspector* screenshots from 2021

permission. Clicking on permission reveals a detailed breakdown of apps utilizing that permission, along with related information.

Pages like “Settings” and “About” are peripheral to the scanning functionality. However, the primary permissions page integrates a search function and sorting mechanism, mirroring the design of the app’s APK information section. Upon selecting an app, users are directed to a detailed page containing extensive information categorized under sections like “General,” “Certificate,” “Permissions Used,” and more. Additionally, users can access modal explanations for unclear terms within the scan results. While *Apk Analyzer* offers a wealth of information, some details may be deemed extraneous, such as app certifications and `AndroidManifest.xml` files. Among the three apps, *Apk Analyzer* emerges as the most innovative in terms of design and scanning capabilities. However, it also underscores the limitations of standalone scanning apps, suggesting the need for supplementary analysis tools. Notably, none of the three apps requested internet permissions during operation, indicating self-sufficiency without reliance on external resources.

3.2. INDIVIDUAL ABILITIES ASSESSMENT

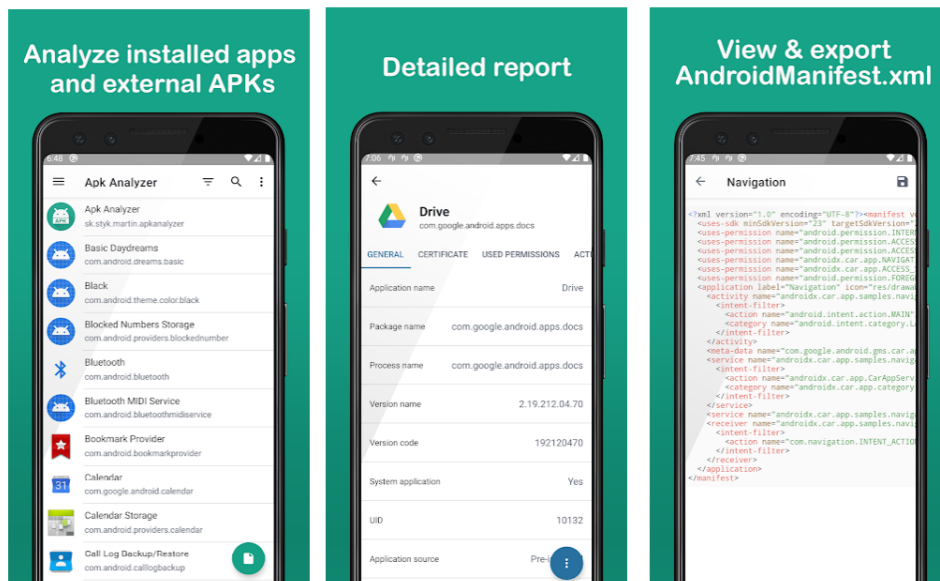


Figure 3.29: The *Apk Analyzer* screenshots from 2021

Design: Introduction Screen When initiating the MASS app for the first time, it is crucial to familiarize the user with its features. The primary objective is to explain the main functionalities quickly and concisely. Two distinct approaches were considered: introducing the user to the app at the outset or integrating explanations within the user’s navigation through small hint boxes across various pages. Given the manageable complexity of the app, the decision was made to opt for an introductory tutorial at the app’s inception. Figure 3.30 illustrates this tutorial.

Users can advance to the next slide either by clicking the “Next” button or swiping their finger from left to right. Throughout the tutorial, users are systematically guided through scanning an app on their smartphone. Upon reaching the final slide, the “Start Search” button directs them to the app’s home screen. Once the user clicks either the “Start Search” or “Skip Tutorial” button, the tutorial ceases to appear upon subsequent app openings. This adherence to the second golden rule, as outlined in the app’s guidelines, ensures that users have the option to bypass the tutorial and dive directly into the app’s core functionality. Considering the diverse user base, the app incorporates functionality allowing users to skip the tutorial at any point and immediately access its main features.

Design: Home Screen Upon reaching the home screen (depicted in Figure 3.31), users are presented with a tab-based navigation system offering two distinct options: either initiating a comprehensive search for all apps on

3.2. INDIVIDUAL ABILITIES ASSESSMENT

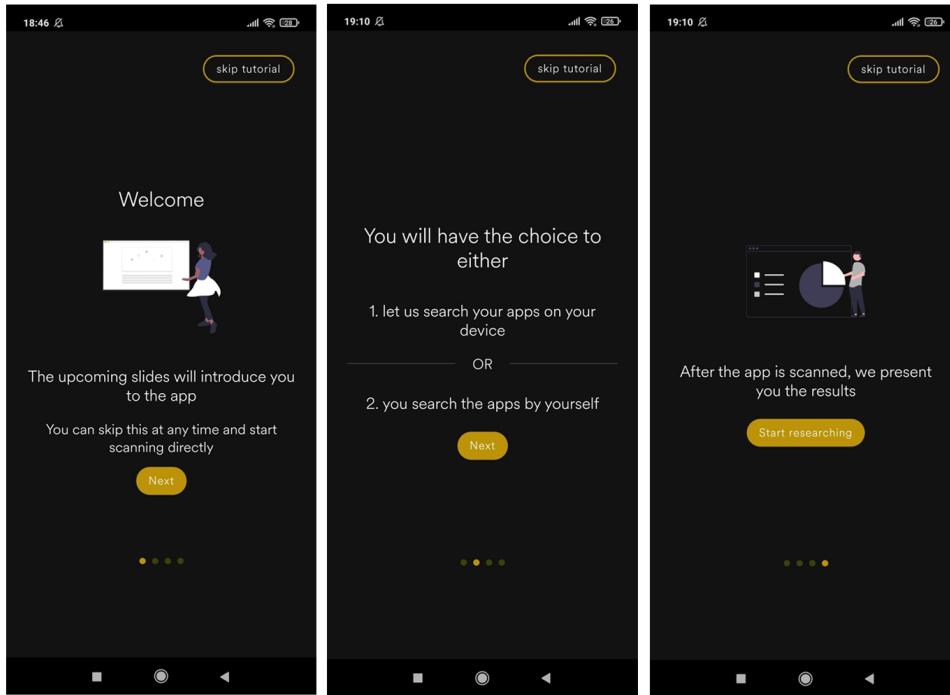


Figure 3.30: First-time Launch of MASS: Introduction to the app

their smartphone using MASS or opting for a standalone search for specific apps. In the first tab, the primary task is to search for and select an app, each option tailored to individual preferences and needs, offering a unique visualization. Once users have made their selection (option one or two), a corresponding feedback message provides confirmation.

Choosing MASS to list all smartphone apps (center screen in Figure 3.31) triggers a brief loading animation before displaying all apps on the screen. A message at the bottom indicates the number of apps found, conveniently echoed in the header for quick reference. This user-friendly option allows for sorting search results according to preference (by newest/oldest installation or alphabetically ascending/descending) and includes a search function for specific app queries. Each app's dangerous permissions, mandated by the Android operating system, are displayed on cards with icons and text. Apps not requiring such permissions are marked with a green thumbs-up icon. Additionally, the installation date is displayed beneath the app name.

In the standalone search scenario (right screen in Figure 3.31), a brief background preparation precedes a readiness message at the bottom of the page. The user's keyboard automatically opens, focusing on the search field. This streamlined option caters to advanced users preferring manual searches

3.2. INDIVIDUAL ABILITIES ASSESSMENT

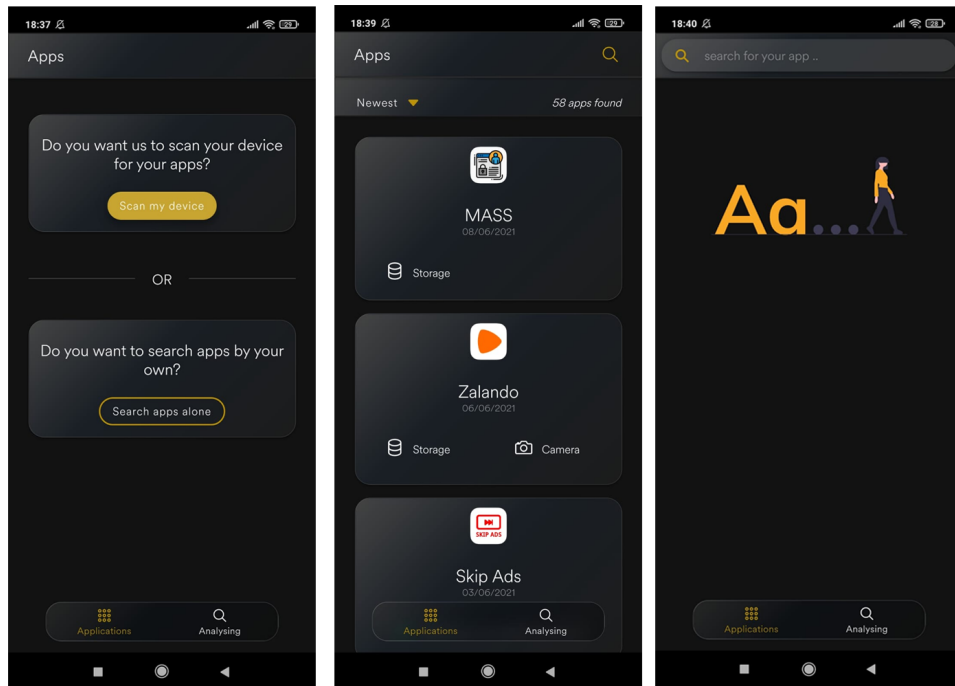


Figure 3.31: First Tab: The home screen of MASS

or prioritizing privacy, as it bypasses the comprehensive scan.

Regardless of the chosen search method, tapping an app triggers a confirmation modal before proceeding to the second tab for deep scanning. This user-centered design, adhering to the second golden rule, caters to users with varying levels of knowledge. The MASS app aligns with the third golden rule by providing feedback for every action. Consistency is ensured by presenting search results uniformly and offering a search field in both variants. Lastly, the core functionality of MASS includes searching, scanning, and obtaining results. This fulfills the fourth golden rule, ensuring the seamless completion of every initiated action sequence.

Design: Scan Execution The second page is the hub for conducting detailed scans of selected apps. Users who attempt to access the second tab without selecting an app are gently reminded to select first (refer to the left screen in Figure 3.32). Once an app is chosen in the first tab and confirmed for scanning in a modal, the center screen of Figure 3.32 emerges, ready for action. Users remain free to return to the first tab and switch selections as needed, even after initially choosing an app. Clicking the “Deep Scan” button triggers the extraction and seamless transmission of the selected app to the MobSF server in the background. Throughout this process, users are

3.2. INDIVIDUAL ABILITIES ASSESSMENT

kept informed with real-time updates at every stage, as exemplified in the right screen of Figure 3.32.

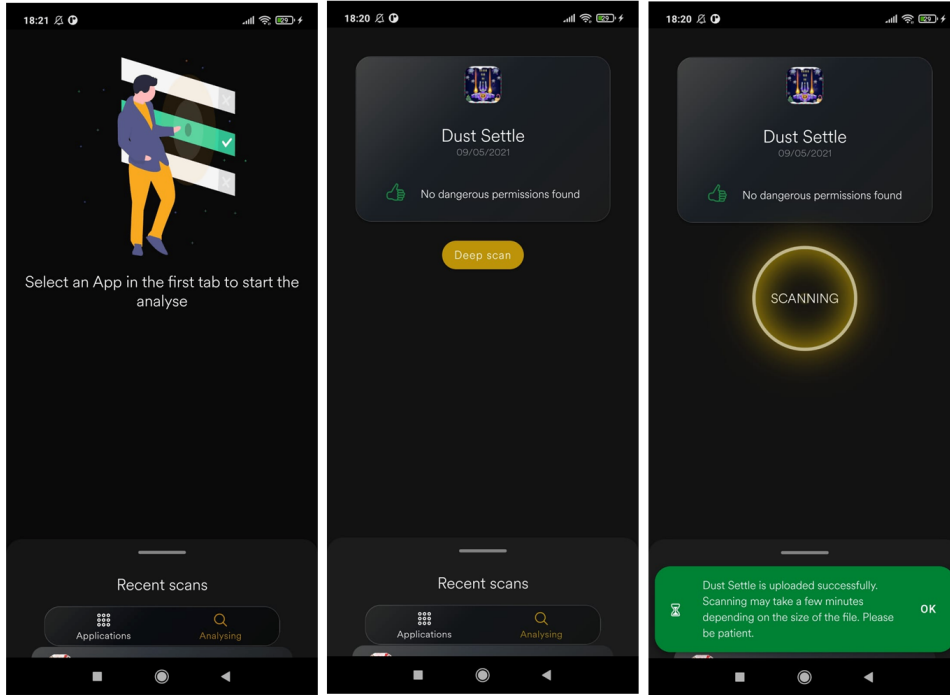


Figure 3.32: Second Tab: Scanning a desired app

Given the asynchronous nature of the client-server interaction, any potential errors are carefully managed. In the event of an issue, a user-friendly message is promptly displayed: “Sorry, the server seems to be unreachable. Contact the developer if this error occurs again.” Once the scan successfully wraps up, the bottom slide page gracefully glides from bottom to top without user intervention. This design adheres to the fifth golden rule by providing clear and understandable messages and ensures that users maintain control and flexibility throughout their actions. The sixth and seventh golden rules are upheld seamlessly, allowing for effortless reversal of actions and empowering users with a sense of agency. Users can switch tabs as needed to fine-tune their app selections, a process that’s as fluid as it is intuitive.

Design: Scan Results The scan results are presented through a slider interface, allowing users to navigate their app history easily. All scans conducted by the user are stored within this slider, enabling convenient retrieval of previously scanned apps without requiring redundant rescans. This feature addresses usability concerns by reducing the need for repetitive scanning for reference or comparison. Upon first interaction with the slider,

3.2. INDIVIDUAL ABILITIES ASSESSMENT

a subtle hint notifies users of the absence of a prior scan history. When users select an app from their history, a streamlined API request is sent to the MobSF server, requiring only Internet permission and avoiding extras.

Within the MASS environment, scan results from MobSF and Polisis are carefully organized, revealing crucial insights such as basic app details, permissions, trackers, server locations, privacy policies, and Google Play Store information. These categories are displayed in an accordion format to prevent information overload. It enables users to delve deeper into specific categories with a simple tap. For instance, upon selecting an app, the expanded permissions section categorizes permissions based on threat levels, with color-coding for quick reference. Users can explore further into each permission by tapping on the info icon, ensuring comprehensive understanding.

MASS enhances MobSF's server localization feature by transforming it into an interactive map display, enabling users to explore server locations easily. This interactive map interface, showcased in the center screen of Figure 3.33, offers users an immersive inquiry experience, complete with zoom and click functionalities for detailed insights. Moreover, the Google Play Store information provided by MASS mirrors the comprehensive details found in the actual store, including star ratings, developer information, download counts, and the privacy policy page of the scanned app.

Integrating MobSF and Polisis enables a deeper analysis of privacy policies extracted from the Google Play Store, providing users with summaries of both positive and negative aspects. The right screen of Figure 3.33 showcases the positive attributes of a scanned app while ensuring accessibility to negative points for comprehensive evaluation. Lastly, the history functionality of MASS aligns with the eighth golden rule by releasing users from the burden of memorizing past scan results, offering effortless access to previous scans whenever needed, thus enhancing user convenience and satisfaction.

User Evaluation

Study Design To address our research question, we launched an empirical study to investigate the effectiveness of combining static analysis of Android with a privacy analysis tool in enabling users to make informed decisions about Android apps. In this study, we deliberately chose a semi-structured interview format (Adams, 2015). We carefully crafted a guideline to outline the interview procedure and questions. However, this document serves solely as a tool for the interviewer and is not shared with participants. Flexibility is allowed in question wording and sequence, enabling the exploration of unforeseen avenues. The interviews included structured tasks, questions, and open-ended inquiries concerning usability, privacy, and data security.

3.2. INDIVIDUAL ABILITIES ASSESSMENT

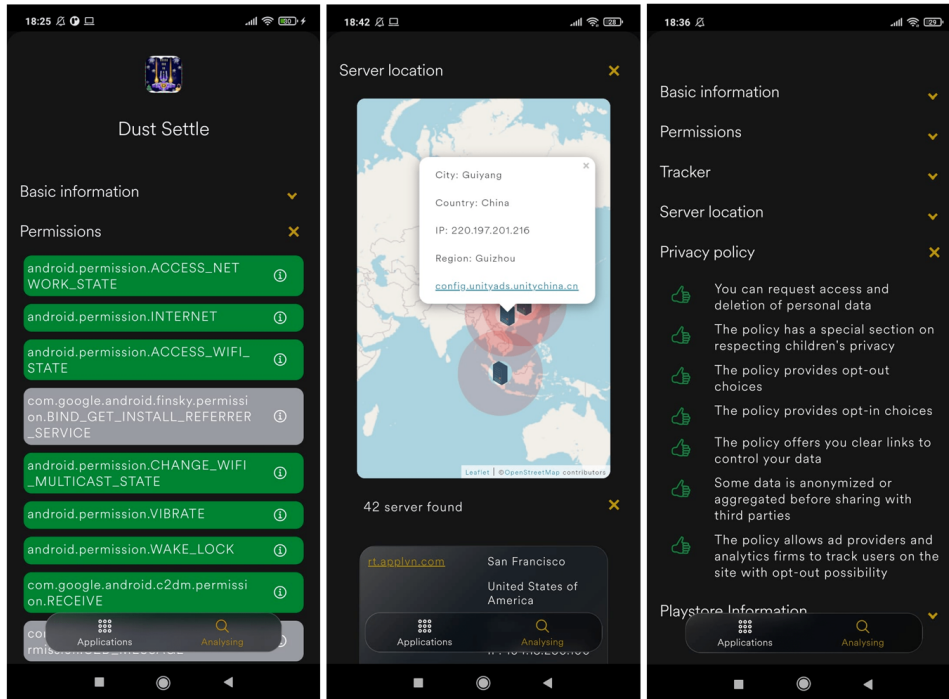


Figure 3.33: Scan results of MobSF in MASS

Additionally, we utilized the thinking-aloud method to ensure accurate documentation and enhance understanding of respondents' perspectives (Charters, 2003). This approach prompted users to verbalize their actions and justify their decisions. It is important to note that users were expected to explain why they took specific actions.

Materials Before commencing the interviews, we initiated the process by posing preliminary questions to the participants, seeking to gain insights into their perspectives and backgrounds. Subsequently, the questionnaire, facilitated through Google Forms and completed on desktop computers, was meticulously crafted to explore various facets of participants' demographics, smartphone expertise, and attitudes toward smartphone security. Covering a broad spectrum of topics, ranging from basic demographic information to nuanced inquiries about privacy and security concepts, the questionnaire aimed to shed light on participants' levels of technological literacy, comprehension of smartphone security and privacy, and the importance they placed on protecting their personal data. Additionally, participants were probed about their concerns regarding the security of their smartphones, their typical methods of app installation, their approaches to app permissions, and their

3.2. INDIVIDUAL ABILITIES ASSESSMENT

overall awareness and familiarity with popular apps like TikTok¹⁴.

The interview comprises four distinct sections, each serving a specific purpose. The first section evaluates the user's awareness regarding collecting and utilizing their personal information within a predetermined application. The second section examines the three scanning applications discussed alongside our developed MASS app. Subsequently, the third section involves scanning the TikTok application using the participant's preferred scanning application. We opted to focus on TikTok for our study, considering its significant number of downloads from the Google Play Store and the mounting privacy concerns it has generated over the past few years (Anderson, 2020). Finally, the fourth section allows participants to provide feedback on the interview process and the scanning apps. Appendix A.1 features a list of interview questions.

The interviews were conducted over two weeks using a Xiaomi Redmi Note 10 smartphone running Android 10 (API level 30), all within the confines of the same controlled environment. Participants were not informed that MASS was the newly developed app from this study. Each interview session, lasting between 30 and 45 minutes, was deliberately structured to ensure comprehensive exploration. Participants did not receive monetary compensation for their involvement.

Procedure The interview commenced with a warm greeting and informal conversation, followed by an explanation of the interview's purpose and procedures. Participants were presented with an informed consent form explicitly outlining the use of screen and audio recordings for thesis purposes. Once consent was obtained, participants completed the necessary questionnaires. Throughout all twelve sessions, the interview director provided continuous guidance as participants navigated through each interview section. Participants were briefed that the entire interview would be conducted exclusively on a designated screen, encompassing the Google Play Store and app settings, thereby restricting access to external sources for solutions. Clear instructions were provided for completing tasks, with each section considered complete once participants either achieved the goal or encountered an insurmountable obstacle. Throughout the interview, both the smartphone screen and the participants' audio were recorded for documentation purposes. Post-interview, the audio data was transcribed, while participants' interactions with the smartphone were visually marked using developer options, streamlining evaluation, and transcription processes.

Pre-Study Before initiating the main study sessions, a thorough pilot test was conducted to confirm the safety and efficacy of the interview process.

¹⁴<https://www.tiktok.com/>

3.2. INDIVIDUAL ABILITIES ASSESSMENT

This preliminary trial involved an individual not part of the study, ensuring an objective assessment of the interview protocol. The primary objective of the pilot test was to identify and address any potential issues or challenges that might arise during the sessions. Feedback from the pilot test proved invaluable, guiding technical enhancements and procedural refinements to optimize the overall interview experience for the participants and the interview director.

Participants The interview engaged twelve participants, comprising five females and seven males. Participants were invited verbally through social media channels, with appointments facilitated by the interview director. Their ages ranged from 21 to 33 years ($M = 25.83$, $SD = 3.31$).

Empirical Findings

Baseline Insight

- *Background and Knowledge:* Among the interviewees, six stated they lacked prior experience in privacy and security. Conversely, two participants boasted professional backgrounds, with an additional three possessing educational qualifications. Only one participant had experienced company-sponsored training.
- *Knowledge of Smartphone:* In the self-evaluation of smartphone knowledge, three participants declared themselves to have a strong understanding. Half of the group deemed their knowledge average, while the remaining three rated their familiarity as low. None classified themselves as experts or complete novices.
- *Understanding of Smartphone Privacy and Security:* Concerning smartphone privacy and security comprehension, two participants rated their understanding as very low, while one labeled it as low. Remarkably, a majority of the participants ($n = 8$) rated their grasp of smartphone security and privacy as average. It is worth noting that despite exactly half of the participants possessing training or professional experience in the field, none considered themselves experts, except for one individual who self-assessed as proficient.
- *Smartphone Privacy and Security Importance:* Participants held diverse views on the importance of smartphone privacy and security. Among the twelve respondents, three felt these aspects were less crucial, while another three viewed them as moderately important. In contrast, three participants highlighted their significance, and strikingly, the remaining three emphasized that security and privacy were highly important.

3.2. INDIVIDUAL ABILITIES ASSESSMENT

Notably, none of the participants dismissed the importance of these factors. Therefore, all participants acknowledged the significance of privacy and security in smartphone usage, regardless of their level of expertise in these areas.

- *Smartphone Privacy and Security Concerns:* Participants' concerns about their smartphone security were reflected in their evaluations of the importance of security and privacy in smartphone use. A quarter of the participants showed relatively low concern about their own smartphone's security, while a third expressed average concern. One participant emphasized the importance of their smartphone's security; notably, four participants were highly concerned about it.
- *Ways to Install Android Apps:* When it comes to installing Android apps on their smartphones, most participants ($n = 10$) prefer the standard method of using the Google Play Store. In contrast, two participants choose to install Android apps from the internet. None of the participants favor receiving Android apps from friends or family through emails or social media.
- *Reviewing App Descriptions Before Installation:* The twelve participants held similar views regarding their attention to app descriptions before installation. Two participants paid neither a significant nor minimal amount of attention. In contrast, seven participants paid relatively little attention, and the remaining three paid hardly any attention at all before installing an app.
- *Understanding Dangerous Permissions:* When asked about dangerous permissions, all participants initially encountered confusion because they were familiar with the term "permission" but had a different understanding when it came to "dangerous" permissions. Eight participants answered the question affirmatively, and only one provided a correct explanation in a single sentence. In their responses, examples such as camera access, location access, or sharing personal information were frequently mentioned. One participant hesitated, unsure if all permissions could be classified as dangerous, ultimately answering the question negatively due to confusion. The remaining three participants promptly answered in the negative.
- *Reviewing App Privacy Policy:* We asked whether they had ever read the privacy policy of an app before or after installation. Ten participants answered no, while only two reported having done so. Each participant

3.2. INDIVIDUAL ABILITIES ASSESSMENT

was familiar with privacy policies, understanding that they typically cover collecting, processing, and using personal data. Interestingly, despite this awareness, ten out of twelve participants are relatively disinterested in how apps handle their personal data. This same disinterest was mirrored when participants were asked whether they read the app description before installation.

- *Permission Granting:* The final question addressed participants' behavior regarding permission modals. Only three participants indicated they consciously decide when granting permissions. The remaining nine participants acknowledged the appearance of permission modals but typically dismissed them without deliberation. Interestingly, while eight participants understood the concept of dangerous permissions in a previous question, only three mentioned consciously granting permissions here. Among those who habitually dismissed modals, four did so out of routine, habitually acknowledging all popups. The remaining five participants dismissed modals to use apps uninterrupted.
- *TikTok App Features and Functions:* TikTok, a widely popular app with high download numbers on the Google Play Store, was recognized by all participants in the survey.

Interview Section 1: User Awareness During the initial interview segment, participants were tasked with assessing their ability to identify and comprehend crucial details regarding app permissions, stored data, and user rights within the TikTok application. The tasks included Task 1A, where participants needed to determine the app's permissions and their intended purposes; Task 1B, focusing on identifying the types of information the app stores; Task 1C, which required locating where this stored information resides; Task 1D, aimed at identifying who can access this information and under what circumstances; and Task 1E, centered on determining the user rights associated with the app's handling of data. Task 1A posed challenges, with only 4 out of 12 participants successfully identifying the app's permissions and their purposes. Participants familiar with the Android system typically navigated directly to the app settings or the Google Play Store to find this information. Tasks 1B and 1C, involving the identification and location of stored data, were similarly challenging, with only 4 participants each successfully completing these tasks. These difficulties underscored the complexity and length of privacy policies. In contrast, Tasks 1D and 1E, which focused on identifying access permissions and user rights, were more successfully completed, with 8 out of 12 participants succeeding. This higher success

3.2. INDIVIDUAL ABILITIES ASSESSMENT

rate was attributed to the clearer presentation of this information within the privacy policy.

Interview Section 2: Testing App Analyzers In the second segment of the interview, participants were assessed on their knowledge related to app analyzers and their understanding of specific terms, followed by their interaction with four different scanning apps. The interview was divided into several tasks and subsections, each evaluating various aspects of participant knowledge and app usability.

- *Familiarity with app analyzers:* A considerable knowledge gap became apparent when evaluating participants' familiarity with app analyzers. None of the 12 participants reported prior familiarity or use of app analyzers when questioned. Specifically, all respondents indicated unfamiliarity with the selected apps. Moreover, none could identify a specific app analyzer or claim to have used one.
- *App analyzers terminology understanding:* We asked participants about their familiarity with various terms related to app analysis at this stage. Among the terms assessed, *permission*, *privacy policy*, *third party*, and *server* stood out as the most recognized, with 11 out of 12 participants providing detailed explanations for *permission* and *privacy policy*, and all 12 participants for *third party* and *server*. Terms such as *certificate* and *user apps/all apps* were familiar to 8 out of 12 participants, while *tracker* was known by 7 out of 12 participants. On the other hand, terms like *activities*, *APK*, *package name*, *target SDK*, *UID*, and *services* were only familiar to one participant each. Participants attributed their familiarity with certain terms to exposure in daily life, media, school, or conversations.
- *Ranking the terms by personal priority:* Following the presentation of thirteen terms, participants were tasked with ranking them according to personal preference, where 1 represented the most important term and 13 the least. The top two terms identified by participants as most crucial were *permission* and *privacy policy*. Half of all participants ranked privacy policy as the most important term and permission as the second most significant. However, rankings for other terms varied widely among participants, reflecting varying levels of familiarity and comfort despite the provided explanations.
- *Exploring app analyzers (What do you spot?):* The participants provided relatively consistent feedback on their perceptions of each app.

3.2. INDIVIDUAL ABILITIES ASSESSMENT

For the first app, *Apk Analyzer*, all participants noted that a list of the smartphone's installed apps is displayed upon opening the app. Two participants immediately recognized that the app aimed to scan these listed apps. Only one participant noticed that the apps are listed alphabetically, with an option to change the sorting order. Additionally, four out of the twelve participants mentioned that the app contains too much unnecessary information for the average user. Specifically, they found the display of the package name in the app lists confusing and the numerous scan categories overwhelming and hard to understand.

Participants had similar reactions regarding the second app, *App Inspector*. They all reported seeing a list of apps upon opening the app. One participant observed the absence of a search field for finding apps, which is present in *Apk Analyzer*. The same four participants who criticized *Apk Analyzer* for excessive information found *App Inspector* more user-friendly because it does not display package names in the app list. Additionally, one participant noted the lack of a permission list in the scan results, a detail that went unnoticed by the others.

When using the third app, *APK-Info*, all participants noticed the differentiation between user apps and all apps. Furthermore, three participants identified the option to change the language, while the others became aware of this feature later. Two participants criticized the presentation of scan results, describing it as cluttered and resembling unprocessed raw text.

Throughout their experience with the first three apps, participants shared a common view regarding their design. All installed apps appear upon opening, and clicking on an app initiates a scan of the selected app. In contrast, the final app, MASS, elicited distinct impressions from the participants. Ten of the twelve participants appreciated the introduction to the app's functions. The remaining two participants acknowledged the tutorial's value but preferred to skip such steps for quicker app usage. All participants agreed that the design of this app was impressive, highlighting the card format for grouping apps as clearer than the list format used in the previous apps. Lastly, all but one participant was impressed with the interaction between the user and the app, deeming it an excellent design. The lone dissenter felt this interactive design hindered quick access to the app's functionalities.

- *Exploring app analyzers (First impressions)*: The participants' responses to the first impression of each app were similar to their answers

3.2. INDIVIDUAL ABILITIES ASSESSMENT

regarding what they observed in the app. For *Apk Analyzer*, opinions were mixed. Five out of twelve participants viewed the app positively, appreciating its simple design and well-structured layout. Two participants rated it as okay, acknowledging the simplicity but feeling overwhelmed by the amount of information provided and deeming the package name in the home menu unnecessary. The remaining five participants were dissatisfied, finding the design overwhelming and the scan results too complex to use. They also found the package name display in the start menu confusing, with three participants noting that the app seemed more suited for developers.

The *App Inspector* app was well-received for its straightforward design, with eight of the twelve participants appreciating the minimalistic presentation of the app icon and name, emphasizing that less is more for the initial app selection menu. Two participants found the app acceptable and praised its simplicity in ensuring tidiness. However, two participants criticized *App Inspector* for its limited information, lack of a search bar, and sorting options. These participants were aware that *App Inspector* provided the least amount of information in its scan results, a point of contention among them.

Regarding the *APK-Info* app, participant opinions were evenly divided: one-third rated it as good, one-third as okay, and one-third as poor. Positive feedback included the ability to cope with advertisements, as some participants rationalized that developers need to profit. The language setting was a unique feature that garnered praise, which was a significant factor for those who rated the app positively. Those who rated it as okay appreciated the clear distinction between normal and dangerous permissions in the scan results and the separation of all apps and user apps in the start menu for better organization. Conversely, participants who rated the app negatively were mainly bothered by the intrusive advertisements and found the arrangement of scan results chaotic and poorly designed.

Eleven participants had positive first impressions of the MASS app, while one had a negative view. The positive feedback highlighted the app's user-friendly tutorial with pictures, comprehensive and impressive scan results, an aesthetically pleasing color scheme with a dark background and golden and white fonts, interactive design requiring user approval for actions, and the feedback mechanism after each action, which made users feel guided. The flashing server locations on the map particularly fascinated these participants. The single participant with

3.2. INDIVIDUAL ABILITIES ASSESSMENT

- a negative impression cited difficulties with the English language used in the app and found the vocabulary too complex. This participant also found the constant interaction and confirmations distracting and annoying, in contrast to the positive feedback from the others, and preferred a lighter background color common in other smartphone apps.
- *Exploring app analyzers (Any uncertainties or lingering questions):* Regarding *Apk Analyzer*, there were no significant questions except for one unclear point. One participant did not realize the listed apps on the home screen could be clicked to access the scan results. They mistakenly thought that the list of apps itself constituted the scan results. In contrast, *App Inspector* confused two participants due to a similar issue. They were surprised by the limited information in the scan results and wondered if this was the full extent of the app’s capabilities. In *APK-Info*, all participants were initially unaware of the distinction between “users” and “all apps.” After a brief investigation, ten out of twelve participants understood the meaning, and the remaining two were subsequently informed. Finally, in *MASS*, one participant had an unresolved question about whether there was a level higher than the orange warning mark in the scan results summary of the privacy policy.
 - *Exploring app analyzers (Understand all UI elements instantly):* Regarding the question of whether the user interface was well designed, all participants agreed that it was effectively executed in all apps, with only minor flaws observed. In the case of *Apk Analyzer*, four participants failed to notice that the individual fields in the scan result were clickable to reveal additional information about each respective field. *App Inspector* exhibited no flaws in its user interface design. Its simplicity and limited amount of information contributed to its effectiveness. All participants found the design well-executed for *APK-Info*, with all touch interactions clearly visible. However, with the *MASS* app, two participants mistakenly believed that the permission icons in the app list were clickable and would open a new window with the corresponding explanations. Upon testing, they discovered that this functionality was not available.
 - *Exploring app analyzers (Share what you like and why):* When evaluating the positive aspects of *Apk Analyzer*, seven participants praised its simple and structured design in the scan results. One participant particularly appreciated the variety of information provided. However,

3.2. INDIVIDUAL ABILITIES ASSESSMENT

the remaining four participants found nothing special about the app. *App Inspector* was also noted for its simple design. Four participants liked its straightforward approach, but the remaining eight did not find anything noteworthy. All participants appreciated the language settings in *APK-Info*. Among the twelve participants, five liked the distinction between user apps and all apps. One participant did not have any positive comments about this app. In the case of MASS, all participants initially described its design as exceptional compared to the other apps. They also favored the presentation of scan results in fold-out (accordion) headings, which prevented information overload. The summary of privacy policies and the localization of app server locations were highly rated. Participants mentioned that none of the previous apps provided such extensive information. According to one participant, the information in the scan results was perfectly tailored to the average consumer and not overly technical.

- *Exploring app analyzers (Share what you dislike and why)*: For the *Apk Analyzer*, all participants concurred that the package name could be omitted. They justified this by noting that the package name was unknown during the interview and found it to be an unnecessary burden. Three out of the twelve participants disliked the simple design, describing it as boring. Additionally, half of the participants expressed an urgent need for information filtering in the scan results, speculating that much of the information was aimed at developers. Regarding *App Inspector*, all participants agreed that the scanning results were insufficient quantitatively and qualitatively, rendering them useless. Over half of the participants (seven out of twelve) stated they would uninstall the app immediately due to its perceived lack of usefulness. *APK-Info* was the only app that contained advertisements, which several participants noted. Five participants immediately identified the advertisements and considered them a source of dubiousness. Of these five, two participants understood that the developers needed to profit somehow. At the same time, the other three indicated a preference for a one-time fee to eliminate advertisements before installing the app. Furthermore, three additional participants criticized the unattractive presentation of the scan results, expressing a desire for more symbols, graphics, and statistics. Lastly, there were two criticisms of the MASS app. First, four suggested removing the deep scan button that appears after selecting an app, as it was redundant. Second, one participant found the constant requests for confirmation to be annoying.

3.2. INDIVIDUAL ABILITIES ASSESSMENT

- *Exploring app analyzers (Change or add something? Why?):* The participants proposed several changes across all apps. Specifically, three participants desired to reduce the amount of information displayed in the *Apk Analyzer* app, focusing only on the most crucial details to avoid overwhelming users. In order to address this issue, a suggestion was made to introduce a setting targeted at researchers, developers, or regular users, allowing them to adjust the type and quantity of information based on their specific needs. Among the twelve participants, five requested that the app’s language be German and that the package name be omitted from the home screen list. Additionally, one participant recommended enhancing the visibility of the search bar, noting that it is currently easy to overlook. Furthermore, three participants suggested incorporating a tutorial to guide users through the app’s functionalities.

There were numerous suggestions for changes to the *App Inspector* as well. Four out of twelve participants preferred the app to support the German language. Two participants requested the addition of a tutorial. Three participants felt that the app currently lacks sufficient information, making it unusable in its current state. One participant suggested implementing a sorting feature similar to that in *Apk Analyzer*. Another three participants pointed out the absence of a search bar. Finally, two participants suggested redesigning the app to include icons and colors, as its current state is perceived as dull and unappealing.

In terms of participant feedback regarding the *APK-Info* app, several key themes emerged. Four participants emphasized the importance of reintroducing the language setting despite its availability. They noted that the current presentation of this feature was not sufficiently highlighted and requested clearer visibility. Additionally, two participants advocated for integrating a tutorial within the app. Four others expressed a desire for a redesigned presentation of scan results, with one suggestion focusing on replacing textual permission listings with icons. Moreover, three participants suggested aligning the layout of all apps on the home screen with the *App Inspector* app, suggesting the exclusion of version numbers and package names in favor of a simplified display featuring only app names and icons.

While the MASS app received high approval from most participants, suggestions were still worth considering. Almost all participants, except one, expressed satisfaction with the current state of MASS. However,

3.2. INDIVIDUAL ABILITIES ASSESSMENT

some participants proposed ideas for future updates that could further enhance the app. Five out of twelve participants desired a language setting similar to the *APK-Info* app, suggesting it should be prominently featured in the tutorial to ensure visibility. Additionally, two participants proposed an innovative idea. During deep scanning of an app, results can be displayed progressively, akin to loading parts of a web page when scrolling down. This approach shrinks the scan duration by allowing interaction with already-loaded information.

- *Comparing app analyzers*: Most participants favored the MASS app across all areas. In the first question regarding which app elicited the strongest initial reaction, all participants except two out of twelve chose the MASS app, with unanimous positive feedback about the app. The single vote for the *APK-Info* app was due to its language setting, catering to a participant's preference for German due to language difficulties. Another vote for the *Apk Analyzer* app stemmed from a participant feeling overwhelmed by the amount of information presented, which aligned with their initial strong reaction. The remaining participants were impressed by the design of the MASS app, which influenced their choice.

In subsequent questions on which app was most understandable, contained the most useful information, and was overall preferred, eleven participants consistently voted for the MASS, while one participant consistently chose the *APK-Info* for the same reason of the availability of the German language. The reasons mentioned by participants who voted for the MASS app predominantly focused on its design, comprehensive information, and quality. Participants noted that the MASS app differs significantly from other scanning apps in design and data presentation. Instead of a conventional list, the MASS uses a card format on the home screen and accordion-style headings in scan results, which were praised for user-friendliness. Participants appreciated the app's animations and color scheme, highlighting a distinct user experience. One participant remarked on the MASS's unique structure: "[...] with MASS the structure is completely different, here I realized that this is in a different league and when I saw the server information, that was wow [...]." Another participant expressed a preference for the MASS app due to menus that do not overwhelm with information upfront but require interaction to reveal details: "I like the fact that these menus do not list everything immediately, but that you have to click on it yourself first and then see the information."

3.2. INDIVIDUAL ABILITIES ASSESSMENT

A significant difference noted with the MASS compared to other apps is its effective presentation of input data in a usable format. Participants confirmed that information derived from static analysis tools can be useful and interesting to end users despite their unfamiliarity with such tools prior to using the MASS app. Participants also appreciated the inclusion of a privacy policy summary in the MASS, which was absent in other apps. One participant noted during a deep scan: “Okay, what I like about this app is that the other apps have not addressed the privacy policy; this app does. So this one shows you that. Not very detailed either, but still enough [...].” Another participant appreciated how the MASS summarized extensive information succinctly: “[...] ah look, what was just so much at TikTok is summarized here in small sentences. That’s a good idea for this app.” The privacy policy summary helped participants understand why certain permissions are necessary, confirming another hypothesis: using summarized privacy policies alongside MobSF information enhances user understanding of personal data usage. Additionally, participants found the MASS easy to use, particularly noting its initial permission request upon app launch. Familiar terminology used within the MASS contributed to its ease of understanding, with most participants recognizing all terms except for two (package name and APK). A participant mentioned, “I was familiar with most of the terms because I worked in this field, but there were also things I had no idea about, but the last app (MASS) had given me the ability to get information on demand.”

Interview Section 3: Analyzing TikTok During the interview, participants were assigned to scan the TikTok app using one of four scanning apps. Eleven participants chose the MASS app, while another opted for *App Inspector*. However, the participant who chose *App Inspector* encountered challenges that prevented task completion. In contrast, the majority successfully completed their tasks using the MASS app.

In task 3A, participants recognized the permissions TikTok requests during installation and comprehended their purposes. All participants who utilized MASS successfully accomplished this task without difficulty. Task 3B presented greater difficulty, as only eight MASS users correctly identified the specific information TikTok stores locally on devices. Nevertheless, those who completed Task 3B using MASS also succeeded in Task 3C, which required them to pinpoint where this stored information resides within the app or device. Additionally, ten out of eleven participants who employed MASS successfully completed the final tasks, 3D and 3E. Task 3D entailed

3.2. INDIVIDUAL ABILITIES ASSESSMENT

identifying who can access the stored information and for what purposes, while Task 3E focused on understanding the user rights associated with personal data within the TikTok app.

Comparing the outcomes of this section to those of the initial part highlights the significant assistance the MASS app provided in addressing previously unanswered questions. Specifically, four participants tried to remember and verbally explain the findings from the first section during this stage. However, this approach was considered inadequate since the task strictly demanded solutions derived exclusively from the scanning app.

Interview Section 4: Participants Feedback Towards the end of the interview, participants provided feedback on the study, the topic, and their future cautiousness regarding apps. All participants confirmed they had gained significant knowledge about Android’s permission model, distinguishing between dangerous and normal permissions. Eight of the twelve participants expressed interest in using scanning apps like MASS privately, driven by curiosity about other apps. Among these eight, three insisted on the app being available in German. One participant explained, “I can see myself installing something like this. If the app can explain terms in German, it would be really interesting.” The remaining four participants declined to use scanning apps privately, sharing nearly identical reasons. One participant noted, “Yes, it makes sense to take a look at it, but I personally would not read it because I could not do much with it. Nevertheless, it is interesting.” Overall, ten participants became more aware of privacy policies and permissions. In the future, they plan to look at permission requests to ensure they are truly necessary. Two participants acknowledged that apps like Instagram access their data and track behavior, but they felt powerless to change this if they wished to use the app. One participant suggested promoting such apps through advertisements to generate more interest, while another proposed integrating the scanning process into the Google Play Store system post-installation to streamline information access.

Eight Golden Rules of Interface Design Participants were expressive in their praise for the design of the MASS app, which raised the question of why it resonated more strongly with them than other apps. To delve into this, one could apply Shneiderman’s eight golden rules for interface design (Wong, 2023) to evaluate the app designs. These rules provide a structured framework focusing on principles such as consistency, feedback, error prevention, and user control. By systematically assessing how well the MASS app adheres to these principles, one can identify specific reasons why participants found it more appealing or effective. This approach highlights the app’s design

3.2. INDIVIDUAL ABILITIES ASSESSMENT

strengths and pinpoints areas where it excels in user experience, offering valuable insights into its success. Table 3.1 presents an evaluation of interface design across four apps, including MASS, *App Inspector*, *APK-Info*, and *Apk Analyzer* based on Shneiderman’s Eight Golden Rules.

- *Strive for consistency*: All apps maintained a consistent interface design except for *APK-Info*, which exhibited inconsistency in how it displayed “permissions.” Some permissions were shown with a mix of lowercase and uppercase letters (e.g., com.android.vending.BILLING), resulting in a less uniform appearance. In contrast, the other apps adhered to a cohesive grid layout and design across all pages. Notably, the MASS app implemented a user-friendly interface featuring two tabs: one for selecting apps and another for displaying scan results, ensuring seamless navigation between these functions.
- *Seek universal usability*: All apps, except *App Inspector*, achieved universal usability. MASS, for instance, provided a tutorial for first-time users, ensuring smooth onboarding and allowing advanced users to initiate app searches, which boosted efficiency independently. *App Inspector*, however, provided a uniform experience without considering user familiarity levels. *APK-Info* included language options to cater to users unfamiliar with English, whereas the *Apk Analyzer* app offered a customizable dark mode feature.
- *Offer informative feedback*: Only the MASS app consistently offered informative feedback for user actions. For instance, when users initiated a “Deep Scan” in MASS, they were notified about the scan’s duration, which ensured transparency. In contrast, other apps did not provide such feedback, leaving users unsure about the results of their actions.
- *Design dialogue to yield closure*: Each app had clear action sequences with clear endpoints, indicating task completion through scan results. However, some users found *App Inspector* unsatisfactory because they perceived its results to contain minimal information.
- *Offer simple error handling*: All apps universally met the criterion of effectively avoiding errors during user interactions.
- *Permit easy reversal of actions*: After scanning an app, all apps allowed users to easily undo actions, typically by navigating back using device or app controls.

3.2. INDIVIDUAL ABILITIES ASSESSMENT

- *Support internal locus of control:* Only the MASS app empowered users by offering them control over their scanning preferences, allowing them to choose between scanning all apps or specific ones. This flexibility was not available in other apps.
- *Reduce short-term memory load:* All apps met this criterion to different extents. Apps such as *App Inspector* and MASS adopted minimalist designs, presenting only essential information to reduce cognitive load. In contrast, *APK-Info* and *Apk Analyzer* included additional details such as version numbers and package names, which might overwhelm users unfamiliar with their significance.

Table 3.1: Interface Design Evaluation Based on Shneiderman’s Eight Golden Rules

| | MASS | App Inspector | APK-Info | Apk Analyzer |
|-----------------------------------|------|---------------|----------|--------------|
| Strive for consistency | Yes | Partial | Partial | Yes |
| Seek universal usability | Yes | No | Yes | Yes |
| Offer informative feedback | Yes | No | No | No |
| Design dialogue to yield closure | Yes | Yes | Yes | Yes |
| Offer simple error handling | Yes | Yes | Yes | Yes |
| Permit easy reversal of actions | Yes | Yes | Yes | Yes |
| Support internal locus of control | Yes | Limited | Limited | Limited |
| Reduce short-term memory load | Yes | Yes | No | No |

Discussion and Limitations

This study investigated the potential influence of security analysis tools on improving user awareness and aiding decision-making concerning Android application permissions and privacy policies. The empirical findings reveal significant gaps in users’ understanding of smartphone privacy and security, with only a minority of participants having professional or educational backgrounds. Despite recognizing the importance of privacy and security, behaviors such as rarely reviewing app descriptions or privacy policies highlight a paradox between awareness and proactive actions (Kokolakis, 2017). Most participants installed apps via the Google Play Store, demonstrating a preference for perceived safety. Nevertheless, they paid little attention to app descriptions or privacy policies, underscoring the need for approaches that bridge this gap. Challenges in understanding app permissions and privacy policies, especially with complex apps like TikTok, revealed the inadequacy of current presentations, which are often too technical and lengthy. Participants struggled to identify permissions and comprehend privacy policies, indicating that existing methods fail to provide accessible and transparent information (Scoccia et al., 2021).

3.2. INDIVIDUAL ABILITIES ASSESSMENT

The study’s introduction of app analyzers exposed a significant knowledge gap, as none of the participants had prior experience with these tools. However, once introduced, participants engaged with them effectively, particularly favoring the MASS app. The MASS app’s user-friendly design, interactive elements, and comprehensive information presentation were consistently praised, underscoring its potential to enhance user understanding and management of app permissions and privacy. This preference highlighted the importance of user-centered design in developing privacy tools (Wong and Mulligan, 2019). The positive feedback for the MASS app, compared to mixed reviews for other tools like *Apk Analyzer*, *App Inspector*, and *APK-Info*, suggests that tools designed with the user in mind can significantly improve comprehension and engagement.

Participants’ evaluations provided valuable insights into effective app design. The MASS app stood out for its intuitive interface, clear presentation of information, and interactive features, which aligned with Shneiderman’s eight golden interface design rules, particularly regarding consistency, feedback, and user control (Wong, 2023). In contrast, other apps like *Apk Analyzer* were criticized for overwhelming users with excessive information, while *App Inspector* was deemed insufficient in providing useful data. *APK-Info* was noted for its cluttered and confusing scan results presentation. These critiques emphasize balancing comprehensive information with clarity and accessibility to avoid overwhelming users.

Practical implications of these findings include the necessity of simplified information presentation, where such tools should use summaries, icons, and visual aids to enhance user comprehension. Incorporating interactive and engaging designs, such as tutorials, feedback mechanisms, and step-by-step guides, can facilitate learning and keep users engaged (Ahmad Faudzi et al., 2023). Customization and flexibility are also crucial, allowing users to adjust the amount and type of information displayed based on their familiarity and needs, catering to both novices and advanced users (Lallé and Conati, 2019). Language support is essential to increase accessibility and usability for non-English speakers, ensuring that tools are available in multiple languages with clear visibility of language settings and localized content. Additionally, promoting awareness and usage of privacy tools through advertising and integration with platforms like the Google Play Store can encourage more users to engage with these tools proactively.

However, there are two types of limitations in this work. First, the study limitations include participants having varied levels of knowledge about privacy policies, Android, and smartphone security. Although daily smartphone users were interviewed, it would be better to have participants with similar

3.2. INDIVIDUAL ABILITIES ASSESSMENT

knowledge levels for more consistent feedback. While data saturation was achieved, indicating the number of participants was valid, a larger sample could provide more potentially different insights. Second, technical limitations in the implementation of the MASS app were noted. When the MASS app was developed, there was no dynamic API for summarizing privacy policies, so the summary was hardcoded. During the pilot study, the MobSF API server setup for app scanning encountered issues. Initially running on Google Cloud Run, it faced a limit of 32 megabytes for apps, such as TikTok, requiring the MobSF API to be hosted locally. Furthermore, other research statistical analysis tools could not be used as they either did not support the current Android version or were no longer developed.

Overall, the study demonstrates that static analysis tools combined with privacy analysis features can significantly enhance user awareness and inform decision-making regarding Android apps. The findings underscore the importance of continuous improvement and user-focused development in this area. By addressing identified challenges and incorporating user-centered features, developers can create more effective privacy tools that empower users to manage their smartphone security proactively. The refined research question remains relevant, providing a focused yet flexible framework for exploring the potential of these tools to improve user awareness and decision-making in an evolving digital landscape.

Acknowledgments

This section is based on the master’s thesis:

Menderes Akyüz. 2022. *The App is Here - Would You Like to Use it? MASS: Static Analysis of Android Applications Based on MobSF and Polisis*. Unpublished master’s thesis. University of Bremen.

My contribution to this work: Conceptualization, data curation, formal analysis, investigation, methodology, project administration, resources, partial software development, supervision, validation, and visualization.

3.2.4 Key Insights of Abilities Assessment

Study 4: Infographics Enhance Game-Based Learning

This study investigated how infographics influence performance in an educational game focused on smart home security. The findings revealed that players exposed to infographic feedback demonstrated significantly higher performance in answering questions correctly compared to those who received textual feedback. This aligns with the Fogg Behavior Model, which posits that simplifying tasks enhances users' ability to perform them. By presenting complex information in a visually engaging and easily digestible format, infographics have increased users' ability to understand and retain the content. Moreover, the study highlighted the motivational benefits of infographics. Players reported higher perceived competence. The sense of mastery and empowerment instilled by the visually appealing format encouraged further engagement with the learning content. This enhancement in self-efficacy translated into greater intrinsic motivation, as users felt more competent and confident in their abilities to tackle security challenges.

Study 5: Critical Data Flows in Mobile Applications

This study focused on the *HappyPermi* app, designed to improve user comprehension of Android permissions through visualization techniques. The app effectively illustrated where users' data is sent and the implications of granting permissions, addressing the often obscure processes associated with data handling by apps. This clarity aligns with the FBM's principle of increasing ability by simplifying complex tasks. The study found that 69% of users chose to turn off contact permissions, demonstrating a practical understanding of the potential risks associated with unnecessary data access. This proactive management of privacy settings reflects enhanced self-efficacy, as users felt capable of making informed decisions to protect their privacy. High usability scores further reinforced the connection between effective visualization, increased ability, and user engagement. Interestingly, the lack of significant emotional differences between the two studied versions suggests that decisions to manage permissions were primarily based on cognitive understanding rather than emotional responses. This indicates that the visualization techniques used by the app successfully enhanced users' self-efficacy and ability to make informed privacy decisions independent of emotional influence.

Study 6: Informed Decisions via Mobile App Analyzers

This study examined the impact of static and privacy analysis tools on user awareness and decision-making regarding Android application permis-

3.2. INDIVIDUAL ABILITIES ASSESSMENT

sions. The study revealed significant gaps in users' understanding of privacy and security, highlighting the inadequacy of current methods for presenting permissions and privacy policies. Participants frequently overlooked app descriptions and privacy policies, demonstrating a disconnect between awareness and proactive actions. However, the introduction of the MASS app, with its user-friendly design and clear presentation of information, significantly improved user engagement and comprehension. Participants favored the MASS app for its intuitive interface and interactive elements, underscoring the importance of user-centered design. This preference highlights how tools that simplify information presentation and enhance usability can bridge the knowledge gap and improve users' ability to manage app permissions.

The positive feedback for the MASS app aligns with the FBM's emphasis on enhancing ability through simplification. By presenting comprehensive information in an accessible manner, the app increased users' perceived competence, thereby boosting self-efficacy. This increase in self-efficacy led to more informed and proactive behavior, as users felt confident in their ability to understand and manage app permissions and privacy policies.

Integration of Theories and Findings

These studies collectively demonstrate that visualization techniques such as infographics and user-centered designs significantly enhance users' perceived abilities in managing privacy settings and implementing security measures. According to the Fogg Behavior Model, enhancing ability by simplifying tasks is crucial for behavior change. These visualization techniques effectively simplify complex information, making it more accessible and understandable for users. Self-efficacy theory further explains the impact of these techniques on user behavior. Visualization techniques boost users' self-efficacy by increasing perceived competence, leading to higher intrinsic motivation and a greater likelihood of adopting informed behaviors. The studies showed that when users feel more confident in their abilities, they are more proactive in managing their privacy settings and security measures.

The strategic integration of visualization techniques within mobile and ubiquitous applications interacts positively with users' self-efficacy beliefs, enhancing their intrinsic motivation and promoting the consistent adoption of informed behaviors. The study findings confirm that simplifying complex information and improving usability empower users to make informed decisions about their privacy and security. This interaction between enhanced perceived abilities and increased self-efficacy leads to more proactive and informed behavior, aligning with our second research question in this work. Thus, visualization techniques effectively improve user comprehension

3.2. INDIVIDUAL ABILITIES ASSESSMENT

and play an essential role in fostering a sense of empowerment and confidence, essential for sustained engagement and behavior change in the digital landscape.

RQ2

How do visualization techniques in ubiquitous and mobile applications enhance users' ability to manage security settings, interact with their self-efficacy, and promote informed behaviors?

By addressing Research Question 2, we explore the pathway from self-efficacy to informed behavior through ability within the model (see Figure 3.34). This question examines how users' skills and understanding influence their capacity to make informed choices in privacy and security contexts. Using HCI approaches such as interactive visualizations, simplified infographics, and user-centered security tools, we made complex security information more accessible and easier to comprehend. This pathway emphasizes that enhancing user ability fosters confidence and empowers individuals to manage privacy and security tasks effectively.

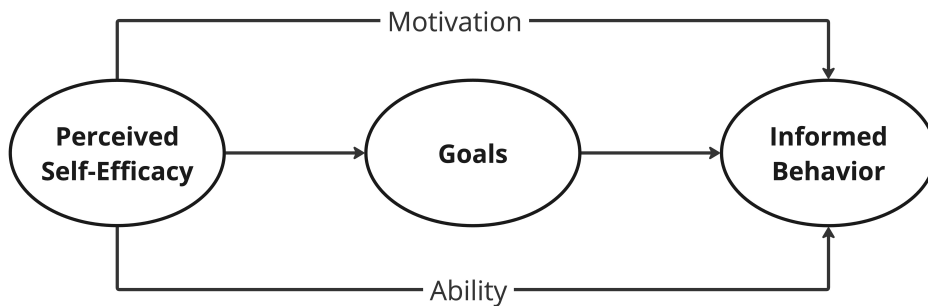


Figure 3.34: Pathway from self-efficacy to informed behavior via ability

3.3 Behavioral Prompts Identification

Triggers are the third cornerstone of the Fogg Behavior Model. They encompass three distinct categories: sparks, facilitators, and signals. Sparks are aimed at individuals with high ability but low motivation, seeking to ignite interest or urgency through compelling cues, such as notifications or alerts. On the other hand, facilitators target scenarios where motivation is high, but ability may be lacking, simplifying tasks or reducing barriers to action with clear instructions or accessible tools. Signals, applicable when motivation and ability are elevated, serve as timely reminders or prompts that reinforce behaviors at appropriate moments, like calendar reminders or push notifications. To explore the role of triggers in the domain of mobile security, we have conducted three studies. These studies investigate how different triggers influence user behaviors and decision-making processes in managing privacy and security challenges within mobile apps and smart home devices.

The first study focuses on sparks and signals within a gamified Android simulator. It aims to improve users' ability to assess privacy and security risks during app installation and configuration. By comparing interfaces like the Android App-Info page and a user data access profile, we investigate how these triggers influence user awareness and understanding of app configurations and permissions. The second study examines facilitators in the design of one-pager privacy policies for smart home apps. Testing various formats such as list, tab-based, and device-based representations, we explore how facilitators simplify user interactions with privacy settings. The study aims to enhance usability and comprehension of privacy policies, ensuring users can easily navigate and understand their privacy options. Lastly, the third study investigates signals, simple reminders, or notifications presented at strategic times to influence users' privacy-related behaviors in smart home apps. By integrating signals during setup, on-demand access, and just-in-time consent needs, we explore how these triggers prompt users to make informed decisions and actively manage their privacy preferences.

These studies collectively highlight the importance of designing effective triggers that accommodate varying user motivations and abilities. By enhancing user engagement and understanding of privacy measures, these approaches aim to empower users to navigate mobile and ubiquitous applications securely and confidently.

3.3.1 Study 7: Raising Security Awareness with Summaries

Introduction and Background

Smartphone apps constitute a fundamental aspect of modern digital life, installed by numerous users seemingly without hesitation Barth et al. (2019). Despite this widespread adoption, users exhibit minimal concern regarding the voluntary disclosure of personal data necessary for successful app installations (Li et al., 2020). These unaware decisions increasingly cause the amount of data surrounding users to map their behavior, interests, and thoughts. Ultimately, they are under constant surveillance and provide more targets for attacks and infiltration (Michel and King, 2019).

Security mechanisms have been implemented and modified for smartphone operating systems to protect the user’s privacy. The permission system is an essential component of operating systems such as Android. Each Android app runs in its sandbox with restricted privileges. If an app needs to access resources or information outside its sandbox, it will ask for the appropriate permission(s) during installation or use. Once an app is installed, a summary of its properties, such as the permissions the app is authorized for, its memory usage, and specific features, including clearing the cache and deleting all data, are available in the “APP-INFO” screen under the Android app settings. Given that the APP-INFO screen does not pop up automatically, users may not constantly review or even be aware of it. Furthermore, studies have revealed that the permission mechanism is often ignored, and users’ comprehension is low (Kelley et al., 2012; Felt et al., 2012). Users may make a separate privacy and security assessment when interacting with such highly customized interfaces (Peruma et al., 2018). They might be comfortable with an app requesting location data for location-based weather forecasting. On the other hand, the same users may find it inappropriate for that same app to access Google account data retrieved for personalized advertising. This ambiguous perception of the app’s behavior and lack of knowledge could raise the risk of unintentional resource usage or installation. As a result, users must be informed about such malicious activities, which would reduce the risks of privacy and security breaches (Di Geronimo et al., 2020).

Previous studies have shown that while many smartphone users are aware of information security concepts, their smartphone protection behavior is poor, and they would benefit from education on potential information security risks (Das and Khan, 2016; Taha and Dahabiyeh, 2021). Furthermore, users might avoid configuring settings due to usability issues, opting for avoidance strategies instead of embracing more effective protective measures (Frik et al., 2022). In addressing the risks tied to personal data handling, Harbach et al.

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

(2014) explored the visualizing of these risks within the specific framework of Android app permissions. They extended Android’s permission dialogues to visually depict accessible private data, leading users to make informed decisions and pay more attention to permission settings. Research has proposed effective methods for enhancing user privacy management. Lin et al. (2014) suggested implementing privacy profiles to aid users in navigating settings, emphasizing the importance of understanding app permissions. Liu et al. (2016) developed a personalized privacy assistant based on user profiles, offering tailored recommendations for settings. Both approaches highlight the significance of user education and personalized guidance in improving privacy management. Additionally, “ProtectMyPrivacy” for Android detects and controls data access by third-party libraries, thereby enhancing user privacy (Chitkara et al., 2017). These innovations aim to empower users with informed decision-making and increased control over their personal data.

Considering the familiarity of Android users with app installation and device configuration, alongside the emerging potential of game-based learning to motivate and enhance knowledge acquisition (Krath et al., 2021), this study aims to compare the impact of two interfaces within a gamified Android simulator. Specifically, our research question in this study is: *How does the automatic appearance of the APP-INFO page, compared to providing users with summaries of their data inputs during app configuration, affect their ability to assess privacy and security risks?* To address this question, we devised a gamified Android simulator enabling users to simulate app store browsing, installation, and customization of privacy and security settings. Two representations depict the outcomes of installed and configured apps in the simulator. The initial version, referred to as the *App-Info*, offers a broad overview of the app and its functionalities, akin to the Android APP-INFO page. The second version, known as the User Data Access Profile (*UDAP*), provides a more comprehensive depiction of the personal data provided by the user. Employing a between-subject design, we conducted a comparison of the two presentations. The evaluation results reveal that participants who interacted with the *UDAP* version demonstrated greater accuracy in evaluating the privacy and security risks of targeted apps compared to the other group. These participants expressed enthusiasm for integrating the *UDAP* approach into the Android operating system, indicating a potential for raising security awareness.

Prototype Description

Concept We developed a gamified simulator app for Android, offering two versions named *UDAP* and *App-Info*. In this simulator, players assist

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

“Simon”, a tax consultant new to Android, in learning how to install and configure apps. The task involves installing four specified apps and entering the necessary information, with Simon’s personal data provided beforehand. The simulator focuses on installing and launching apps from four common categories: tools, games, health & fitness, and social media, commonly used by Android users (Appfigures and Statista, 2022). Player actions and choices during installation and setup are evaluated within the simulator. The development of the simulator followed an iterative and user-centered design approach (Abrás et al., 2004). An initial prototype was devised and assessed by potential smartphone users on the university campus. Feedback was collected through various means, including user interactions, observations, and discussions, covering interface clarity and navigation ease. This input guided refinements in design, leading to the simulator’s development via Android Studio. The prototype prioritizes augmenting users’ procedural knowledge by integrating gamification features such as storytelling, challenges, and feedback. The simulator mirrored the latest Android version and behavior from the Google Play Store as of March 2022.

Design The simulator features an interactive avatar that guides players textually and verbally. He introduces himself and presents his problem upon app launch. Players progress through dialogue by tapping the screen. Simon disappears after his explanation, allowing players to access the App Store icon. Throughout the simulation, he prompts players to install an app from the store, which, once installed, appears on the home screen. The simulated App Store mirrors the Google Play Store, enabling horizontal and vertical scrolling to explore various app categories (Figure 3.35 shows this setup).

Players view detailed information on a dedicated screen after selecting an app in the App Store. They can scroll down to read the full description and tap “See More” to view all required permissions. If a player decides to install the app and matches Simon’s desired category, it proceeds with installation; otherwise, he intervenes. After successful installation, Simon provides further instructions, including launching the app and configuring it according to preferences. The setup process remains consistent for all four applications, granting players control over required data. Users are prompted to create an account or skip this step upon app launch. Subsequent screens prompt for demographic details, which players can skip (see Figure 3.36).

The app permissions screen follows, allowing players to review and modify permissions if desired. Additional screens may request information on financial status, health, and religious affiliation, prompting players to decide if this data is necessary (see Figure 3.37).

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

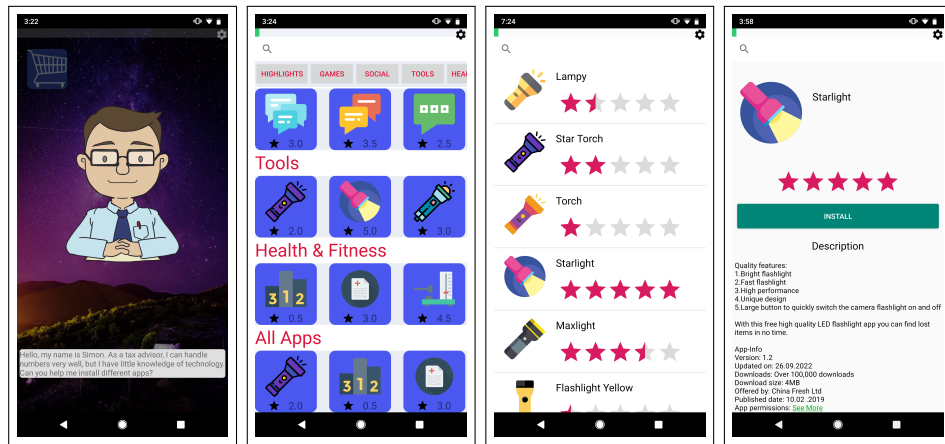


Figure 3.35: On the left side, Simon introduces himself; the App Store and the list of flashlight apps are in the middle, while information about the flashlight app is on the right.

Although users can decide what information and permissions the app categories require to run, we have considered certain requirements for each category. Therefore, after the last settings screen and before launching the app, the requirements are prompted depending on the app category. These requirements also play a crucial role in defining the risk level associated with each app. The flashlight app necessitates camera permission, which is considered high-risk due to privacy concerns. Seemingly innocuous apps seeking such permissions can still pose risks. For instance, the flashlight app could misuse camera access to capture media without consent. Additionally, when coupled with apparently harmless permissions like Internet access, the app could exploit data to compromise user privacy (Karthick and Binu, 2017). The game app's risk level is considered to be medium. Besides the normal permissions, such as Internet access, it requests permission to access the user's location, which introduces a moderate level of risk, as the app may share the user's location data within the app, potentially compromising privacy. While location data could enhance gameplay experiences, users should be cautious about sharing it. Conversely, the health & fitness app aims to be safe and low-risk. It requests health information, body sensor permission, and demographic data to function optimally and provides personalized health insights and guidance. The app's risk level is intentionally kept low, as its query data primarily revolve around improving the user's well-being and overall experience. Lastly, the social media app falls under the neutral risk category. Users must create an account, which involves sharing personal details like name, email, and password. Additionally, the app requests

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

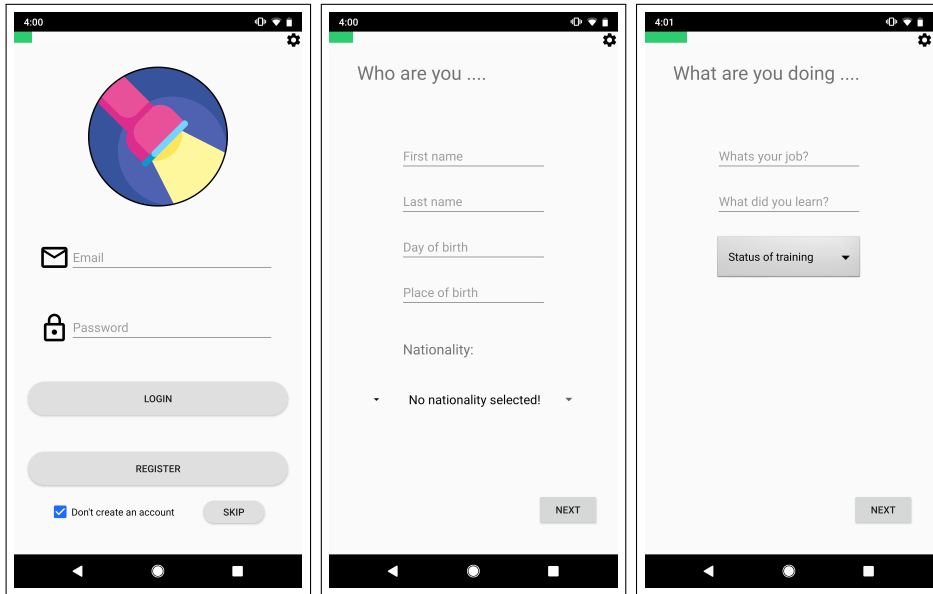


Figure 3.36: During this step, the user installs the desired app, in this case, a flashlight, and launches it for the first time. To utilize the app, the player needs to configure its settings. On the left, the player can create an account; in the middle, provide demographic information; and on the right, specify Simon's job occupation. The player must decide for each step whether this information is required when using this app.

camera permission to facilitate photo and video sharing. While the risk here is relatively balanced, users need to be mindful of the information they share on social media platforms, considering potential implications on privacy and security.

Simulator Versions After the players successfully install and set up the fourth app, they will encounter one of two screens based on their assigned group. In *App-Info* screen version, Simon pops up again and informs the player what kind of data and to what extent these four apps access his information. For this purpose, each installed app has an *App-Info* page, which mimics the foundational elements of the Info-Page of the latest Android. The player can navigate through the four *App-Info* pages with the left and right arrow keys and view the granted permissions. The app details are also accessible when the player scrolls down. This shortcut directs the player to the app store, providing more details about the app that the player may not have checked before installing. Alternatively, in the *UDAP* screen version, Simon explains how the *UDAP* functions and the information it offers. Similar to the previous one, the player can navigate between the *UDAPs* of the four installed apps. The *UDAP* representation consists of different sections. At

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

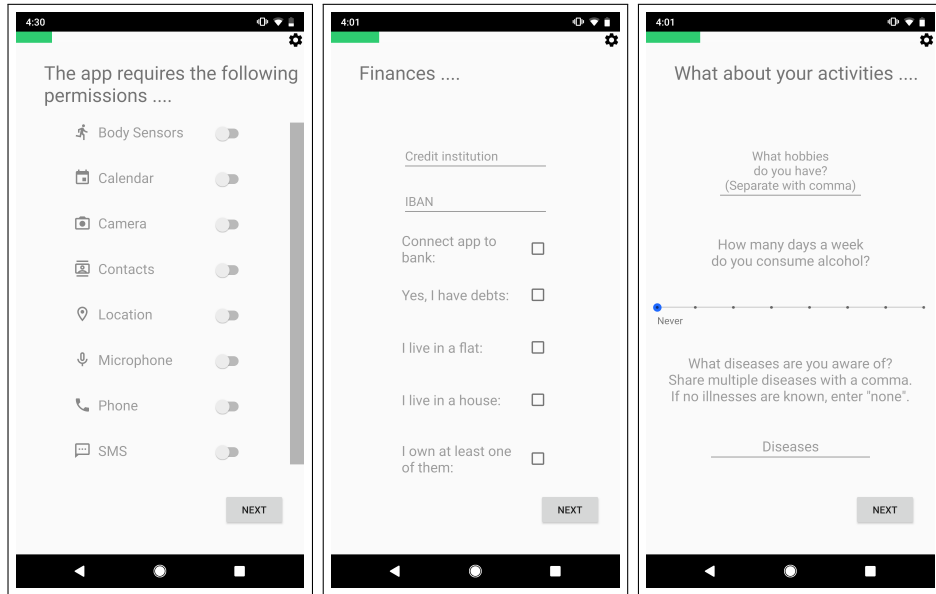


Figure 3.37: The three screenshots offer users various choices: granting permissions on the left, inputting financial information in the middle, and providing health information on the right.

the top, the name of the installed app, its corresponding category, and the app's icon are displayed. The Info button in the bottom left corner provides the player details about the colors used in the *UDAP*. Green indicates no issues with the category's settings, yellow signifies that some unnecessary data or permissions were granted, and red implies that the category has been incorrectly configured, potentially leading to personal information exposure. For instance, in the case of the flashlight app, when both camera permissions and internet access are combined, it opens up the possibility of data misuse. Consequently, in Figure 3.38, the standard permission category is shaded in red to denote this issue.

The *UDAP* incorporates eight sections that align with the information categories set up by the player within the app. Each *UDAP* category offers the player detailed insights into how their actions and the app's features may result in data leakage. The player can review all the entered data by tapping on a category. For each one, privacy and security statements are presented to the player. The privacy recommendations primarily center on protecting personal information and the right to control its dissemination. These guidelines advise users on how to limit the collection, usage, and sharing of their data. At the same time, the security recommendations revolve around safeguarding Android operating systems, networks, and devices from unauthorized access,

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

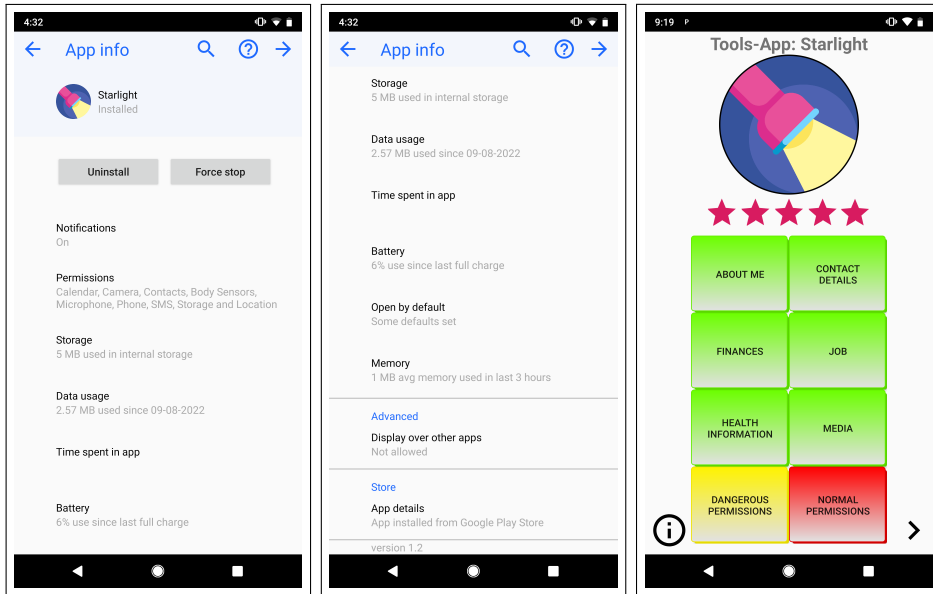


Figure 3.38: Simulator versions: left and middle: the *App-Info* version and right: the *UDAP*

cyberattacks, and data breaches. The explanations encompass both normal permissions, necessary for the app's regular functionality, and runtime permissions, also known as dangerous permissions, which provide the app with additional access to specified data or the ability to perform restricted actions (see Figure 3.39).

Feedback After completing the simulator, the player is awarded a star ranking based on the entered data. The player's granted permissions and entered data are compared against the recommendations for each app. When the player's decisions align with the advice, points are awarded. A maximum of 25 points can be earned per category, totaling 100 points across the four installed apps. Depending on the player's accumulated points, Simon expresses gratitude with three facial expressions: happy, neutral, or sad.

User Evaluation

Study Design Employing a between-subjects design, we carried out a user study involving 32 participants, equally divided into two groups of 16 each. These experiments took place in the laboratory, each session lasting about 50 minutes per participant.

Materials Two questionnaires were developed for the data collection. One questionnaire refers to the App-Info variant, and the other to the *UDAP* variant. Consequently, the results for the two variants were collected sepa-

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

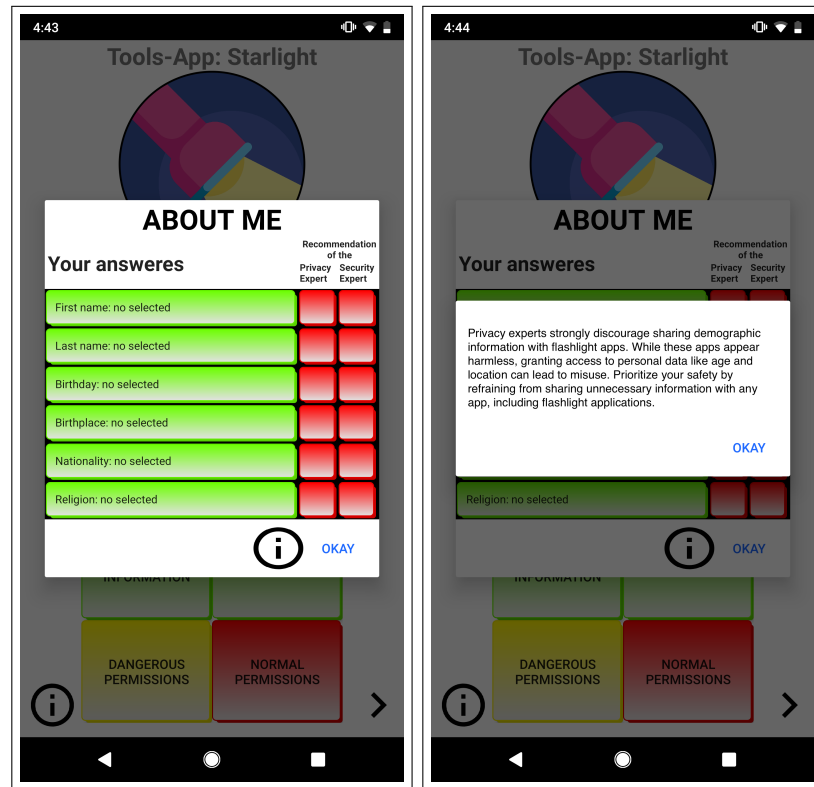


Figure 3.39: The screenshots guide users regarding the “About Me” category in *UDAP*, showing insights into possible data leakage from actions and app features. These insights are accessible through tapping and accompanying privacy and security statements.

rately to be evaluated afterward. Both questionnaire sections were identically structured to allow a comparison between the two variants. The pre-exposure questionnaires deal with the participant’s demographic information, including gender and age. They also include questions about installing an Android app to obtain the participants’ awareness and attitude toward this topic. The post-exposure questionnaires have three sections. In the first one, we requested participants to deliver an overall risk assessment concerning the four installed apps, utilizing a 5-point Likert scale that measures individuals’ risk perceptions from “Not Risky at All” to “Very Risky”. Participants then had to assess the privacy risk associated with each app requirement, including account creation, personal data, bank account information, health data, and claimed permissions. Similar to the initial section, 5-point Likert scales were employed for each inquiry, maintaining the same scope. Finally, the post-exposure questionnaires comprised specific questions about the respective simulator variants. The aim was to collect participant feedback regarding

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

their experiences with the specified simulator. They were asked to express their general opinion and address the potential and challenges of simulators. We provided each group a Google Pixel 2 XL featuring a 6-inch display to experience the prototype version. Appendix A.2 features the questionnaires.

Procedure We conducted the study in German, with exclusively German-speaking participants selected through a quota sampling strategy based on predetermined criteria. This recruitment approach aimed to obtain a sample of Android users who were unique to each condition. The participation was entirely voluntary and without remuneration. Participants were recruited through mailing lists, social networks, and word-of-mouth. Once participants provided informed consent, the study director instructed them to complete pre-exposure questionnaires. Following that, the study instructor explained the simulator’s functionality and provided instructions for the experiment. Participants then began playing the simulator according to the assigned version. After completing the simulator, participants were asked to fill out post-exposure questionnaires.

Participants In the *App-Info* group, 16 participants (8 female and 8 males) were between 18 and 31 years aged ($M = 25, 1$, $SD = 3.7$). Within the *UDAP* group, 16 participants (7 females and 9 males) were between 19 and 32 years old ($M = 25, 7$, $SD = 3.16$). All participants used the Google Play store to search for and install new apps. Regarding the information they look for before installing a new app, all respondents indicated that they pay attention to the name of the app they seek and whether it is cost-free. In the *App-Info* group, seven respondents said they check for ratings and reviews of the apps, as do 11 respondents in the *UDAP* group. Two participants in each group also pay attention to the app description.

We asked participants if they pay attention to app permissions and decide whether or not to use an app based on those permissions and if they can identify whether the requested permissions are essential. In the *App-Info* group, only one user sometimes attends to permissions. 2 participants rarely, and 13 of them never. Fifteen stated that permissions do not influence their decision to use an app. Only one person specified rarely. 2 participants in this group stated that they could sometimes understand why an app requests permissions. Twelve participants were not able to, and 2 participants rarely. Among the *UDAP* group, four users rarely pay attention to permissions, and 12 never do. Fifteen of them stated that permissions do not influence their decision to use an app or not, and only one person rarely. 2 participants in this group said they rarely know why an app requests permissions, and 14 participants cannot understand.

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

Following these questions, we further asked participants how concerned they are about their privacy when installing a new app and whether they can quickly determine whether an app violates their privacy. In the *App-Info* group, 5 participants indicated concern about their privacy, and six were somewhat concerned. Two participants are neutral, one is relatively unconcerned, and one is unconcerned. Eleven participants stated that they could never tell if an app violates their privacy, four users rarely, and only one person frequently. Within the *UDAP* group, 5 participants reported concern about their privacy when installing a new app; nine users are somewhat concerned, and two are neutral. Regarding whether an app violates their privacy, 9 participants can never determine this, and seven users can rarely find out.

Empirical Findings

Overall Risk assessment Participants were asked to assess the overall risk of the four installed apps. We applied statistical analysis to determine possible differences between the two groups. An alpha level of 0.05 was used for all statistical tests. The independent t-test Student (1908) demonstrated that participants in the *UDAP* group ($M = 4.81$, $SD = 0.4$) considered the flashlight app significantly riskier ($t(30) = -4.25$, $p < .001$, $Cohen'sd = -1.5$) than participants in the *App-Info* group ($M = 3.31$, $SD = 1.35$). The independent t-tests for the other three app categories revealed no significant differences between the two conditions ($p > .05$) (see Table 3.2).

Table 3.2: Overall Risk Assessment of Game, Health & Fitness, and Social Media

| | Game | | Health & Fitness | | Social Media | |
|----------------|----------|------|------------------|------|--------------|------|
| | App-Info | UDAP | App-Info | UDAP | App-Info | UDAP |
| Mean | 3.44 | 4.06 | 3.13 | 2.44 | 3.44 | 3.69 |
| Std. Deviation | 1.26 | 0.77 | 1.41 | 1.09 | 1.41 | 1.35 |

Categories Risk assessment We asked players in both groups to evaluate the risks of 5 categories of requested data, including account creation, personal data, bank account information, health data, and requested permissions in each app category.

- **Tools:** The independent t-test showed that participants in the *UDAP* group ($M = 4.88$, $SD = 0.45$) found creating an account significantly riskier ($t(30) = -5.53$, $p < .001$, $Cohen'sd = -1.95$) than participants in the *App-Info* group ($M = 3.25$, $SD = 1.13$). The players in the *UDAP* group ($M = 4.94$, $SD = 0.25$) perceived entering personal

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

data to be riskier ($t(30) = -3.08$, $p = 0.004$, $Cohen'sd = -1.09$) than players in the *App-Info* group ($M = 4.13$, $SD = 1.03$). The statistical test confirmed that asking for bank account data was riskier ($t(30) = -3.17$, $p = 0.003$, $Cohen'sd = -1.12$) for the *UDAP* players ($M = 4.94$, $SD = 0.25$) than for the players in the *App-Info* group ($M = 4$, $SD = 1.16$). Similarly, giving camera permission was riskier ($t(30) = -2.27$, $p = 0.03$, $Cohen'sd = -0.8$) for participants in the *UDAP* group ($M = 3.94$, $SD = 0.77$) than for the *App-Info* group ($M = 3.38$, $SD = 0.62$). We did not find significant changes in giving health information between the *App-Info* group ($M = 4.31$, $SD = 1.14$) and the *UDAP* group ($M = 4.88$, $SD = 0.34$) ($p > .05$) (see Figure 3.40).

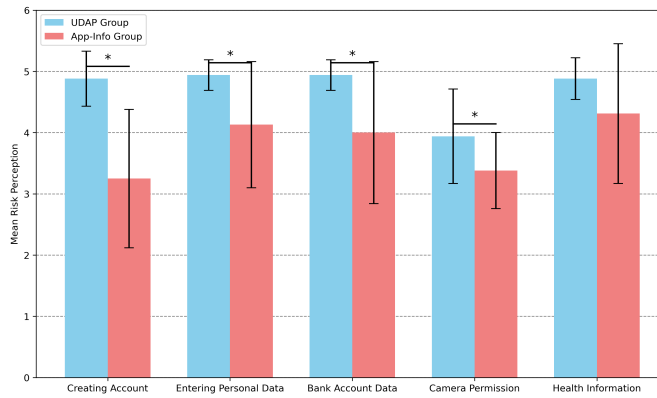


Figure 3.40: Risk perception comparison between the *UDAP* and *App-Info* groups across five data requests related to tools.

- Games:** The independent t-test revealed that participants in the *App-Info* group ($M = 3.56$, $SD = 1.03$) found creating an account significantly riskier ($t(30) = 3.96$, $p < .001$, $Cohen'sd = 1.4$) than participants in the *UDAP* group ($M = 2.13$, $SD = 1.03$). The statistical test indicated that asking for bank account data was riskier ($t(30) = -3.05$, $p = 0.005$, $Cohen'sd = -1.08$) for the *UDAP* players ($M = 4.88$, $SD = 0.34$) than for the players in the *App-Info* group ($M = 3.75$, $SD = 1.44$). The players in the *UDAP* group ($M = 4.88$, $SD = 0.34$) perceived entering health data to be riskier ($t(30) = -2.51$, $p = 0.018$, $Cohen'sd = -0.87$) than players in the *App-Info* group ($M = 4.15$, $SD = 1.15$). Granting location permission was also riskier ($t(30) = 2.18$, $p = 0.037$, $Cohen'sd = 0.77$) for participants in the *App-Info* group ($M = 4$, $SD = 0.82$) than for the *UDAP* group ($M = 3.44$, $SD = 0.63$). We did not find significant changes in giving personal data between

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

the *App-Info* group ($M = 3.63$, $SD = 1.59$) and the *UDAP* group ($M = 4.0$, $SD = 0.52$) ($p > .05$) (see Figure 3.41).

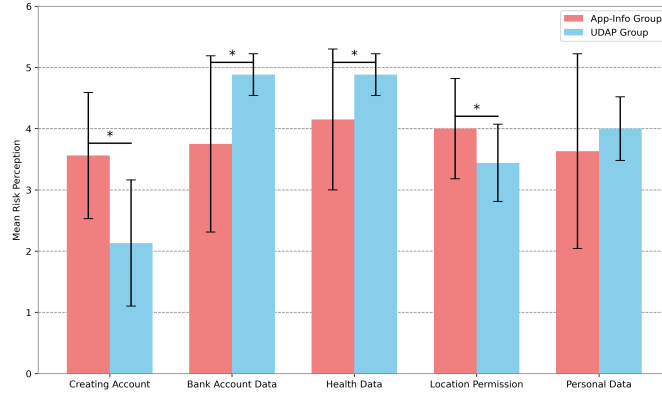


Figure 3.41: Risk perception comparison between the *UDAP* and *App-Info* groups across five data requests related to Games.

- Health & Fitness:** The independent t-test indicated that asking for bank account data was riskier ($t(30) = -3.07$, $p = 0.005$, $Cohen'sd = -1.08$) for the *UDAP* players ($M = 4.63$, $SD = 0.72$) than for the players in the *App-Info* group ($M = 3.13$, $SD = 1.82$). The participants in the *App-Info* group ($M = 3.5$, $SD = 1.55$) perceived entering health data to be riskier ($t(30) = -2.15$, $p = 0.040$, $Cohen'sd = -0.76$) than participants in the *UDAP* group ($M = 2.63$, $SD = 0.5$). Granting body sensor permission was also riskier ($t(30) = 3.51$, $p = 0.001$, $Cohen'sd = 1.24$) for players in the *App-Info* group ($M = 3.25$, $SD = 1.39$) than for the *UDAP* group ($M = 1.88$, $SD = 0.72$). We observed no significant differences in setting up an account and entering personal data ($p > .05$). The risk assessment mean scores for account creation were 3.06 ($SD = 1.44$) for the *App-Info* group and 2.25 ($SD = 1.13$) for the *UDAP* group. For entering personal data, the risk assessment mean scores were 3.19 ($SD = 1.68$) for the *App-Info* group and 3.25 ($SD = 0.45$) for the *UDAP* group (see Figure 3.42).
- Social Media:** The statistical test indicated that participants in the *App-Info* group ($M = 3.63$, $SD = 1.2$) found creating an account significantly riskier ($t(30) = 4.44$, $p < .001$, $Cohen'sd = -1.57$) than participants in the *UDAP* group ($M = 1.94$, $SD = 0.93$). There were no significant changes in the entry of personal data, bank account information, health data, and granting camera permission ($p > .05$). The risk assessment mean scores of entering personal data were 3.63

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

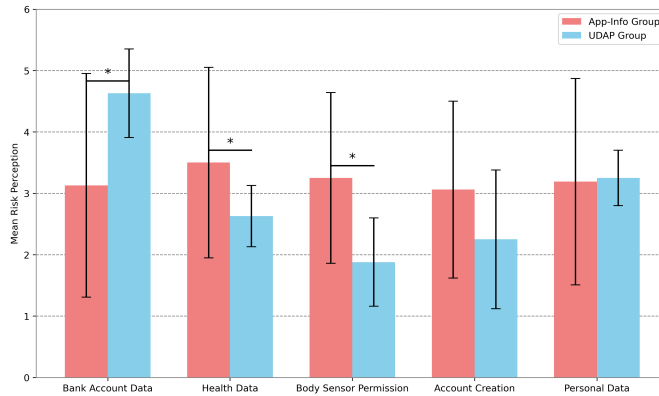


Figure 3.42: Risk perception comparison between the *UDAP* and *App-Info* groups across five data requests related to health & fitness.

($SD = 1.41$) for the *App-Info* group and 3.06 ($SD = 0.77$) for the *UDAP* group. For bank account information, mean scores were 3.88 ($SD = 1.54$) for the *App-Info* group and 4.63 ($SD = 0.81$) for the *UDAP* group. For entering health data, mean scores were 4.06 ($SD = 1.34$) for the *App-Info* group and 4.56 ($SD = 0.81$) for the *UDAP* group. The risk assessment mean scores of granting camera permission were 3.50 ($SD = 1.26$) for the *App-Info* group and 4.06 ($SD = 0.57$) for the *UDAP* group (see Figure 3.43).

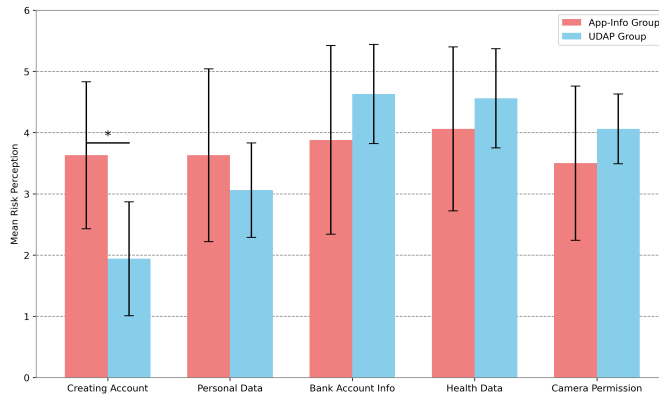


Figure 3.43: Risk perception comparison between the *UDAP* and *App-Info* groups across five data requests related to social media.

Participants Feedback Within the *App-Info* group, 14 participants stated that they were unaware of the *App-Info* page on Android, and only two used it sometimes. One player was very dissatisfied with the *App-Info* page providing enough security and privacy information about the particular app.

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

Seven participants were dissatisfied, and eight users were neutral. Fifteen participants stated that Android needs a mechanism to display security and privacy concerns regarding an app. Only one respondent indicated that this might be the case. All respondents indicated that a mechanism is required to provide more information on the privacy and security of apps. Three respondents specified that the goal of permissions should be more precise. Two respondents specified that this mechanism needs to be able to be turned on or off by users.

In contrast, all participants in the *UDAP* group indicated that they use the *UDAP* mechanism whenever they install new apps if it is available on their smartphone. Fourteen users were delighted that the *UDAP* provided enough privacy and security information about the particular app, and only two were satisfied. All respondents mentioned that Android requires the *UDAP* mechanism to indicate privacy concerns regarding an app. Similarly, all users reported wanting to see this mechanism on Android rather than in the Google Play Store. 12 participants claimed that the *UDAP* mechanism informed them very well, and they could quickly find out the privacy and security statements. 2 participants thought there should be a way for the *UDAP* mechanism to automatically set the apps according to the recommendations if requested by the user. One suggested displaying this mechanism before the app is launched so that users can get information beforehand.

Discussion and Limitations

In this study, we have investigated the impact of the automatic appearance of the APP-INFO page compared to providing users with summaries of their data inputs during app configuration on their ability to assess privacy and security risks.

It is evident from the findings that the *UDAP* group tends to have a more conservative and cautious approach, likely due to a heightened awareness of privacy and security issues, which is reflected in their accurate high-risk assessment of the flashlight app. This group's sensitivity to privacy infringements may derive from a more robust understanding or prior negative experiences with app permissions. On the other hand, the *App-Info* group's assessments of the game and social media apps indicate a slight understanding of risk that aligns well with real-world app usage scenarios, recognizing the trade-offs between functionality and potential privacy concerns (Wottrich et al., 2018). Their evaluations suggest that while they may not always perceive higher risks, they are attuned to the specific risks that are more prevalent or impactful. This divergence in risk perception highlights the critical need for developing effective educational tools and clearer privacy

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

information mechanisms (Frik et al., 2022). Such initiatives should aim to bridge the procedural knowledge and risk awareness gap, ensuring that all users, regardless of their initial awareness level, can make informed decisions about app installations and data sharing.

The qualitative feedback from participants provided further insights into their perceptions and preferences. In the *App-Info* group, many participants expressed a lack of awareness about the *App-Info* page on Android. Several participants expressed dissatisfaction with the level of privacy and security information provided on the *App-Info* page. They emphasized the need for Android to display more comprehensive privacy and security concerns regarding an app. Conversely, players in the *UDAP* group conveyed their readiness to incorporate the *UDAP* interface into their routine for installing new apps, expressing satisfaction with its capability to furnish privacy and security details. They emphasized the need for Android to integrate the *UDAP* mechanism rather than relying solely on the Google Play Store.

Some participants suggested additional features or improvements, such as automatic app configuration based on recommendations and displaying the *UDAP* before launching an app. These suggestions reflect users' desire for a more seamless and integrated experience supporting their decision-making while prioritizing privacy and security concerns. Overall, the study's findings demonstrate the potential of the *App-Info* and *UDAP* approaches to improve users' ability to assess privacy and security risks associated with app usage. By providing users with transparent and comprehensive information, these approaches can enhance users' procedural knowledge and contribute to a more privacy-conscious app installation process (Ebert et al., 2021). Further research and development could help refine these approaches and address users' needs and preferences, ultimately fostering a safer and more user-centered app ecosystem (Alsoubai et al., 2022).

While the study provides valuable insights, it is essential to consider its limitations for a comprehensive interpretation of the findings. The sample size was relatively small, and the study focused on German-speaking participants, limiting the generalizability of the results. Our comprehension of the impact of the feedback mechanism (facial expressions: happy, neutral, or sad) on participants' post-exposure responses remains limited, leaving a gap in our knowledge of how this mechanism shapes individuals' answers following their exposure to certain stimuli or experiences. Moreover, the reliance on self-reported data introduces the possibility of biases and subjective interpretations. A simulated environment may not fully capture real-world app usage scenarios, potentially affecting participants' behavior and risk assessments. Additionally, the study focused on specific app categories, potentially

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

overlooking risks associated with other types of apps and comparing only two interfaces, which might cover only a portion of the complete range of possibilities

Acknowledgments

This section is based on the publication:

Mehrdad Bahrini, Joffrey Weglewski, Karsten Sohr, and Rainer Malaka. 2024. *Empowering User Security Awareness and Risk Assessment Within Gamified Smartphone Environment*. In *Entertainment Computing – ICEC (ICEC 2024)*. Springer, Cham. DOI: 10.1007/978-3-031-74353-5_2

My contribution to this work: Conceptualization, data curation, formal analysis, investigation, methodology, project administration, resources, part of software development, supervision, validation, visualization, and contribution to all parts of the manuscript.

3.3.2 Study 8: Smart Home App One-Pager Privacy Policy

Introduction and Background

Our recent study highlighted the importance of presenting users with a concise summary of the data they input during the initial setup of smartphone apps. This mechanism empowered users to make informed decisions, significantly influencing their privacy and security risk assessment accuracy. Participants expressed keen interest in integrating this approach into mobile operating systems, suggesting its potential to bolster security awareness. In addition to privacy and security settings, which are typically adjustable after the initial use of apps, users are immediately greeted with the app’s privacy policy upon launching mobile applications for the first time. This policy outlines the terms and conditions governing data handling and user privacy. Subsequently, users are prompted to provide explicit consent, indicating their understanding and agreement to adhere to these policies. This act grants authorization for the utilization of the application’s functionalities.

The necessity for user consent in such agreements stems from the imperative to address privacy and security concerns. For instance, the development of a smart environment entails a system comprised of distributed sensors and devices designed to gather extensive data about the physical environment and its occupants. The success and appropriateness of this smart home system hinge upon the quantity and quality of information it collects. Consequently, smart home service providers gather and aggregate vast amounts of end-user data (Almusaylim and Zaman, 2019). Despite users’ awareness of data collection by their smart home devices, they often lack control over how companies utilize their digital footprints. This lack of control creates a significant information disparity, as users are uncertain about the handling of their personal data once it is disclosed (Clark et al., 2015; Kang et al., 2015; Tabassum et al., 2019).

Tackling such concerns, the EU General Data Protection Regulation (GDPR) has implemented a set of legal obligations, which took effect on May 25, 2018, governing the processing of personal data for businesses operating within or handling data of EU citizens. This legislation aims to uphold the utmost transparency and control, striking a balance between data subjects and recipients of their information. The introduction of the GDPR underscores the significance of providing stakeholders with essential information regarding data protection, reinforcing requirements for obtaining valid consent from data subjects, and expanding their rights, particularly concerning information and disclosure (IT Governance Privacy Team, 2020). Consequently, privacy policies have become the primary avenue through

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

which service providers communicate their data processing practices. Given that smart home control systems feature a user interface interacting with devices such as tablets, smartphones, or computers, GDPR mandates that application users, akin to web users, are informed about collecting, using, and processing their personal data. Articles 12, 13, and 14 of the GDPR outline detailed guidelines for crafting policies, emphasizing ensuring their clarity and accessibility. Hence, smart home vendors, like others dealing with end-user data, must prioritize GDPR compliance when formulating their data privacy policies. However, beyond meeting regulatory requirements, it is equally imperative for manufacturers or trusted third parties to provide smart home users with reliable, impartial information. This proactive approach helps minimize the likelihood of users making uninformed decisions about their personal data (Haney et al., 2021) and should be customized to address recipients' specific requirements (Kolter and Pernul, 2009).

On the flip side, the current design patterns employed in privacy policy interfaces pose significant challenges for user experience (Jensen and Potts, 2004; Luger et al., 2013; Kitkowska et al., 2020b). A survey on data protection by the European Commission one year after the application of the GDPR shows that from the 60% of Europeans who read the privacy policies, only 13% read them thoroughly (Wigand and Soumillion, 2019). The limited engagement with privacy policies can be attributed to their wordiness and complexity, as they are commonly lengthy and written in a difficult-to-understand language (Fabian et al., 2017). This complex and wordy format often leads users to ignore such information (Milne and Culnan, 2004) to focus on digital production objectives (Tabassum et al., 2018; Obar and Oeldorf-Hirsch, 2020).

Various approaches have been explored to enhance users' understanding of privacy policies in an organized and interactive manner (Brodie et al., 2005; Kelley et al., 2009; Reinhardt et al., 2021). Studies have indicated that users prefer a compact, contextual presentation of privacy policies that includes a simple abstract of all statements, summarised by short labels (Reeder et al., 2008; Lipford et al., 2010). Kelley et al. (2010) developed a standardized table format for privacy policies that is readable and concise. They found that their representation enabled users to better and more quickly understand privacy policies. Furthermore, researchers have investigated different approaches to improve the readability and comprehensibility of privacy policies by using modality methods, such as combining images with text (Chen et al., 2011), and personalization through the use of personal pronouns (Needham, 2011) and highlighting text (Choe et al., 2013) to illustrate potential consequences for data subjects. Visual enhancements, such as textured consents utilizing

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

factoids, vignettes, and iconic symbols, significantly increase user engagement compared to plain-text presentations (Kay and Terry, 2010). Additionally, the visual interactive design of privacy policies leads to higher attractiveness, stimulation, novelty, and transparency than a standard policy with long text (Reinhardt et al., 2021). In order to motivate users to pay more attention to privacy policies and raise awareness, enhancing them with more visual approaches and different representation formats has shown to be specifically beneficial (Tabassum et al., 2018). Visual assistance such as animations or comics in consenting digital products provides distinct motivation and convenient understanding (Poneris et al., 2018; Kitkowska et al., 2020a).

Despite efforts to improve awareness and dissemination of data protection rights and information, especially post-GDPR, users have not necessarily benefited. Privacy policy interfaces have grown significantly in length in terms of syllables, words, and sentences (Linden et al., 2018). Since smartphones are the primary interface for interacting with smart home devices, reading lengthy texts on small screens can be challenging and ineffective (Raptis et al., 2013). Therefore, various graphical user interface designs and input methods for mobile devices have been explored to manage and display more content on a single screen effectively. These designs focus on the overall layout of the user interface, including aspects such as scrolling and tabs (Balagtas-Fernandez et al., 2009; Raneburger et al., 2013). Harms et al. (2015) compared scrolling, tabs, menus, and collapsible fields for navigating long forms on devices with small screens. They discovered that scrolling performed the least effectively among the methods, whereas the other three designs performed equally well, providing a more comprehensive overview. Tab-based prototypes offer users an efficient way to navigate the system and quickly access the desired information (Kilsdonk et al., 2016). This approach is particularly effective when dealing with a limited number of content groups or tabs, typically five or fewer (Griffith, 2017). Furthermore, by segmenting long forms into different tabs with clear labels, the tab-based approach helps minimize the cognitive load by avoiding displaying an overwhelming list of choices on a single screen (Zhang and Adipat, 2005).

In an effort to streamline privacy statements, the German Federal Ministry of Justice and Consumer Protection introduced a “Model for Data Protection Notices” on a single page on November 19, 2015 (Diercks, 2015). This brief document, commonly referred to as a “One Pager,” aims to help companies communicate their data processing practices transparently to consumers online. While these condensed versions endorsed by the ministry serve as supplementary resources, they do not replace formal privacy statements; rather, they provide a simplified overview of the key points. Later, researchers

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

compiled the GDPR requirements into a concise one-page privacy policy checklist and a user guide while providing a privacy policy template. The resulting approach featured simplicity and clarity, employing icons to outline sections and images to bolster user confidence (Renaud and Shepherd, 2018). Expanding upon the foundation of this one-page template, Faurie et al. (2020) explored the potential impact of various methods for presenting the privacy policy on user behavior and awareness, aiming to enhance users' understanding of their consent. Their findings demonstrated that the policy template, along with videos, significantly increased user awareness of the policy content and increased user satisfaction in terms of the usability of the privacy policy. The one-pager approach attempts to reduce the text length of privacy policies, simplify the language, and increase clarity (Feldner, 2020) and can significantly impact user awareness (Ebert et al., 2021).

Building on previous work on the one-pager concept, using applicable techniques and approaches that are simple to implement and preserve policies' effectiveness and transparency, this study investigates three different one-pager representations, including a *list*, a *tab-based*, and a *device-based* version in an attempt to make them more usable and keep the content clear and easy to understand. In this work, we specifically follow this research question: *What are the impacts of using a list, a tab-based, or a device-based representation for a one-pager privacy policy on users' perceived usability and workload in a smart home application?*

Findings derived from the study indicate that while the *list* condition was considered to have average usability, the *tab-based* and the *device-based* conditions were highly rated in this regard. The *tab-based* condition proved to be the most user-friendly and required less workload from users. Our contribution contains design recommendations for one-pager privacy policy representation that could improve the existing design. Adopting this approach could also assist smart home manufacturers in making smart home privacy more visible in their general privacy statements.

Prototype Description

Concept In pursuit of our research question, we crafted a mobile application that empowers users to manage their smart home devices while accessing relevant privacy policies. Employing a user-centered methodology, we iteratively gathered requirements to refine the prototype's development, drawing insights from user-centered design principles (Abrams et al., 2004) and mobile interface design guidelines (Gong et al., 2004). By integrating content from the Bosch Smart Home¹⁵ provider, we seamlessly incorporated their devices

¹⁵<https://www.bosch-smarthome.com/>

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

and respective privacy policies into our development. Our mobile application aids users in navigating data protection concerns, and it was not meant to be a replicated version of the Bosch Smart Home app.

General Design The iOS application is developed with a specific login process. Users must first create an account within the app to access its features. After completing the registration, users are presented with a privacy policy declaration outlining their rights, contact information, and handling of provided data. The main menu consists of four sections: devices, user, privacy policy, and further information, accessible at the bottom of the app. Notably, our three prototypes primarily differ in the privacy policy section. However, all other aspects of the prototypes remain identical. In the device section, users can add various smart home devices to their virtual setup by searching for specific devices or typing their names (see Figure 3.44). Upon adding a device, users are prompted to consent to its corresponding privacy policy, with the agreed-upon statements also included in the privacy policy section. The user section displays the personal information of the logged-in user, including first name, last name, username, and email. In further information, users have the option to log out or reset the application, removing all added devices and associated privacy policies. The reset feature is primarily designed for experimental purposes (see Figure 3.45).

Icon Design Drawing from design recommendations and insights gleaned from previous research (Egelman et al., 2008; Felt et al., 2016; Harkous et al., 2018), we incorporated an icon system to provide additional details for each heading. Across all three versions of the privacy policy presentations, we employed four types of icons: a green thumb, an exclamation mark, a blue gavel, and a person (see Figure 3.45). A visible green thumb indicates that the personal data of the user is not stored, either directly or via third parties. The presence of an exclamation mark signifies the storage of personal or sensitive user data, as well as the transfer of data to third parties, whether domestically or internationally. Additionally, it indicates that users are not notified when the privacy policy changes. The blue gavel is intended to highlight user rights (Rossi and Palmirani, 2019). Clicking on these segments provides users with information about their rights and the necessary steps to exercise them. When a person icon is displayed, the segment lists contact persons. Users can access information about icons by clicking the information button in the upper right corner of any app screen.

Privacy Policy Design We developed three versions of the privacy policy section for this app, drawing on previous research and user interface design guidelines (Balagtas-Fernandez et al., 2009; Raneburger et al., 2013; Harms

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

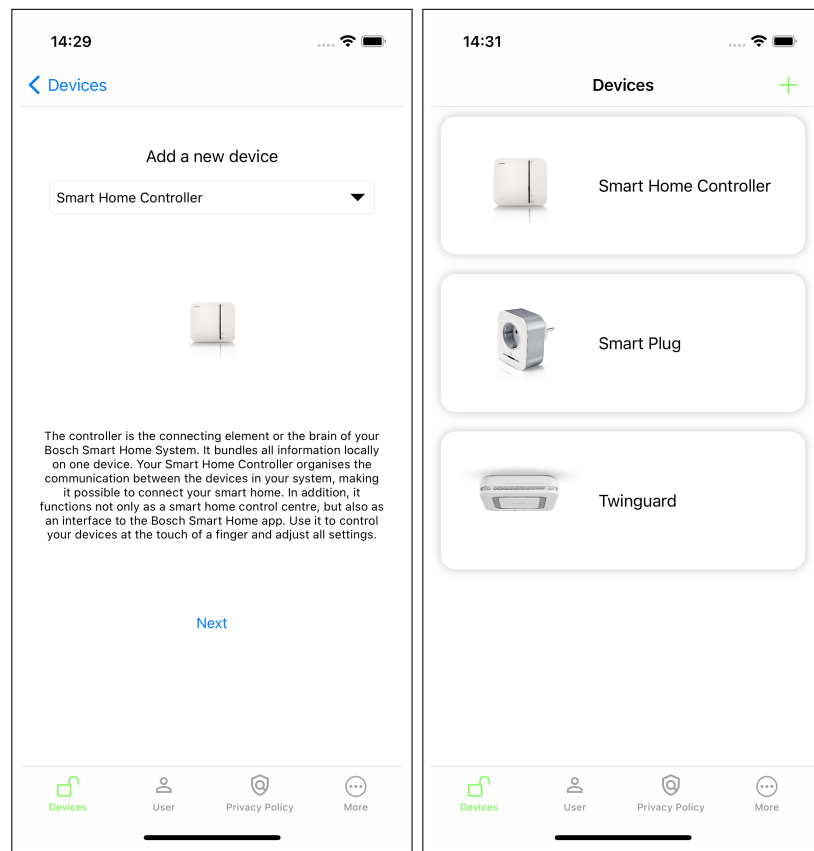


Figure 3.44: The screens on the left and the right display the devices section, where the participants have to look for certain devices and add them to their smart home.

et al., 2015). Across all versions, the privacy policy was summarized and segmented for clarity. Headings and segment texts were written in plain language to enhance understanding, avoiding acronyms and technical jargon. Our approach focused on personalized wording to facilitate user comprehension and engagement with the privacy policy (Redmiles et al., 2017). Rather than relying on generic statements, we utilized second-person narratives and personalized phrases such as “Your personal data...” and “You can...”. Each segment was summarized in a single line to emphasize key information, with the option for users to access further details by clicking on each segment.

The first version, known as the *List* interface, addresses the challenge of navigating on mobile devices when presenting a large amount of information on a small screen. Scrolling, commonly used in user interface design for browsing content like list views, is generally preferred over pagination (Punchoojit and Hongwarittorn, 2017). Within the *List* interface, the entire privacy policies are visible through scrolling (refer to Figure 3.46). This

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

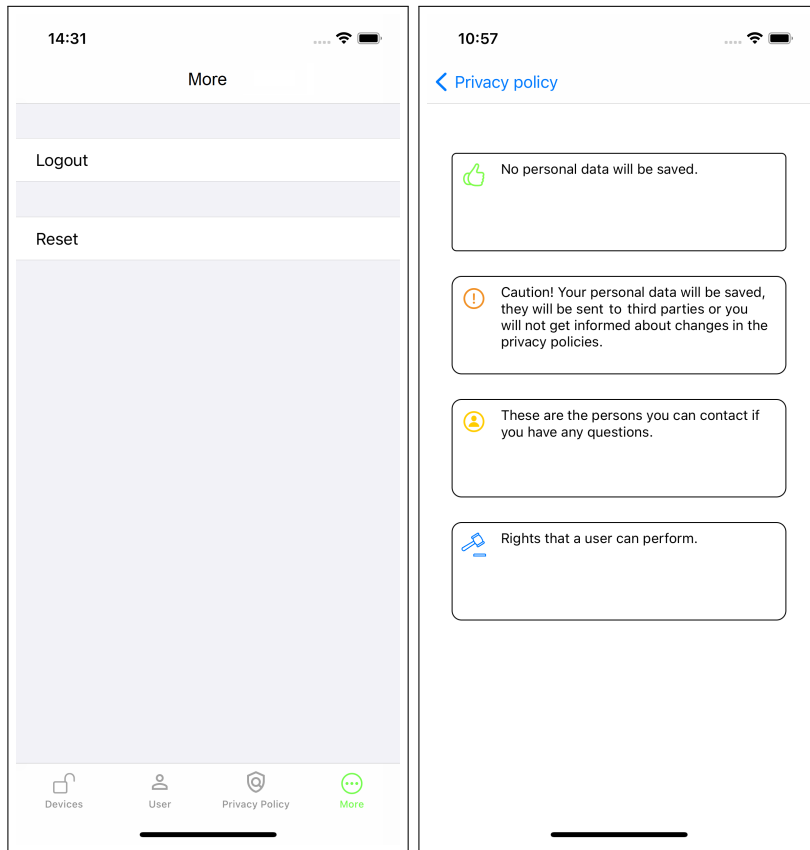


Figure 3.45: The screen on the left shows further information on where participants can log out or reset the app. The screen on the right side shows the explanation for the icons used in the prototypes to describe each heading further.

design choice offers users insights into data handling procedures, the necessity thereof, their rights, and available points of contact. Each segment features a simplified heading and an indicator, which can be clicked on to reveal summarized text, providing further details. This prototype version served as the experiment’s control group.

The second version introduces a *tab-based* interface. In accordance with design recommendations by Zhang and Adipat (2005), we divided the entire privacy policy into three tabs to consolidate information onto one screen, minimizing the need for scrolling. These tabs encompass “Data,” “Rights,” and “Contacts.” Within the Data tab, we detail the key aspects of data protection, covering processing, storage, deletion, and disclosure. Users seeking insights into how the smart home company handles their data can find comprehensive information here. The Rights tab enumerates all user rights under GDPR. Lastly, the Contacts tab provides information on

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

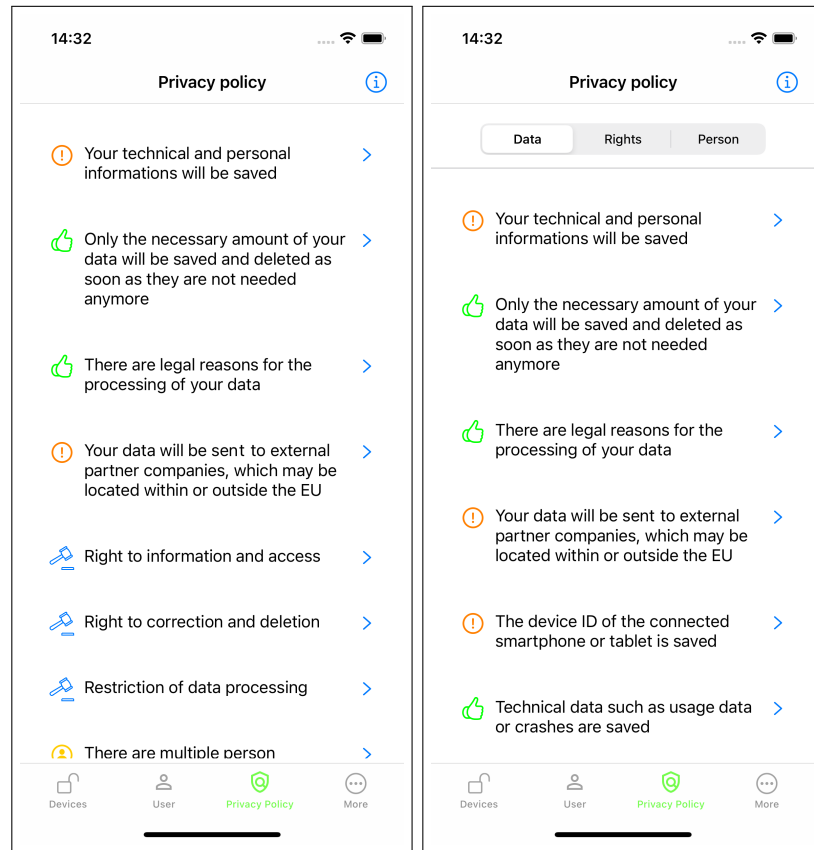


Figure 3.46: The privacy policy section: on the left is *List* interface, while on the right is *tab-based* interface.

individuals users can contact with questions about data protection. The layout remains similar to the previous version, with the main distinction being dividing the policy into three tabs (see Figure 3.46).

The final interface is *Device-based* and features two tabs. In the basic tab, users can view the data protection details agreed upon during registration. This tab encompasses GDPR-related user rights, contact information, registration data, and the rationale and duration of data retention. The secondary tab lists all devices added by the user. The *Device-based* interface employs just-in-time notifications (Almuhimedi et al., 2015; Schaub et al., 2015; Feng et al., 2021). Rather than presenting a single privacy policy upon launching the smart home application, privacy policies are seamlessly integrated into the app's functionality. By selecting a specific device, the corresponding privacy policy is promptly displayed. These policies are dynamically updated when new devices are added to the list (refer to Figure 3.47).

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

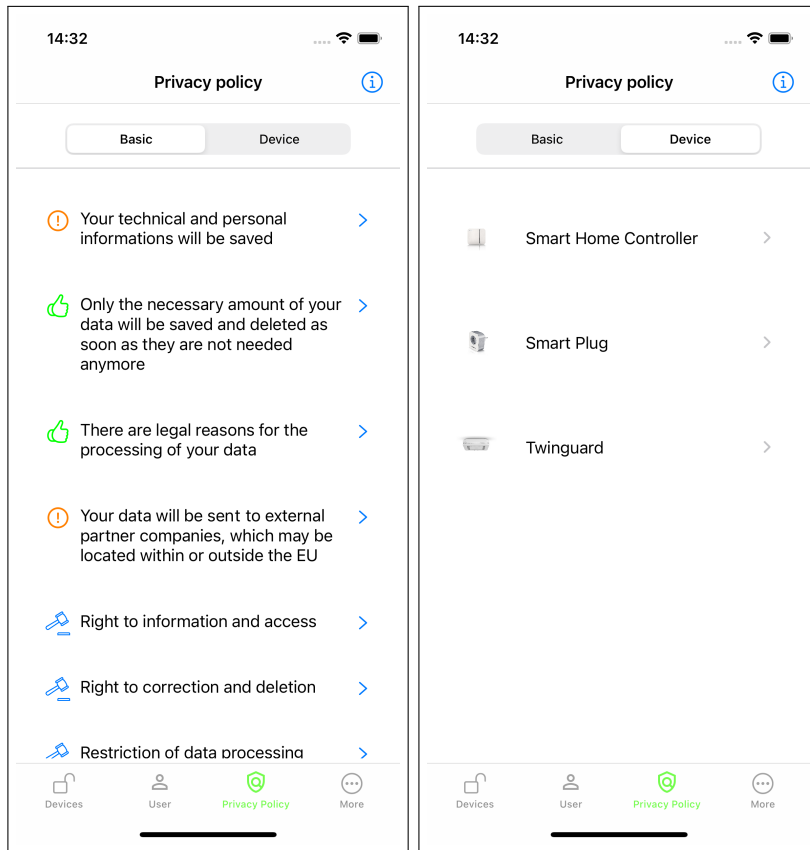


Figure 3.47: The privacy policy section: the *Device-based* interface

User Evaluation

Study Design We conducted an online user study with 30 participants employing our three prototype versions to evaluate the usability and user-friendliness of the privacy policy interfaces. Opting for a within-subjects study design, we ensured participants interacted with all three versions, compared them, and selected the most suitable in their opinion. This approach also reduced the required sample size and minimized random noise. Participants should set up virtual smart home devices within the app and respond to questions about data protection based on the app's privacy policy, which was presented in different formats. They did not need to install the app on their smartphones; instead, they remotely controlled it using the study conductor's emulator, accessible via Zoom's¹⁶ remote control feature. Participants received a survey link to answer study questions on their personal devices. The experiment sessions lasted approximately 45 to 75 minutes.

¹⁶<https://zoom.us/>

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

Materials We utilized standardized and customized questionnaires to measure users' workload and the perceived usability of the app. The standardized questionnaires employed were the raw NASA-TLX Hart and Staveland (1988) and the System Usability Scale (Brooke, 1996), both widely recognized measurement tools ensuring strong comparability. The NASA-TLX assesses six dimensions of workload: *Mental Demand*, *Physical Demand*, *Temporal Demand*, *Performance*, *Effort*, and *Frustration*. Meanwhile, the SUS evaluates usability based on ISO standards, encompassing effectiveness, efficiency, and satisfaction. At the conclusion of the study, participants were tasked with responding to a series of tailored questions. They were prompted to share their perspectives on the three representations, including which representation they found most appealing and why. Additionally, participants were asked to identify the strengths and weaknesses of each representation and offer suggestions for enhancement. One question solicited recommendations for an ideal representation based on the participant's preferences.

Statistical Analysis We conducted a repeated measures ANOVA test (Gir- den, 1992) to determine statistically significant differences between conditions, maintaining an alpha level of .05 for all statistical analyses. For the open-ended custom questions, we employed a summative content analysis approach involving counting and comparing keywords or content, followed by contextual interpretation (Hsieh and Shannon, 2005). Responses were scrutinized, with semantic units marked as codes and categorized by three researchers (Graneheim and Lundman, 2004). Numerical counts within each category were then elucidated within the context to enhance comprehension of participants' perceptions.

Procedure Upon providing informed consent, participants proceeded to answer a series of demographic questions. Following this, they were greeted with a welcome message and received an introduction to the app, familiarizing them with its functionalities and usage. The experimenter provided specific registration information to users beforehand to maintain anonymity. Subsequently, participants were tasked with setting up three new devices within the app and responding to a set of five questions concerning the data protection of these installed devices. To address these questions, participants had to refer to the privacy policy interfaces in the prototype. Once they completed these tasks, participants filled out post-exposure questionnaires. This process was repeated thrice for each participant, with each repetition involving the installation of three different devices and answering a new set of questions using a different format of the privacy policy. Thus, each participant underwent an assessment with all three prototype versions. We crafted

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

three sets of questionnaires, each comprising five multiple-choice questions. The first questionnaire contained questions about general policies, the second included questions about user rights, and the third contained device-specific policies (see Appendix A.3). For all participants, the questionnaires followed a fixed sequence. However, the order of conditions was counterbalanced using Latin squares to mitigate learning effects, ensuring an even distribution of responses to each questionnaire across all conditions.

Pre-Study We first performed a preliminary study involving three participants. This initial phase aimed to identify any potential shortcomings in the study’s design and assess the efficacy of its structure. The preliminary study was conducted online, with the study conductor sharing their screen with participants and granting them remote control over the prototype. Despite encountering occasional delays in screen sharing due to connectivity issues and latency, participants adapted well and successfully completed the study without significant disruptions. The pre-study revealed a few mistakes within the questionnaires, such as typos and formatting inconsistencies. However, participants encountered no difficulties while interacting with the app. Upon analyzing the pre-study outcomes, we implemented final adjustments to the questionnaires in preparation for the main experiment.

Participants The user study was conducted in German and involved only German-speaking participants. Participants were recruited through mailing lists, social networks, and word-of-mouth, with participation being voluntary and uncompensated. Prior to the study, an *a priori power analysis* was performed using *G*Power* (Faul et al., 2007) to determine the minimum sample size needed to address the research question effectively. The analysis revealed that to achieve 80% power for detecting a medium effect size, with a significance level of $\alpha = 0.05$, a minimum sample size of $N = 27$ for repeated measures ANOVA within factors was required. We successfully recruited 30 participants, with 11 identifying as female and 19 as male, exceeding the minimum requirement. Participants’ ages ranged from 23 to 55 years ($M = 28.73$, $SD = 8.19$), and we employed a quota sampling method for recruitment. All participants demonstrated adequate knowledge of computer and mobile interaction, though none were privacy experts. Regarding experience with smart home devices, seven participants reported having over four years of experience, eleven between one and four years, eleven less than a year, and one individual had no prior experience with such devices. Concerning the privacy policies of their smart home devices, twenty-two participants admitted to not having read them at all, eight had read only parts, and none had read the entire declaration.

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

Ethical Considerations In alignment with the ethical principles upheld throughout this dissertation, participants were instructed to anonymize their names before engaging in the study. Additionally, the consent form provided a link to Zoom’s privacy policy to ensure participants were informed. Throughout the Zoom session, participants were muted, and camera use was disabled. Any inquiries were to be communicated via the chat function, with the study director addressing them verbally over the microphone.

Empirical Findings

User Performance All participants provided responses to the data protection questions in each condition. In the *list* scenario, participants, on average, achieved a correct response rate of 82%. This rate increased to 90% for the *tab-based* condition and 87% for the *device-based* condition. Notably, we observed no significant differences among the three conditions in terms of correct responses. We also measured the average time taken by participants to respond to the data protection questions in each condition. The *tab-based* condition exhibited the shortest completion time, with an average of 6 minutes and 12 seconds, followed by the *device-based* condition at 6 minutes and 20 seconds, and finally, the *list* condition at 7 minutes and 16 seconds. However, we found no significant differences in the time taken to answer the questions across the conditions ($p > .05$).

Usability Concerning the usability of the app, the SUS scores achieved an average of 68.25 ($SD = 23.32$) within the *list* condition, 86.33 ($SD = 18.64$) within the *tab-based* condition, and 78.83 ($SD = 19.68$) within the *device-based* condition.

We performed a repeated measures ANOVA test to determine whether there were statistically significant differences in SUS scores between the three conditions. The assumption of sphericity was violated, as assessed by Mauchly’s Test of Sphericity, $p = 0.007$. Therefore, a Greenhouse-Geisser correction was applied ($\epsilon = 0.769$). The SUS scores elicited statistically significant changes between conditions ($F(1.54, 44.58) = 10.10$, $p < .001$, $\eta^2 = 0.26$). *Post-hoc* analysis with a Bonferroni adjustment revealed that the *tab-based* condition had significantly better SUS score compared to the *list* condition ($M = -18.08$, $p = 0.003$, $d = -0.67$) and the *device-based* condition ($M = 7.50$, $p = 0.049$, $d = 0.47$). It is also showed that the SUS score of the *device-based* condition was significantly higher than the *list* condition ($M = -10.58$, $p = 0.041$, $d = -0.48$) (see Figure 3.48).

Workload Dimensions Participants completed the NASA-TLX questionnaire for all three conditions as part of the evaluation process to calculate

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

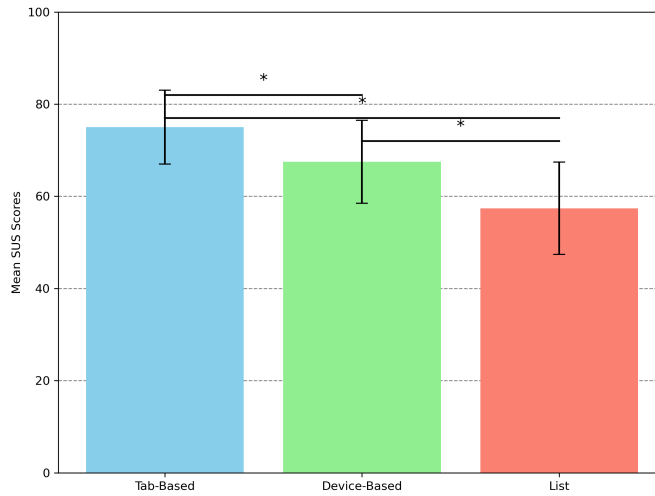


Figure 3.48: SUS scores comparison across conditions.

their workload. The overall task load was calculated for each participant and averaged across the various conditions on a scale between 0 and 100, where 100 is the highest. When the participants used the *list* condition to complete the tasks, they provided an overall mean unweighted workload of 40.72 ($SD = 18.10$), while for the *tab-based* condition, they rated an overall mean unweighted workload of 34.94 ($SD = 13.56$). In terms of the *device-based* condition, participants demonstrated an overall mean unweighted workload of 35.44 ($SD = 13.32$). The mean scores of the NASA-TLX dimensions are summarized in Table 3.3.

Workload Comparisons The repeated ANOVA test showed that there were statistically significant differences in terms of *Mental Demand* values between conditions ($F(2, 58) = 6.77, p = 0.002, \eta^2 = 0.19$). *Post-hoc* analysis with a Bonferroni adjustment revealed that the *tab-based* condition had significantly lower *Mental Demand* value compared to the *list* condition ($M = 11.50, p = 0.030, d = 0.50$). In addition, it is demonstrated that the *Mental Demand* value of the *device-based* condition was significantly lower than the *list* condition ($M = -11.83, p = 0.008, d = -0.60$). We did not witness any significant difference between *tab-based* and *device-based* conditions ($p > .05$).

Regarding *Physical Demand*, the repeated ANOVA test revealed significant differences between three conditions ($F(2, 58) = 11.64, p < .001, \eta^2 = 0.29$). *Post-hoc* analysis with a Bonferroni adjustment showed that the *tab-based* condition had significantly lower *Physical Demand* value compared to the *list* condition ($M = 15.50, p = 0.002, d = 0.69$). In addition, it

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

Table 3.3: NASA-TLX Dimensions

| | Conditions | Mean | SD |
|-----------------|--------------|-------|-------|
| Mental Demand | List | 53.50 | 23.38 |
| | Tab-based | 42.00 | 23.07 |
| | Device-based | 40.67 | 23.11 |
| Physical Demand | List | 35.17 | 23.87 |
| | Tab-based | 19.67 | 19.56 |
| | Device-based | 20.17 | 18.73 |
| Temporal Demand | List | 24.17 | 24.50 |
| | Tab-based | 20.17 | 19.99 |
| | Device-based | 22.17 | 20.96 |
| Performance | List | 54.00 | 23.36 |
| | Tab-based | 65.67 | 28.76 |
| | Device-based | 63.50 | 27.55 |
| Effort | List | 44.67 | 23.78 |
| | Tab-based | 30.67 | 20.71 |
| | Device-based | 35.83 | 21.86 |
| Frustration | List | 40.67 | 26.48 |
| | Tab-based | 31.50 | 21.34 |
| | Device-based | 30.33 | 21.61 |

is indicated that the *Physical Demand* value of the *device-based* condition was significantly lower than the *list* condition ($M = -15.00$, $p = 0.001$, $d = -0.72$). The data showed no significant difference between *tab-based* and *device-based* conditions ($p > .05$).

The analysis also showed statistically significant differences in *Effort* values between three conditions ($F(2, 58) = 5.44$, $p = 0.007$, $\eta^2 = 0.16$). *Post-hoc* analysis with a Bonferroni adjustment revealed that the *tab-based* condition had significantly lower *Effort* value compared to the *list* condition ($M = 14.00$, $p = 0.009$, $d = 0.59$). We did not witness any significant difference between *device-based* and *list* conditions ($p > .05$). The data also showed no significant difference between *tab-based* and *device-based* conditions ($p > .05$). In contrast, we did not find any significant differences for the dimensions of *Temporal Demand*, *Performance*, and *Frustration* between the three conditions ($p > .05$). Figure 3.49 3 shows the comparison of mean

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

NASA-TLX scores across six dimensions.

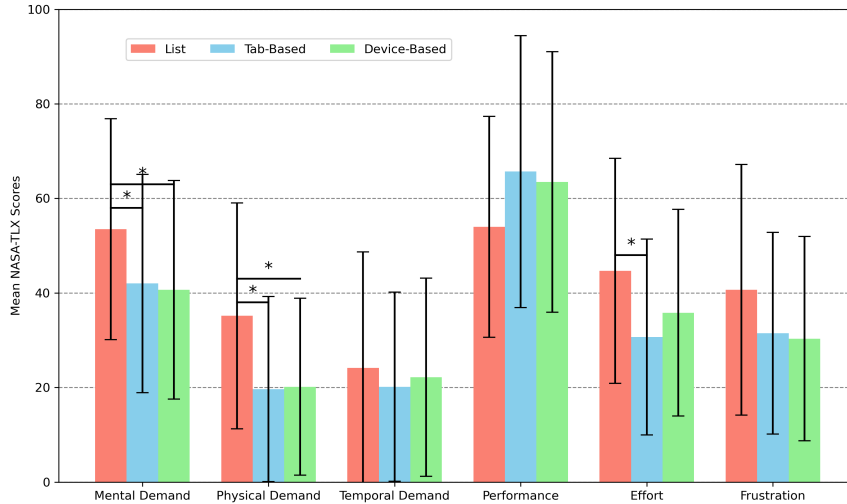


Figure 3.49: NASA-TLX Dimensions Comparison Across Conditions.

Exploratory User Responses The participants provided feedback on their opinions about each representation format. The initial question revolved around which representation was considered the best by the respondents. Twenty-three participants found the *tab-based* to be the best, while seven chose the *device-based*. None of the participants preferred the *list* condition. Respondents highlighted various points when considering the positive and negative aspects of our three prototypes. Four participants rated the simplicity of the *list* presentation positively. However, ten respondents found this version confusing and unclear. Additionally, eight participants pointed out that the presentation was lengthy. On the other hand, two participants highlighted the advantages of the classic representation of the privacy policy, mentioning that this layout is suitable as long as the privacy policy is kept short and everything is immediately visible at a glance. Lastly, four respondents mentioned that the presentation became quite long and confusing as soon as they added devices, resulting in the privacy policy getting longer.

With the *tab-based* prototype, nine participants appreciated the clear separation of the privacy policies into data, rights, and persons, and eighteen respondents mentioned that it made the interface clear and easier to follow. In addition, five participants positively noted that due to the separation into three tabs, the individual areas contained relatively small lists of privacy policies. They highlighted the advantage of viewing all information within each tab at a glance, which resulted in minimal or no need for scrolling through the lists.

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

In terms of the *device-based* prototype, eight participants found the division between basic and individual-specific privacy policies beneficial. Two respondents highly valued the tab feature, enabling direct device selection and immediate access to device-specific privacy policies. This design streamlined their ability to address device-related questions swiftly. Despite positive feedback, participants also identified negative aspects. Four participants found the naming of the tabs confusing, particularly *Basic*, which lacked clarity. Additionally, two participants noted the inconvenience of constantly switching between tabs. This confusion stemmed from participants' uncertainty about the content allocation between the basic and device tabs. Furthermore, one participant criticized the nesting depth of the device tab.

Participants provided various comments and suggestions for improvement. Three users criticized the icons used in the prototypes, finding them unclear. Additionally, four respondents felt that a missing feature was the search function, while two participants desired a filter function. Moreover, one user recommended the inclusion of a FAQ page for quick access to commonly searched information. A drawback of the *tab-based* presentation arose when devices were added. Three participants disliked the inability to immediately determine the newly added information in the privacy policy. Two suggested highlighting the recently added information using a marker. Eleven participants expressed a preference for a combination of *tab-based* and *device-based* prototypes for presenting privacy policies. Furthermore, one participant proposed incorporating gamification features, such as a reward system, to enhance individuals' willingness to engage with and read the privacy policies.

Discussion and Limitations

This study aimed to improve the one-pager privacy policy by employing various representation formats and investigating their effects on usability and users' workload. Consistent with prior research (Renaud and Shepherd, 2018; Faurie et al., 2020; Feldner, 2020), we found that the one-pager interface was a beneficial and promising strategy for enhancing usability and alleviating the burden of privacy statements for smartphone users. Participants stressed the importance of not being flooded with complex information, indicating a positive reception overall.

In terms of performance, participants in the *tab-based* condition demonstrated quicker response times compared to the other two conditions. However, no significant differences were observed regarding the time taken to answer questions and the accuracy of responses. Participants' feedback indicated that depending on the condition, scrolling through the list and the app's nesting depth extended the time spent searching for correct answers. Feedback on the

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

tab-based and *device-based* prototypes highlighted the benefits of separating and structuring the content of the privacy policy in a meaningful manner. These interfaces helped users better understand the information and provided a clear overview, aligning with findings from previous research (Reeder et al., 2008; Lipford et al., 2010).

Significant differences were observed in the usability ratings of the prototypes across the three conditions. While both the *tab-based* and *device-based* conditions received above-average usability scores, the *tab-based* prototype exhibited superior performance compared to the other two. Both the *tab-based* and *device-based* conditions received significantly higher ratings than the *list* version. This finding suggests that additional categorization and further structuring of the one-page format could enhance the usability and clarity of privacy policies. Participants were able to quickly locate the information they sought within the privacy policy, which was considered highly positive through user comments. However, it is essential to note that usability issues arose, particularly in the *device-based* condition, due to problems with tab naming. Once participants understood the content of each tab, they were able to navigate to their desired information swiftly.

We utilized NASA-TLX to measure perceived workload during interactions with privacy policy representations. Subsequently, the exploratory user responses in the study confirmed the questionnaire results. The segmentation of privacy policies played a crucial role in reducing the overall average workload among participants, which is consistent with research by Zhang and Adipat (2005) suggesting that dividing the lengthy text into tabs can alleviate the cognitive load.

In evaluating workload, the *tab-based* prototype received lower ratings than the other two conditions. Significant disparities were noted between the *list* condition and the other two regarding *Physical* and *Mental Demands*, as well as *Effort*. These results demonstrated that participants encountered greater mental and physical demands with the *list* prototype than with the other conditions. Consequently, representations with subdivision into multiple areas proved more suitable than the *list* representation in this regard. User feedback further supports this observation, indicating that while the *list* version initially appears straightforward, it becomes increasingly challenging to use over time. This trend is also evident in terms of *Effort*, as participants exerted significantly more steps when answering questions compared to the *tab-based* version. *Temporal Demand* was originally introduced in NASA-TLX as a measure of temporal pressure during a task, specifically how quickly tasks were performed. While this dimension is adept at addressing time-based scenarios, its relevance to our privacy tasks remains uncertain in its

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

current form. Therefore, the average values of the three conditions showed a very low demand on time by the participants. Regarding *Performance* and *Frustration*, the study results reflect positively, showing no significant impact on participants' ability to answer the questions presented.

Upon interpreting the quantitative results and participant feedback, it became evident that the *tab-based* version was rated the highest among the conditions and strongly preferred by participants. However, there is room for improvement in this concept. Segmenting data protection into distinct areas could be a logical step towards enhancing usability (Harms et al., 2015). Therefore, it is advisable to apply specific design principles. For instance, our study revealed that labeling tabs could confuse participants. To address this, clear and understandable names should be utilized. Additionally, incorporating sufficient explanatory text and employing appropriate visuals such as icons and images while avoiding complex computer terminology could enhance the interface's usability, particularly for users with limited computer literacy (Darejeh and Singh, 2013). As the length of privacy policies continues to increase (Amos et al., 2021), the list of different segments can still become lengthy despite subdivision into tabs. Other factors need to be considered to provide users with a quick overview of the data being processed. Approaches for managing complex tasks in mobile web browsers could be employed to prevent the expansion of policy length (Hahn et al., 2018; Chang et al., 2021).

In both the *list* and *tab-based* prototypes, the absence of clear indications linking data protection points to specific devices was noted as a disadvantage. Participants recommended consolidating the *tab-based* and *device-based* conditions into a unified interface to optimize the user experience. Furthermore, participants proposed integrating additional features such as a search field and an FAQ page and highlighting newly added information to enhance usability. Subsequent research could delve into these suggestions and their implications for usability and workload.

In an effort to make privacy policies more understandable and reduce workload, the following implications emerge from the findings of this study. Improving the length of privacy statements is crucial to ensuring they are appropriately concise. The concept of condensing privacy policies into simplified one-line sentences with brief presentations was positively received in this study. If a significant reduction in length is not feasible, then subdividing them into different tabs could be considered. The tab-based presentation division proved most advantageous in this study. Users can readily access all aspects of their data processing, identify their rights at a glance, and locate contact information for responsible parties. Simplifying the language of privacy policies is essential to enhancing their comprehensibility. This

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

approach enables users to understand explanations regarding their data, their rights, and their usage more easily.

However, our study is subject to certain limitations. Firstly, we collected our data under uncontrolled conditions, making it challenging to generalize our results to other situations where participants may face distractions, such as the presence of other people. Additionally, participants interacted with the app using their own screens, leading to screen size variations that could affect the content's readability. Another limitation stems from the remote setting of the study. Natural distractions in real-world scenarios may have influenced our results differently. Although we evaluated certain design elements like icons, simplified sentences, and text segmentation in our pre-study, further design guidelines require testing for their applicability.

Furthermore, our study did not involve real-world usage of actual devices. As a result, it remains unclear whether participants were adequately prepared for the types of data collection that could occur during active device use. Presenting the privacy policy for a real device to a user before they have the opportunity to use it may underscore the importance of understanding such policies. However, this approach may inadvertently result in the collection of participants' personal data, such as log files or IP addresses, when the smart home devices are activated. In our approach, we sought to mitigate such data collection methods.

Acknowledgments

This section is based on the publication:

Mehrdad Bahrini, Nima Zargham, Alexander Wolff, Dennis-Kenji Kipker, Karsten Sohr, and Rainer Malaka. 2022. *It's Long and Complicated! Enhancing One-Pager Privacy Policies in Smart Home Applications..* In *Nordic Human-Computer Interaction Conference (NordiCHI '22)*. Association for Computing Machinery. DOI: 10.1145/3546155.3546657

My contribution to this work: Conceptualization, data curation, formal analysis, investigation, methodology, project administration, resources, part of software development, supervision, validation, visualization, and contribution to all parts of the manuscript.

3.3.3 Study 9: Protective Behavior Toward Privacy Choices

Introduction and Background

In our recent study, we investigated the effectiveness of multiple one-pager design layouts in improving the usability of privacy policies for smart home apps (Bahrini et al., 2022). Our approach ensured that users had access to privacy policy information at three key points in time. Initially, the policies were easily accessible during the setup of a smart home app. Secondly, users could review the consented privacy policies on demand by accessing the privacy tab within the app. Additionally, users encountered these policies just in time, particularly when adding new devices to their smart homes. Generally, privacy policies inform individuals about current or possible practices involving collecting, using, and sharing their personal data. In contrast, privacy choices allow users to manage the collection, processing, disclosure, and storage of their personal data (Feng et al., 2021). Effective timing in delivering privacy choices is crucial for shaping how users engage with privacy notices and make decisions that reflect their preferences. Optimal timing, whether at setup, on-demand, or just in time, ensures choices are contextually relevant and effective. It also influences users' perception of privacy risks and their overall experience with digital systems, while helping organizations to meet regulatory requirements for informed consent and periodic updates on data practices. The timing strategies selected for delivering privacy choices resonate with the Fogg Behavior Model, which emphasizes triggering behavior change through optimal timing when motivation or ability may not be optimal (Fogg, 2009). Therefore, understanding user behavior helps us comprehend why users frequently ignore privacy choices despite voicing concerns about their personal data (Rudolph et al., 2018).

As stated in the background, psychological factors, particularly self-efficacy, defined as confidence in one's ability to manage privacy in a given context, are necessary for explaining user behavior (Bandura, 1977). Studies indicated that higher self-efficacy correlates with increased adoption of security software, regular application of updates, and conscientious security practices like strong password use and data backups. Conversely, experiencing security breaches or lacking confidence in controlling security threats can reduce self-efficacy (Rhee et al., 2009). Higher self-efficacy, influenced by mastery experiences, vicarious experiences, social persuasion, and physiological feedback, leads to more proactive privacy management (Milne et al., 2009; Lunenburg, 2011). Furthermore, self-efficacy influences how users manage privacy in smart home devices like smart speakers, particularly by moderating the impact of perceived privacy risks on their chosen privacy strategies. It

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

suggests that users with greater self-efficacy may mitigate concerns about risks, leading to more expansive privacy practices (Kang and Oh, 2023).

Building upon integrating theoretical frameworks and practical approaches, we pose the following question: *How does integrating self-efficacy factors with varying timing of privacy choice presentations impact individual privacy-related behaviors and their perceived privacy protection?* In exploring our research question, we developed a web interface that integrates elements such as mastery experiences, vicarious experiences, and social persuasion, along with presenting privacy choices at different times. Within this interface, users navigate a registration process for a smart home device and are prompted to subscribe to cloud storage. Throughout this process, users must make critical decisions regarding their privacy preferences. The interface includes three distinct timing dimensions for presenting privacy choices: At-Setup, which shows privacy policies at startup; On-Demand, where privacy choices are readily accessible compared to At-Setup; and Just-in-time, where privacy choices are presented when specific consents are needed.

This study significantly contributes to understanding privacy management and user interaction with smart home devices by examining the impact of timing on privacy choice presentations. By applying the self-efficacy theory in study design, the findings reveal that just-in-time presentations enhance users' perceived awareness and satisfaction, boosting their confidence in managing privacy settings. Empirical data and qualitative insights highlight user behaviors, challenges, and preferences, emphasizing the importance of timely and accessible privacy information.

Prototype Description

Concept We crafted a web interface prototype embodying essential aspects of self-efficacy components. Developed using Vue.js ¹⁷, a progressive JavaScript framework, this prototype simulates an online platform akin to a smart home system provider offering cloud subscriptions to consumers. Users commence their journey through the web application by entering the participation ID, which serves as their gateway to access and navigate the various features and functionalities provided. The first step in the process entails watching instructional videos and engaging with a short narrative story. Following that, participants are required to complete various tasks. The tasks are aligned with privacy choices in the smart home field, ensuring participants engage directly with relevant privacy-related decisions and actions.

¹⁷<https://vuejs.org/>

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

Design: Verbal Persuasion and Vicarious Experiences Verbal persuasion, a cornerstone of Bandura’s self-efficacy theory, transmits knowledge through language via lectures, scientific literature, and motivational speeches (Graber, 1976). In contrast, vicarious learning supplements this by allowing individuals to learn through observation, such as studying documentaries for insights into ecosystems, analyzing historical events to understand past challenges, and observing role models to develop crucial life skills. We have prepared two videos and one text story to facilitate verbal persuasion and vicarious learning. These narratives collectively demonstrate the persuasive power of verbal communication and experiences in shaping individuals’ attitudes and behaviors toward privacy practices. They underscore the importance of informed decision-making and proactive privacy management in an increasingly interconnected digital world. The first video, featured in “The Verge,” revolves around the video “Why Privacy Matters”¹⁸ (see Figure 3.50). This video briefly outlines the significance of privacy concerns in today’s digital landscape, emphasizing the necessity of reading and understanding website privacy policies. It illustrates practical examples of navigating privacy settings on websites and explores the evolving role of Artificial Intelligence in shaping privacy regulations.

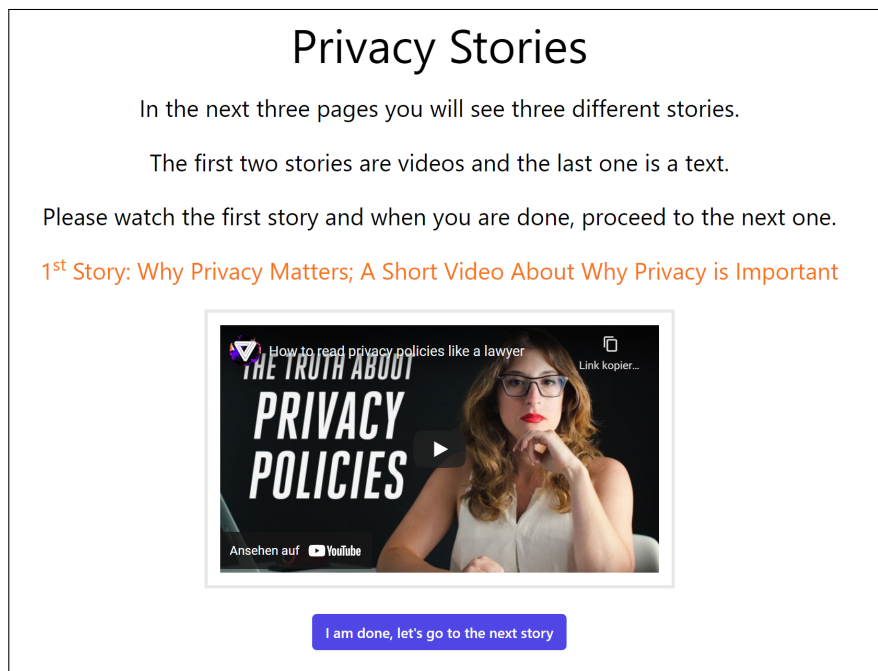


Figure 3.50: First story: Why privacy matters?

¹⁸<https://youtu.be/zZkY3MLBGh8>

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

In the second one, powered by “CNET,” the video “Amazon Audio Leakage”¹⁹, sheds light on a concerning incident involving an Amazon Echo device (see Figure 3.51). It recounts how the device inadvertently recorded a private conversation and sent it to a contact without explicit consent, underscoring the potential risks of privacy breaches in smart home technologies.

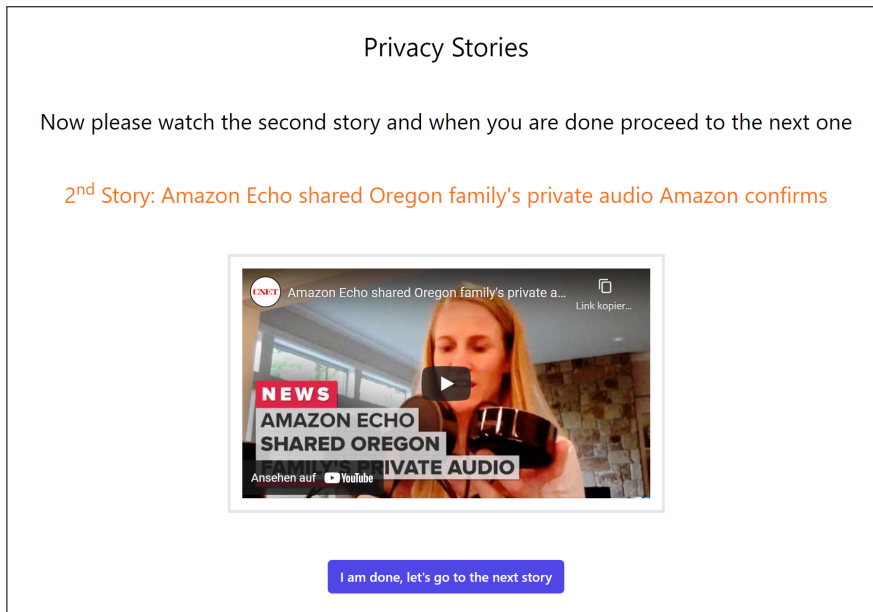


Figure 3.51: Second story: Amazon Echo shared audio

The third narrative is a thought-provoking fictional text scenario illustrating the repercussions of a security vulnerability in a smart home device (see Figure 3.52). This narrative serves as a cautionary tale, highlighting the importance of carefully reviewing privacy policies before integrating smart technologies into one’s home to mitigate security risks and protect privacy.

Design: User Tasks After users have watched the videos and thoroughly reviewed the accompanying text, they will engage in a scenario centered on smart homes. In this scenario, users undertake several tasks. Initially, they register an IP camera with its respective company and input the necessary information. Additionally, they are prompted to buy cloud storage to keep videos in the cloud. During these steps, users will encounter three distinct interfaces: At-Setup, On-Demand, and Just-in-Time. These interfaces are presented based on a between-subject study design, meaning users experience them according to their assigned group. Each interface is specifically tailored to address privacy choices across various temporal dimensions.

¹⁹<https://youtu.be/EW14SgVTtoA>

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

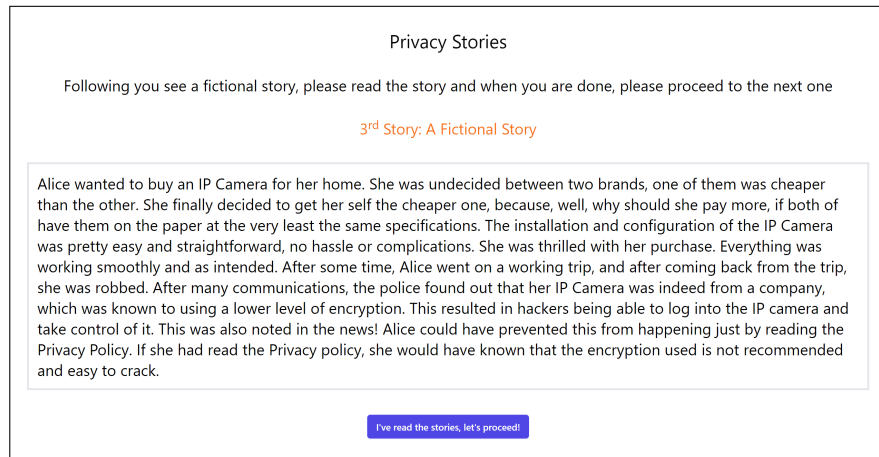


Figure 3.52: Third story: A fictional story

Before delving into the distinctions, we outline the primary tasks users need to complete. The journey begins with users entering the device's serial number and optionally providing a name for the device (refer to Figure 3.53).

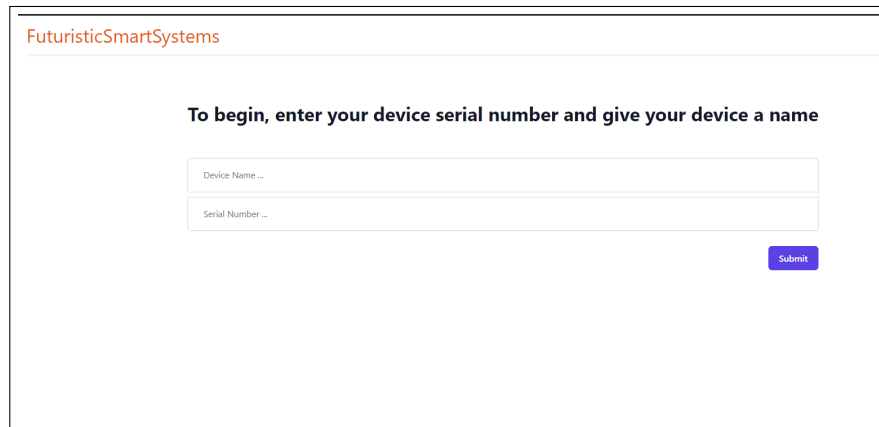


Figure 3.53: IP camera registration screen

On the subsequent page, users are instructed to input personal information. Notably, no genuine personal data is demanded; instead, participants are provided with simulated data (see Figure 3.54). This approach ensured privacy and ethical data collection compliance in the study. Once users enter their information, they proceed to select the IP camera. In our study, we specifically use the Bosch Smart Home IP camera model. Upon selecting the IP camera, they encounter a screen indicating that the cloud service is unavailable for use. Rather, they are prompted to purchase a cloud storage subscription (see Figure 3.55).

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

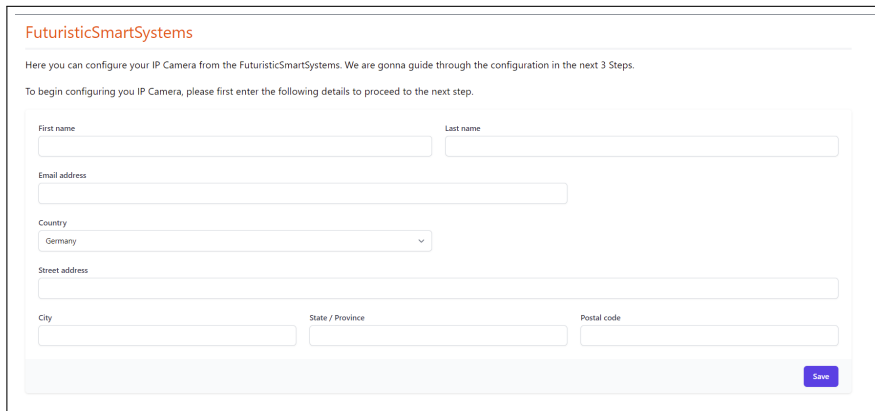


Figure 3.54: Personal data screen

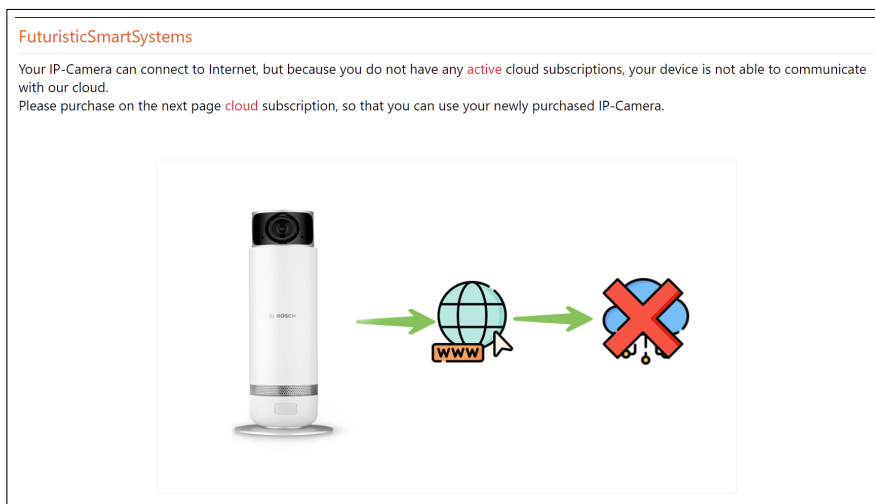


Figure 3.55: IP camera cloud subscription

Users complete the purchase of a cloud subscription for their IP Camera by entering credit card information (see Figure 3.56). To protect user privacy, we provided participants with pre-generated credit card data for this step, along with detailed instructions to ensure they could complete the process without using their own personal information. Once they save this information, users are presented with an information summary and an order summary (see Figure 3.57). They will proceed to checkout only after confirming their agreement with the entered data.

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

The screenshot shows a web form titled "FuturisticSmartSystems" for entering payment information. It includes a "Card number" field with a placeholder "0000 0000 0000", an "Expire date" field with a placeholder "MM/YY", and a "CVC/CVV" field with a placeholder "...". A blue "Save" button is located at the bottom left of the form.

Figure 3.56: Payment information

The screenshot shows a "Summary" page for the checkout process. It displays the user's name, address, country, state, zip code, name on card, credit card number, expiration date, and CVV. An "Order summary" table shows the subtotal, shipping, and total amounts. A blue "Checkout" button is located at the bottom right.

| Order summary | |
|---------------|---------------|
| Subtotal | € 9,99 |
| Shipping | € 0 |
| Total | € 9,99 |

Figure 3.57: Checkout summary

In the final component of the main interaction phase of the study, participants are shown that the IP camera has successfully connected to the cloud provider (see Figure 3.58). This step verifies the integration of the IP camera into the cloud service, representing a key point in the interaction process and demonstrating the system's functionality within the smart home environment.

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

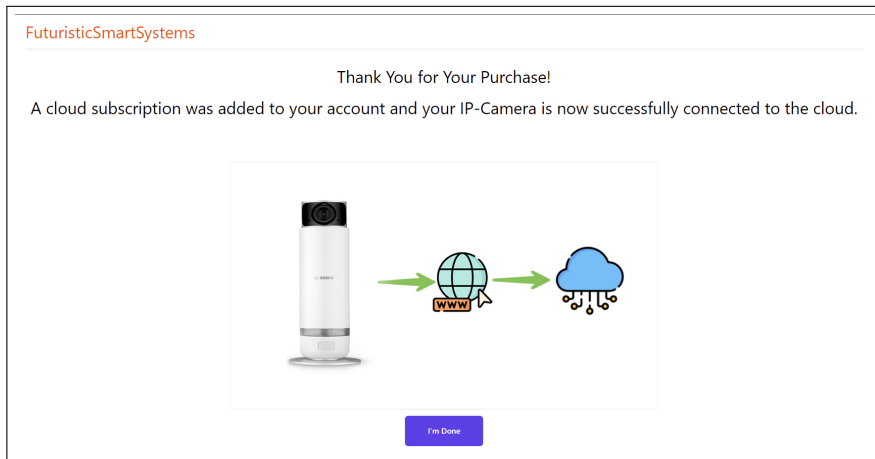


Figure 3.58: Successful cloud subscription for the IP camera

Design: At-Setup and On-Demand Dimensions As previously mentioned, users are presented with three distinct interfaces designed for making privacy choices. Each interface is tailored to accommodate privacy preferences across different time dimensions. In the At-Setup and On-Demand timing modes, users encounter an essential privacy choice presented at the beginning of the setup process and cannot be altered. The interface utilizes dark pattern designs where supplementary choices are concealed behind a settings button, potentially reducing their visibility or accessibility to users initially (see Figure 3.59).

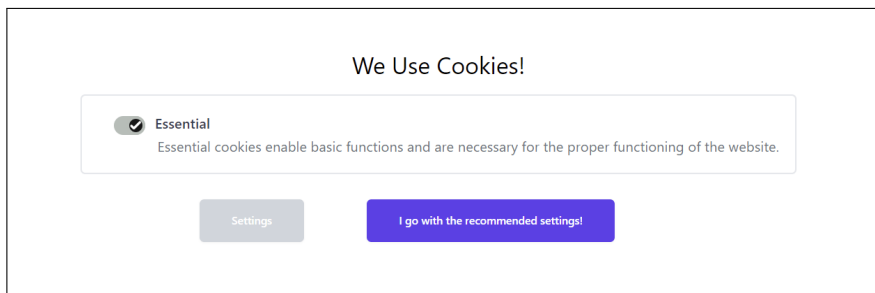


Figure 3.59: Initial presentation of privacy choices in At-Setup and On-Demand

Users who click “Settings” are presented with an array of privacy choices (see Figure 3.60). This study categorizes these choices into essential, statistical, marketing cookies, performance measurement, and personalization preferences. Users can decide which options are relevant to their preferences.

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

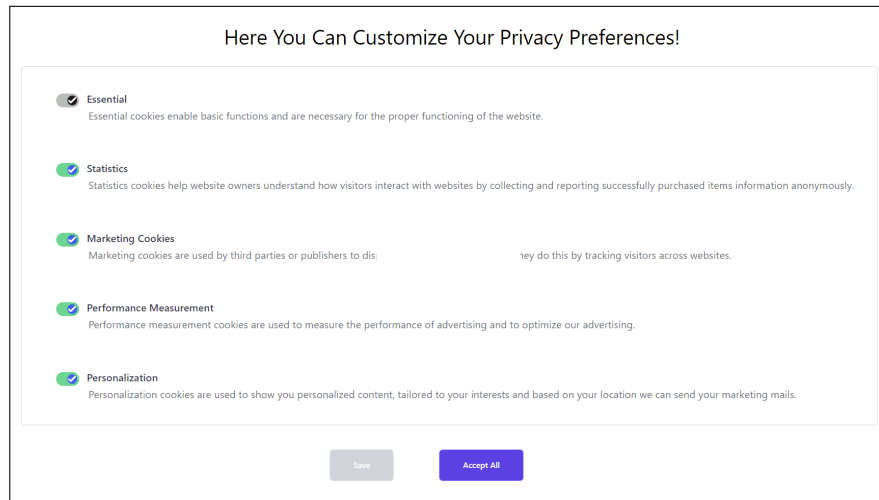


Figure 3.60: User-customizable privacy choices

The On-Demand mode distinguishes itself from At-Setup with an accessible design where privacy choices are prominently displayed on the navigation bar, easily reachable with a single click. However, in At-Setup, users need to navigate to the settings tab to find privacy choices, which adds an extra step to the process. This streamlined approach in On-Demand facilitates convenient review and management of privacy preferences without the complexity of navigating through multiple menus or settings (see Figure 3.61).

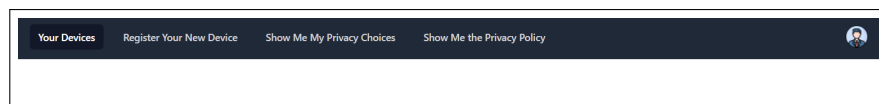


Figure 3.61: On-Demand: Navigation bar

Design: Just-in-Time Dimension In the Just-in-Time dimension, the privacy choices are prominently displayed directly under the input fields, as shown in Figure 3.62. We distributed the configurable choices across three distinct stages. Firstly, during the device registration process, users encounter initial configuration options. Secondly, when adding personal information, users are prompted to make additional configurable choices related to privacy and personalization settings. Lastly, users are given further configurable options when entering their credit card information.

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

The figure displays three sequential screenshots of the FuturisticSmartSystems device setup interface, illustrating the distribution of configurable choices during the setup process.

Screen 1: Device Identification
The interface prompts the user to "To begin, enter your device serial number and give your device a name". It features two input fields: "Device Name ..." and "Serial Number ...". Below these fields, there is a "Choose Your Privacy Preference" section with a checked checkbox for "Performance measurement cookies are used to measure the performance of advertising and to optimize our advertising." A "Submit" button is located at the bottom right.

Screen 2: Personal Information
The interface prompts the user to "Here you can configure your IP Camera from the FuturisticSmartSystems. We are gonna guide through the configuration in the next 3 Steps." and "To begin configuring you IP Camera, please first enter the following details to proceed to the next step." It features several input fields: "First name", "Last name", "Email address", "Country" (a dropdown menu currently showing "Germany"), "Street address", "City", "State / Province", and "Postal code". Below these fields, there is a "Choose Your Privacy Preference" section with a checked checkbox for "Personalization cookies are used to show you personalized content, tailored to your interests and based on your location we can send your marketing mails." A "Save" button is located at the bottom right.

Screen 3: Card Information
The interface prompts the user to "Enter your card number" and "Please enter the following details to proceed to the last step." It features several input fields: "Card number" (with a masked input field showing "0000 0000 0000"), "Expire date" (with a masked input field showing "MM/YY"), and "CVC/CVV" (with a masked input field showing "..."). Below these fields, there is a "Choose Your Privacy Preferences" section with two checked checkboxes: "Statistics cookies help website owners understand how visitors interact with websites by collecting and reporting successfully purchased items information anonymously." and "Marketing cookies are used by third parties or publishers to display personalized advertising. They do this by tracking visitors across websites." A "Save" button is located at the bottom left.

Figure 3.62: Sequential distribution of configurable choices during device setup

Design: Settings Interface Both At-Setup and Just-in-Time feature a settings page accessible via the profile icon (see Figure 3.63). Users access this page by clicking the profile icon and navigating to settings. Within this settings component, participants can view and manage their privacy choices.

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

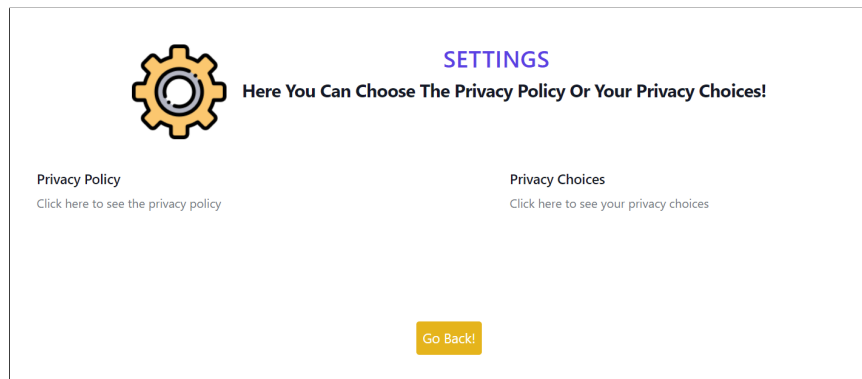


Figure 3.63: At-Setup/Just-in-Time: Settings interface

Design: Performance Outcomes Upon clicking “Done,” participants proceed to the final segment, which is informative rather than interactive. Privacy choices stored in the web interface are analyzed and visualized using a progress bar (see Figure 3.64). The progress bar serves as an indicator of the company’s satisfaction with the extent of user data access, highlighting that greater user consent correlates with higher levels of company satisfaction.

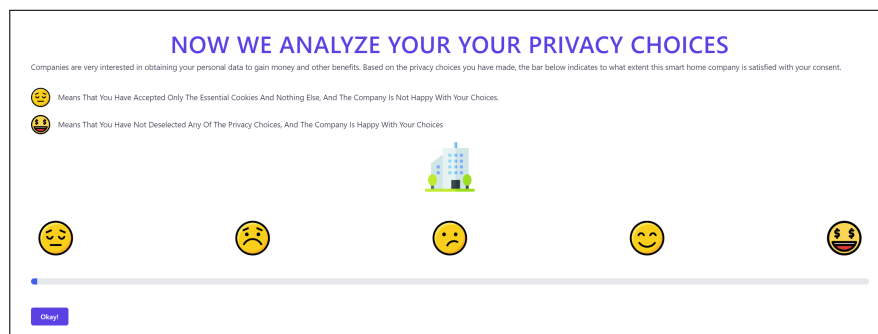


Figure 3.64: At-Setup/On-Demand/Just-in-Time privacy choices analyze

User Evaluation

Study Design In a laboratory-based between-subject study design, we recruited 48 participants, divided into three groups: At-Setup, On-Demand, and Just-in-Time, with 16 participants in each group. Participation was voluntary, and upon completing the study, participants received a 5 Euro Amazon gift card. Recruitment was conducted through university-wide email announcements and word of mouth. The study sessions typically lasted between 20 to 45 minutes on average.

Materials The data collection process utilized standardized questionnaires alongside customized items tailored to elicit participant responses.

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

- *Baseline Insight:* In this study, participants were questioned on aspects of smart home technology and privacy practices. They were asked whether they owned any smart home devices and, if so, to specify which ones. Additionally, participants were questioned about the duration of time they have been utilizing smart home systems. Another inquiry focused on whether participants had ever reviewed the privacy policy associated with their smart home devices.
- *Affinity for Technology Interaction:* We employed the 9-item Affinity for Technology Interaction (ATI) questionnaire to gauge participants' inclination towards technology interaction (Attig et al., 2017; Franke et al., 2019). This questionnaire utilizes a 6-point Likert scale, with responses ranging from "Completely Disagree" (1) to "Completely Agree" (6). Notably, responses must be reversed during analysis for the three negatively worded items (3, 6, 8). Subsequently, we calculate the mean score by averaging responses across all nine items, providing an overarching measure of participants' affinity for technology interaction.
- *Privacy Concerns:* The Internet Users' Information Privacy Concerns (IUIPC) questionnaire is designed to assess users' privacy concerns, focusing on software companies that provide online services and collect user data (Malhotra et al., 2004). The questionnaire comprises three dimensions: control, awareness, and collection. The control dimension measures the extent to which users desire control over disclosing and transferring their personal information. The awareness dimension assesses the degree to which users want to be informed about how and to whom their personal information is disclosed. Finally, the collection dimension examines how important it is for users to know which personal data is being collected. All items used a seven-point Likert-type scale ranging from "Strongly Disagree" (1) to "Strongly Agree" (7).
- *Self-Efficacy:* The self-efficacy questions were selected based on insights from three distinct research studies. Firstly, a study focused on smart speakers integrated privacy self-efficacy into the privacy calculus model, revealing that it enhances strategies such as privacy disclosure and boundary control while moderating perceived risks and amplifying perceived benefits (Kang and Oh, 2023). Secondly, research on computer and mobile device security behavior underscored the roles of perceived vulnerability, self-efficacy, and psychological ownership in influencing security intentions and actions among users (Thompson et al., 2017).

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

Lastly, an investigation into IoT privacy decision-making found that heightened privacy awareness correlates with more cautious and confident decisions across various IoT service scenarios, validated through machine learning experiments that emphasized the importance of privacy awareness in predicting user choices (Lee and Kobsa, 2019). These studies collectively informed the development of self-efficacy questions to assess users' capabilities and confidence in managing privacy and security concerns across different technological contexts. The selected queries were measured on a 7-point Likert scale from 1, "Strongly Disagree," to 7, "Strongly Agree." The detailed list of the self-efficacy questions is provided in Appendix A.4.

- *Perceived Privacy Protection:* Perceived privacy protection relates to how consumers perceive an internet vendor's efforts to protect their confidential information gathered during electronic transactions, preventing unauthorized use or disclosure. During these transactions, online sellers typically gather buyers' names, email addresses, phone numbers, and home addresses, with some vendors sharing this data with spammers, telemarketers, and direct mailers (Kim et al., 2008). Our selected questions are based on a study illustrating that consumers' trust and perceived risk significantly influence their purchasing decisions in online settings. Factors such as consumer trust predisposition, reputation, privacy and security concerns, website information quality, and company reputation strongly affect how consumers perceive trust in a website (Kim et al., 2008). The selected queries were rated on a 7-point Likert scale from 1, "Strongly Disagree," to 7, "Strongly Agree." The detailed list of perceived privacy protection questions is available in Appendix A.4.
- *Awareness Assessment:* Participants in the study were surveyed to evaluate their level of awareness regarding different dimensions of privacy choices within each group. This process included participants providing a rating on a scale from 1 to 10.
- *Feedback:* Finally, participants were invited to provide feedback on their interactions with privacy choices within each respective group.

Statistical Analysis We employed a one-way ANOVA test (Girden, 1992) to examine and identify statistically significant differences between conditions. The significance level for all statistical analyses was set at $\alpha = 0.05$, with results below this threshold considered statistically significant.

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

Procedure After obtaining consent, participants were warmly welcomed by the study director, who comprehensively explained the study procedures. The study was structured into three parts to explore participants' experiences and perceptions comprehensively. The first part involved administering a baseline questionnaire to gather initial participant information and perceptions. This questionnaire assessed participants' affinity for technology interaction, concerns about internet users' information privacy, and their experience with smart homes and privacy policies. The second part simulated a web application designed to replicate the process of registering an IP Camera. Participants interacted with this simulated platform, engaging in virtual decision-making and navigating through various privacy and camera configuration settings. In the third part of the study, participants completed a questionnaire focused on assessing their self-efficacy in managing privacy settings and their perceived level of privacy protection within the context of the simulated web application. This phase evaluated participants' confidence in making privacy-related decisions and their satisfaction with the privacy features presented.

Participants Out of the 48 participants involved in the study, they were evenly divided into three groups, each consisting of 16 individuals. Among them, there were 30 males, 17 females, and one participant who chose not to disclose their gender. The participants ranged from 21 to 51 years, with an average age of 27.75 ($SD = 5.95$). In the At-Setup group, 11 males, four females, and 1 participant chose not to disclose their gender. The On-Demand group had an equal split of 8 males and eight females. In the Just-in-Time group, there were 11 males and 5 females.

Empirical Findings

Baseline Insight This study explored participants' ownership of smart home devices, their experience with them, and their awareness of associated privacy policies. Among the 48 participants surveyed, 32 reported owning a smart home device, while 16 did not. In the At-Setup group, 7 participants owned a smart device, with the remainder not owning one. In the On-Demand group, 12 participants had a smart device, while 13 participants owned such devices in the Just-in-Time group.

Regarding experience, 21 participants had used smart home devices for less than a year, 18 had between 1 and 4 years of experience, and 9 had more than four years of experience. In the At-Setup group, 11 participants had less than a year of experience, four had between 1 and 4 years, and 1 had more than four years. In the On-Demand group, 4 participants had less than a year of experience, eight had between 1 and 4 years, and the rest had more

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

than four years. In the Just-in-Time group, six respondents had less than a year of experience, six had between 1 and 4 years, and 4 had more than four years.

Concerning privacy policies, 33 participants had never read them, 13 had only read part of them, one had read them in full, and one always did so. In the At-Setup group, 14 respondents had never read them, and two had read part. In the On-Demand group, ten participants had never read them, and five had read part of them. In the Just-in-Time group, nine had never read them, six had read part of them, and one had read them in full.

ATI The findings from the ATI questionnaire, as presented in Table 3.4 across all groups, indicate a predominantly favorable attitude toward technology. The questionnaire demonstrated acceptable reliability, with a Cronbach's alpha coefficient of 0.75, signifying strong internal consistency among the scale items.

Table 3.4: ATI Scales Across All Groups

| | At-Setup | On-Demand | Just-in-Time |
|----------------|----------|-----------|--------------|
| Mean | 3.83 | 3.89 | 3.99 |
| Std. Deviation | 0.73 | 0.75 | 0.60 |

IUIPC The overall mean score of the IUIPC questionnaire (Control, Awareness, and Collection) for participants was 5.91 ($SD = 1.45$) with a Cronbach's alpha coefficient of 0.78. The questionnaire revealed diverse levels of concern across its subscales: Control scored a mean of 5.66 ($SD = 1.78$), Awareness averaged 6.13 ($SD = 1.01$), and Collection averaged 5.93 ($SD = 1.19$). Table 3.5 illustrates these scores for each group.

Table 3.5: IUIPC Subscales Across All Groups

| | Control | | | Awareness | | | Collection | | |
|----------------|----------|-----------|--------------|-----------|-----------|--------------|------------|-----------|--------------|
| | At-Setup | On-Demand | Just-in-Time | At-Setup | On-Demand | Just-in-Time | At-Setup | On-Demand | Just-in-Time |
| Mean | 5.35 | 5.71 | 5.92 | 6.02 | 6.17 | 6.21 | 5.78 | 5.83 | 6.17 |
| Std. Deviation | 1.18 | 1.37 | 0.90 | 1.04 | 1.08 | 0.90 | 1.17 | 1.20 | 1.16 |

Self-Efficacy For each group, we calculated the mean and standard deviation of self-efficacy scores (refer to Table 3.6). A one-way ANOVA test was conducted to understand the differences in self-efficacy responses among the At-Setup group, On-Demand group, and Just-in-Time group. The results showed no statistically significant difference ($p = 0.19$), indicating that the levels of self-efficacy were similar across these groups.

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

Table 3.6: Self-Efficacy Across All Groups

| | At-Setup | On-Demand | Just-in-Time |
|----------------|----------|-----------|--------------|
| Mean | 4.02 | 3.75 | 4.50 |
| Std. Deviation | 1.08 | 1.31 | 1.10 |

Awareness Assessment Participants demonstrated varied levels of awareness across different timing conditions. The mean awareness scores were 3.69 for At-Setup, 4.88 for On-Demand, and 6.38 for Just-in-Time. These results indicate a progressive increase in perceived awareness as the timing of information delivery aligned more closely with the moment of need. The standard deviations of the three groups, respectively, suggest moderate variability around these mean scores (see Table 3.7).

A one-way ANOVA test confirmed these observations, revealing a statistically significant difference between the groups ($F(2, 45) = 3.50$, $p = 0.04$, $\eta^2 = 0.13$). Subsequent Bonferroni-adjusted *Post-hoc* analysis further clarified that the difference in awareness between the At-Setup and Just-in-Time conditions was statistically significant ($M = -2.69$, $p = 0.034$, $d = -0.93$). However, no statistically significant differences were found between the At-Setup and On-Demand conditions, nor between the On-Demand and Just-in-Time conditions ($p > 0.05$ for all comparisons).

Table 3.7: Awareness Assessment

| | At-Setup | On-Demand | Just-in-Time |
|----------------|----------|-----------|--------------|
| Mean | 3.69 | 4.88 | 6.38 |
| Std. Deviation | 2.91 | 2.73 | 2.99 |

Perceived Privacy Protection The perceived privacy protection means and standard deviations for the three groups are detailed in Table 3.8. Furthermore, the results of a one-way ANOVA test indicated that there was no statistically significant difference among the three groups ($p = 0.91$).

Table 3.8: Perceived Privacy Protection

| | At-Setup | On-Demand | Just-in-Time |
|----------------|----------|-----------|--------------|
| Mean | 4.30 | 4.30 | 4.46 |
| Std. Deviation | 1.32 | 1.26 | 1.04 |

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

Number of Checked Privacy Choices We analyzed the number of privacy choices made by participants to assess their willingness to share data. A higher count of checked checkboxes typically signifies greater readiness to share information, whereas fewer checkboxes indicate a privacy preference. Specifically, participants in the Just-in-Time group exhibited the lowest average number of checked checkboxes, with a mean of 3.5.

In contrast, those in the At-Startup group showed the highest average at 4.25 checkboxes. Table 3.9 details the average number of checked checkboxes and their standard deviations across each group, providing insights into participants' privacy preferences during the study. However, a one-way ANOVA test revealed no statistically significant differences between the three groups ($p = 0.41$).

Table 3.9: Average Number of Checked Checkboxes

| | At-Setup | On-Demand | Just-in-Time |
|----------------|----------|-----------|--------------|
| Mean | 4.25 | 3.56 | 3.50 |
| Std. Deviation | 1.61 | 1.93 | 1.71 |

Exploring Relationships The overall correlation analysis between IUIPC and awareness yielded a Pearson's correlation coefficient of $r = 0.16$ ($p = 0.28$). This indicates a weak positive linear relationship between these variables. However, the p-value of 0.28 suggests that this correlation is not statistically significant at the 0.05 level. Therefore, we do not find sufficient evidence to conclude that there is a significant relationship between IUIPC and awareness in our sample. This pattern was observed consistently across all groups within the dataset.

Examining the relationship between IUIPC and perceived privacy protection, we found a Pearson's correlation coefficient of $r = 0.11$ ($p = 0.46$). This suggests a weak positive linear relationship between these variables. Similarly, the p-value of 0.46 indicates this correlation is not statistically significant. Thus, we do not have enough evidence to support a significant relationship between IUIPC and perceived privacy protection. This finding was consistent across all groups analyzed in the dataset.

Qualitative Feedback Based on the qualitative data, we observed distinct perspectives and experiences regarding privacy choice implementation. In the At-Setup group, eight participants reported difficulties locating the privacy choices, expressing frustration with the visibility and accessibility of these options. For instance, one participant noted, "I could not find the privacy choices," highlighting interface challenges. Additionally, five participants

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

indicated indifference towards privacy options, with comments such as, “I don’t care to read the privacy policy because it is too long.”

Moving to the On-Demand group, six participants also faced challenges in finding privacy choices, echoing concerns about interface clarity. One participant stated, “I couldn’t see any privacy choices,” reflecting on the difficulty in identifying and accessing relevant settings. In contrast, five participants appreciated the structured representation of privacy choices, with one mentioning, “The policy was clear and easy to understand.” However, concerns about interface design were evident, with two participants disliking the light-gray color of the “save” button, which they found confusing.

In the Just-in-Time group, ten out of sixteen participants expressed satisfaction with the presentation of privacy choices, indicating a higher level of engagement and understanding. However, five participants still faced challenges locating these choices, suggesting room for improvement in interface accessibility. One participant’s data was excluded due to insufficient information for analysis.

Discussion and Limitations

This study explored whether adjusting the timing of privacy choice presentations, alongside applying principles from Bandura’s self-efficacy theory, could influence individuals’ behaviors. A web application was developed based on this theory and integrated three timing dimensions proposed by Feng et al. (2021) for presenting privacy choices.

The study’s baseline insights reveal that despite a high ownership rate of smart home devices among participants, a significant portion had never engaged with privacy policies. Of 48 participants, 32 owned smart home devices, yet 33 had never read the associated privacy policies. This indicates a general disengagement with privacy policies, underscoring the necessity for more effective presentation methods (Jensen and Potts, 2004; Luger et al., 2013; Kitkowska et al., 2020b).

Participants’ favorable attitudes towards technology, as indicated by the ATI scores, suggest that they are open to technological solutions, which is promising for interventions to improve privacy behaviors. However, the moderate Internet Users’ Information Privacy Concerns scores, particularly high in awareness, did not correlate significantly with increased privacy protection actions, indicating a gap between privacy concerns and the actual behavior of our participants (Kokolakis, 2017).

The study examined differences between groups in terms of self-efficacy, awareness, perceived privacy protection, and the number of checked privacy choices. The Just-in-Time group exhibited slightly higher self-efficacy scores,

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

suggesting that timely presentation of privacy choices might enhance users' confidence in managing their privacy settings (Feng et al., 2021). Awareness scores significantly differed between groups, with the Just-in-Time group showing the highest mean awareness score. This implies that presenting privacy choices at the moment of need can substantially enhance users' perceived awareness, supporting the idea that timely information is more effective (Feng et al., 2021). However, there were no significant differences in perceived privacy protection among the groups, suggesting that while timing affects immediate awareness, it might not influence deeper perceptions of privacy protection abilities. The Just-in-Time group also showed a lower average number of checked privacy choices, indicating a more cautious approach to sharing information, likely due to increased awareness and understanding (Van Kleek et al., 2017).

The correlation analysis between IUIPC and awareness and IUIPC and perceived privacy protection revealed weak and statistically insignificant relationships. This suggests that participants' privacy concerns do not necessarily translate into higher awareness or perceived ability to protect their privacy (Tabassum et al., 2019). Including this finding in the discussion emphasizes the complexity of privacy behaviors and the need for multifaceted approaches to enhance privacy protection. Simply improving awareness of privacy issues might not be sufficient to change behaviors. However, it is essential to consider factors such as the timing of information presentation and the overall user experience to effectively enhance individuals' privacy behaviors.

Qualitative feedback further highlights the importance of presentation timing. Participants in the At-Setup group reported difficulties locating privacy choices and expressed frustration with their visibility and accessibility, suggesting that presenting these choices only during the initial setup is ineffective. The On-Demand group had mixed experiences; while some participants appreciated the structured representation of privacy choices, others struggled to find them, indicating that on-demand presentation improves accessibility but might not suffice for all users. The Just-in-Time group reported higher satisfaction with the presentation of privacy choices, indicating that timely information delivery enhances user engagement and understanding. However, some participants still faced challenges, pointing to the need for continuous improvements in interface design.

The findings can be further understood through the lens of the Fogg Behavior Model, which posits that behavior is a product of motivation, ability, and a trigger. In this study, the timing of privacy choices served as the trigger (Fogg, 2009). The just-in-time presentation of privacy information

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

effectively triggers user engagement by aligning with users' immediate needs and context, thereby enhancing their ability to process and act on privacy information (Feng et al., 2021). This alignment supports the idea that optimal timing can significantly impact user behavior by making the information more relevant and actionable at the moment it is needed (Fogg, 2009).

The study had several limitations related to the implementation of the web application and the overall study design. One significant limitation was the inability to incorporate the physiological feedback aspects of self-efficacy theory into the main study. Despite numerous attempts, integrating these psychological aspects into a web application proved challenging. Another limitation concerned the study environment. Participants could deliberate on the privacy choices presented to them in a non-stressful setting.

In contrast, typical website users often seek to achieve their goals quickly and might be hurried. Their reactions might differ significantly in a real-world scenario where users face time constraints and potential frustration from initial privacy prompts. Thus, a more realistic environment requiring task completion within a limited timeframe might yield different results. Additionally, the data entered by participants during the study was fictitious, which could have influenced the outcomes. Participants might handle their actual personal data more cautiously than invented data. This difference in data treatment could affect the validity of the findings.

The study was performed only once, although repeated trials might yield different results under varying conditions. Furthermore, the study was limited to a web application setting. Conducting the study on smart devices could potentially lead to different findings due to variations in user interaction with different platforms. Moreover, the study presented only five privacy choices to participants, whereas real websites often offer many more options. Increasing the number of choices might affect user behavior, potentially leading to different outcomes.

In conclusion, the study underscores the significance of presenting privacy choices at optimal times to enhance user engagement and perceived awareness. The just-in-time approach appears most effective, aligning with self-efficacy theory by increasing users' confidence and competence in managing their privacy settings. However, the lack of a significant correlation between privacy concerns and awareness or perceived privacy protection suggests that a comprehensive approach is needed to address privacy behaviors effectively. This includes improving the visibility and accessibility of privacy choices and ensuring that users feel capable of managing their privacy settings regardless of their initial concerns.

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

Acknowledgments

This section is based on the master's thesis:

Mohammad Sajjad Khoshrou. 2023. *Protective Behavior Toward Privacy Policies: Exploring the Impacts of Changing Display Time on Data Subjects in Privacy Policy Design*. Unpublished master's thesis. University of Bremen.

My contribution to this work: Conceptualization, data curation, formal analysis, investigation, methodology, project administration, resources, partial software development, supervision, validation, and visualization.

3.3.4 Key Insights of Behavioral Prompts

Study 7: Raising Security Awareness with Summaries

This study explored the impact of automatic presentation of the APP-INFO page compared to providing data summaries during app configuration. The findings revealed that users in the *UDAP* group exhibited a more conservative and cautious approach to privacy and security risks. This heightened awareness, and accurate risk assessment suggest that timely and comprehensive information presentation effectively triggers user engagement and informed decision-making.

The automatic appearance of the APP-INFO page and the summaries acted as triggers, aligning with the FBM's emphasis on delivering prompts at the right moment to drive behavior. By providing detailed and timely privacy information, the *UDAP* interface increased users' ability to assess risks accurately. This enhancement in ability, combined with the immediate trigger, facilitated more informed and cautious behavior, aligning with the FBM's principles. The study also highlighted that providing users with clear and comprehensive privacy information increased their procedural knowledge and confidence in managing app permissions. This boost in perceived competence reflects an increase in self-efficacy, as users felt more capable of making informed decisions about app installations and data sharing. The higher self-efficacy led to more proactive and cautious privacy management, underscoring the importance of timely and relevant information triggers.

Study 8: Smart Home App One-Pager Privacy Policy

This study investigated different formats for presenting one-pager privacy policies and their effects on usability and cognitive load. The *tab-based* and *device-based* formats, which segmented and structured the content meaningfully, were more effective than the *list* format. These structured presentations acted as practical triggers, making accessing and understanding privacy information easier for users.

The *tab-based* format, in particular, demonstrated quicker response times and lower perceived workload, suggesting that well-organized information presentation reduces cognitive load and enhances usability. This aligns with the FBM's principle of simplifying tasks to enhance users' ability to act on the information. By making privacy policies more accessible and understandable, these formats triggered more efficient user interactions and better comprehension. Participants reported higher usability ratings and lower cognitive load with the *tab-based* format, indicating increased self-efficacy.

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

The ability to quickly locate and comprehend privacy details enhanced their confidence in managing privacy settings. This boost in self-efficacy reflects users' belief in their capability to execute the necessary behaviors to protect their privacy, leading to more informed and proactive decision-making.

Study 9: Protective Behavior Toward Privacy Choices

This study examined how different timings of privacy choice presentations (Just-in-Time, At-Setup, On-Demand) influenced user behavior. The Just-in-Time group showed higher self-efficacy and awareness, indicating that presenting privacy choices at the moment of need is most effective. These timely triggers aligned with users' immediate context, enhancing their ability to process and act on private information.

The Just-in-Time triggers effectively served as prompts, driving user engagement by providing relevant information when users needed it most. This approach aligns with the FBM, which posits that behavior is a product of motivation, ability, and a trigger. By delivering privacy information at the right time, these triggers enhanced users' ability to make informed decisions, thereby improving their privacy management behaviors.

The study also found that timely presentation of privacy choices increased users' confidence and understanding, leading to higher self-efficacy. Participants in the Just-in-Time group reported greater satisfaction with the privacy choice presentation, reflecting their increased competence and readiness to manage privacy settings. This heightened self-efficacy contributed to a more cautious approach to sharing information, indicating that users felt more capable of protecting their privacy.

Integration of Theories and Findings

These studies collectively demonstrate that the temporal precision of triggers, including the timing and contextual relevance of notifications, significantly impacts users' decision-making and actions when configuring privacy and security settings. According to the Fogg Behavior Model, behavior change occurs when motivation, ability, and triggers converge. Timely and contextually relevant triggers enhance users' ability to act on information, driving more informed and proactive behaviors. Self-efficacy theory further elucidates the impact of these triggers on user behavior. By increasing perceived competence, timely information presentation boosts users' self-efficacy, leading to higher intrinsic motivation and a greater likelihood of adopting informed behaviors. When users receive privacy and security information at the moment of need, they feel more confident and capable of managing their settings, reflecting increased self-efficacy.

3.3. BEHAVIORAL PROMPTS IDENTIFICATION

The temporal precision of triggers, including the timing and contextual relevance of notifications, significantly enhances users' decision-making and actions when configuring privacy and security settings within ubiquitous and mobile applications. The findings from Studies 7, 8, and 9 confirm that timely and relevant triggers, such as the automatic presentation of privacy information, structured privacy policy formats, and Just-in-Time privacy choice presentations, effectively enhance users' ability and self-efficacy.

Study 7 demonstrated that automatic and timely information presentation (*UDAP* interface) improves users' assessment of privacy and security risks, leading to more informed behavior. Study 8 showed that structured presentation formats (*tab-based*) reduce cognitive load and improve usability, thereby boosting self-efficacy and enabling more effective privacy management. Study 9 highlighted that Just-in-Time triggers significantly enhance self-efficacy and awareness, leading to a more cautious and informed approach to privacy choices.

Overall, these studies underscore the importance of delivering privacy and security information at the right time and context. By aligning triggers with users' immediate needs and providing clear, accessible information, applications can enhance users' confidence and competence in managing their privacy settings. This approach fosters informed behavior and promotes a more privacy-conscious and secure user experience, effectively addressing our third research question in this dissertation.

RQ3

How does the temporal precision of triggers impact users' decision-making and actions when configuring privacy and security settings within ubiquitous and mobile applications?

By addressing Research Question 3, we examine the role of goal-setting in guiding user engagement with privacy and security tasks. This question explores how establishing clear goals and using triggers, such as prompts and reminders, can direct users to take action in privacy and security contexts. Through HCI approaches like context-sensitive notifications and timely cues, we aimed to create interventions that align with users' privacy and security intentions, highlighting the importance of structured guidance to effectively support users in managing their digital privacy.

4

Empowering User Behavior

This chapter underscores the need for a paradigm shift to empower users to manage privacy and security within mobile and ubiquitous applications. Building on foundational models like Social Cognitive Theory (SCT) and Fogg Behavior Model (FBM) and progressing toward Bandura's self-efficacy theory, we emphasize enhancing user motivation and ability to engage with digital security. Our studies address key aspects of user empowerment, including understanding privacy terms, data practices transparency, and using Augmented Reality (AR) to simplify complex security concepts. Initial studies assess users' comprehension of privacy and security terms and evaluate how fitness and health apps communicate data practices, including potential dark patterns. Further, we explore both AR and 2D interfaces as tools to enhance procedural knowledge, particularly in smart homes, where visual representations and interactive indicators can make security settings more accessible. Together, these studies support transparent, user-centered design and interactive technologies to enable users to confidently make informed, secure choices, aligning with user needs and regulatory standards.

4.1 The Imperative for a Paradigm Shift

Our exploration thus far has traced a transformative journey from overarching meta-models such as Social Cognitive Theory and the Fogg Behavior Model towards more nuanced and targeted conceptual frameworks, exemplified by Bandura's theory of self-efficacy. This progression has provided insights into how enhancing both the motivation and ability of end users can significantly amplify the effectiveness of behavioral triggers.

However, this evolution raises the question of what motivates the need to empower users. From a legal and ethical standpoint, we have discussed the far-reaching implications of regulations like the General Data Protection Regulation on companies handling personal data. However, the focus now shifts to the subjective experiences of users themselves. Are they adequately informed and empowered when navigating their rights within the complex landscape of mobile and ubiquitous applications? Conversely, are companies effectively integrating privacy and security principles by design to honor user rights and comply with regulatory frameworks? The following studies aim to delve deeper into these critical questions, employing a blend of theoretical frameworks and empirical research to illuminate the dynamics of user empowerment in contemporary digital environments.

The first study evaluates users' understanding levels, which are essential for developing impactful educational strategies and communication materials. By examining users' grasp of terms concerning privacy and security, the study aims to ascertain whether users feel adequately informed when making decisions about their privacy and security in smart home environments. Furthermore, the study investigates how exposure to these technical terms influences users' behavioral intentions.

The second study conducts technical analyses by analyzing the code and privacy policies of fitness and health apps. It investigates whether these policies clearly communicate how user data is used and shared. By examining the presence of dark patterns, the study aims to evaluate how effectively companies prioritize user understanding and consent.

Together, these studies deepen our understanding of the dynamic relationships among user empowerment, information transparency, and regulatory compliance in mobile and ubiquitous applications. They offer insights into whether current practices adequately inform and empower users while encouraging companies to adopt robust privacy and security measures that align with user expectations and legal standards.

4.1.1 Study 10: Security Literacy and Behavioral Intentions

Introduction and Background

In today’s smart home apps, users encounter a variety of technical terms and concepts that may not immediately resonate with them. As they explore popular apps like Amazon Alexa, Google Home, and Smart Life- Smart Living, they come across terms like authentication, password, and multi-factor authentication within the login interfaces of these platforms. Here, users are prompted to verify their identity through familiar means such as usernames and passwords. Alternatively, they can opt for added security via third-party authentication services like Google or Apple accounts. Privacy becomes a paramount concern, with terms like encryption and anonymization appearing in the privacy policies and device settings of these apps (see Table 4.1). Users navigate through these settings in apps such as Philips Hue, Ring, and Eufy Security, where they can manage firmware versions, security updates, and access controls for their devices. Throughout this journey, users are challenged to understand and engage with these terms and concepts, ultimately striving to harness the full potential of their smart homes while ensuring their privacy and security remain intact (Haney et al., 2020).

Table 4.1: Locations of Terms in Some Widespread Smart Home Apps.

| Term | Location | Apps |
|-----------------------------|------------------------------------|---|
| Authentication | Login Interface | Amazon Alexa, Google Home, Smart Life- Smart Living |
| Password | Login Interface | Amazon Alexa, Google Home, Smart Life- Smart Living |
| Multi-Factor Authentication | Login Interface | Amazon Alexa, Google Home, Smart Life- Smart Living |
| Third-Party Authentication | Login Interface | Amazon Alexa, Google Home, Smart Life- Smart Living |
| Encryption | Privacy Policies, Device Settings | Amazon Alexa, Google Home, Smart Life- Smart Living |
| Anonymization | Privacy Policies, Device Settings | Amazon Alexa, Google Home, Smart Life- Smart Living |
| Physical Security | Privacy Policies | Amazon Alexa, Google Home, Smart Life- Smart Living |
| Firmware Version | Device Settings | Philips Hue, Ring, Eufy Security |
| Security Updates | Device Settings | Philips Hue, Ring, Eufy Security |
| Access Control | Device Settings | Philips Hue, Ring, Eufy Security |
| Privacy | Privacy Policies, Privacy Settings | Amazon Alexa, Google Home, Smart Life- Smart Living |
| Privacy Policy | Privacy Policies, Privacy Settings | Amazon Alexa, Google Home, Smart Life- Smart Living |
| Communication Protocol | Privacy Policies, Device Setup | Amazon Alexa, Google Home, Smart Life- Smart Living |

Technical literature has thoroughly explored these terms and concepts, elucidating them as necessary prerequisites for ensuring robust smart home security systems. Recent research in the field of smart homes and Internet of Things (IoT) security has highlighted several key challenges and potential solutions. Komninos et al. (2014) conducted a comprehensive survey focusing on the security issues in smart grids and smart homes. They emphasized terms such as privacy, access control, authentication, security updates, password management, communication protocols, encryption, anonymization, and physical security. Building upon this foundational work, Hossain et al. (2015) provided further analysis of security issues in the broader IoT

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

landscape. Their study explored topics such as privacy concerns, password management, anonymization techniques, authentication mechanisms, access control policies, firmware security, and the importance of regular security updates. Researchers contributed to this body of knowledge by proposing a comprehensive security framework specifically tailored for IoT-based Smart Homes (Sotoudeh et al., 2020). They emphasized the significance of privacy protection, robust password policies, encryption techniques, secure communication protocols, authentication mechanisms, and access control strategies. Hammi et al. (2022) extended these discussions with a survey focusing on vulnerabilities, risks, and countermeasures in smart homes. Their research underscored the importance of physical security measures, privacy preservation techniques, secure communication protocols, anonymization methods, robust authentication mechanisms, pseudonymization practices, firmware security, and timely security updates.

These studies emphasize the necessity of adopting a holistic strategy to tackle the varied security challenges encountered by smart homes and IoT ecosystems. They also prompt an essential question about the extent of comprehension among end-users regarding these technical terms, particularly as they are prevalent in smart home applications. Drawing upon pertinent technical terminology in the domains of privacy and security, sourced from academic papers and smart home applications, we seek to address two essential inquiries in this work: *Q1) To what degree are users able to grasp the meanings and implications of these terms?* Understanding the level of comprehension among users is crucial for designing effective communication strategies and educational materials in privacy and security. *Q2) When users are exposed to these technical terms, how does it impact their behavioral intentions?* In other words, does familiarity with these terms lead to an increased inclination among users to adopt more secure practices or take proactive measures to protect their privacy?

In this study, we focused on several essential aspects, including authentication, password management, multi-factor authentication, third-party authentication, encryption techniques, anonymization methods, physical security measures, security updates, access control policies, privacy preservation, privacy policy adherence, and communication protocols. These areas were selected based on their significance in ensuring the integrity and security of smart home systems and IoT environments. By exploring the relationship between exposure to technical terminology and subsequent behavioral intentions, we aim to uncover how communication efforts promote user awareness and engagement in privacy and security matters.

Prototype Description

Concept Navigating the complexities of smart home technology can prove challenging, particularly given the multitude of devices and concepts users must grapple with when configuring smart home networks. To illustrate this process, we have developed a wizard that users experience during the smart home network configurations. This wizard, a website developed with HTML and CSS, replicates the interface of a desktop smart home application. Spanning 23 pages, it systematically guides users through setting up three smart home devices, followed by connecting two of them. This immersive experience mimics typical user interactions with new smart home devices.

Design Users configure three devices within the wizard: a smart light bulb, camera, and speaker. Each device presents its own set of security risks, impacting setup decisions. The light bulb, which collects minimal personal data, poses the lowest risk and requires fewer adjustments. In contrast, the camera records images and potentially audio, storing and processing them in the cloud, necessitating more extensive customization. Meanwhile, the speaker, which also functions as a voice assistant for controlling other household devices, offers the most comprehensive settings at this stage (see Figure 4.1). If users require further explanation about configuration terms, tooltips, which are small pop-up windows, are provided to enhance clarity.

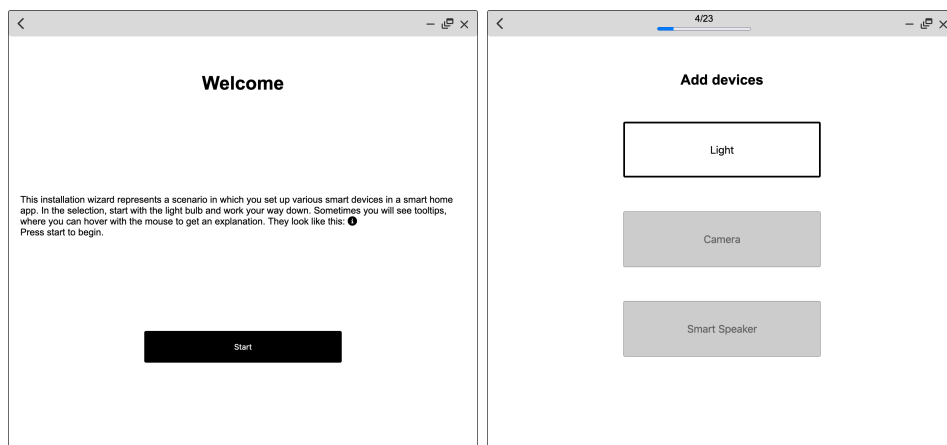


Figure 4.1: On the left is the start screen, and on the right is the device installation choice in the smart home configuration wizard.

For the light bulb setup, participants are first asked to create a password. Although this step remains consistent for all three devices, the password becomes pertinent later on solely for the light bulb. Subsequently, participants can specify their preferences regarding sharing personal data with third

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

parties. They have the option to grant unrestricted access to their data, which provides the advantage of personalized offerings, such as those from utility providers. Alternatively, they can opt to anonymize their data or refrain from sharing it all together (see Figure 4.2).

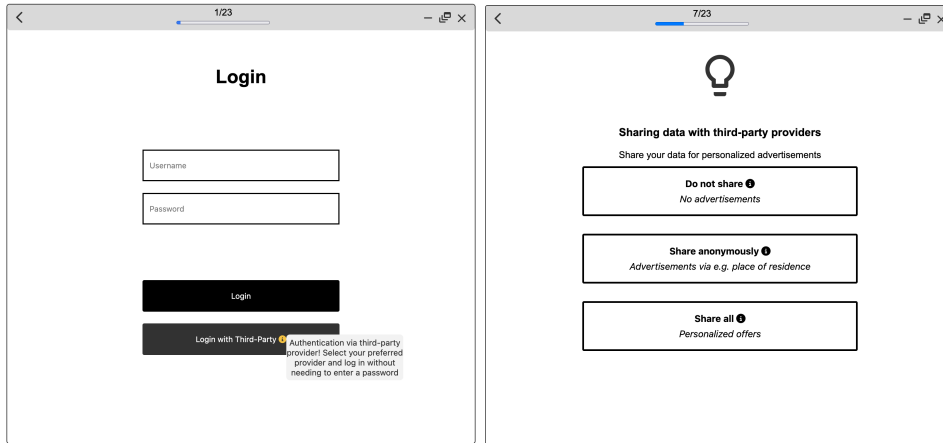


Figure 4.2: On the left side, users encounter the login screen for the light bulb, while on the right side, they are presented with options for sharing personal data.

Similarly to the light bulb setup process, users are prompted to configure the encryption settings for the camera stream once the password is established. This process does not involve implementing encryption mechanisms but rather provides users with a conceptual understanding of weak or strong encryption and gives users insight into the potential security benefits of implementing encryption measures. Users can select from different encryption levels within these settings, including none, weak, and strong encryption options. Figure 4.3 illustrates how an encrypted image might appear to hackers. Following this, the user is given the option to either proceed with a security update or skip this step altogether. This decision allows users to prioritize their security preferences based on their needs and circumstances.

At the speaker setup stage, users are first prompted to configure their preferences for data anonymization, allowing them to choose the desired level of anonymization from options including no anonymization, pseudonymization, and complete anonymization (see Figure 4.4). Following this initial step, an activity log is presented to users, displaying any recorded activities and providing the option to delete them. Although users are setting up the system and have no prior activity history, this feature serves as a demonstration of the system's ability to log activities, which can be cleared as needed. Moving forward, users encounter the access control screen, where they can assign four types of user rights: owner, admin, family member, and

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

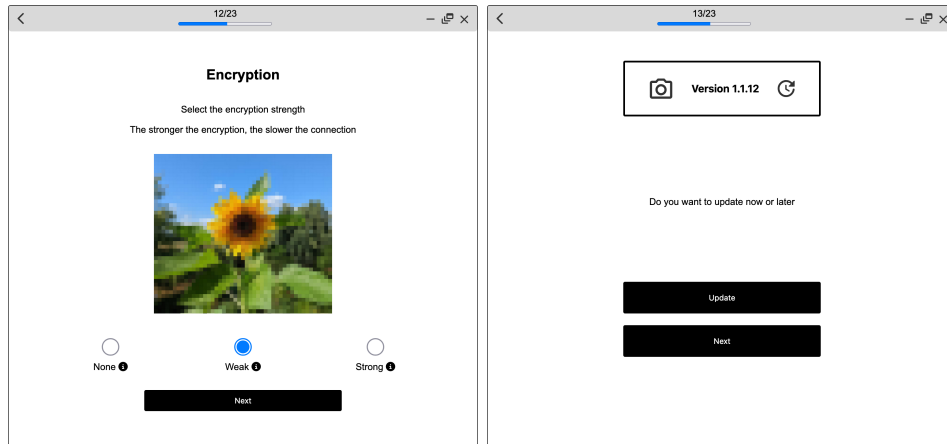


Figure 4.3: On the left side is the encryption screen, where users can adjust encryption settings for the camera stream. On the right side is the option for a security update specifically for the camera.

guest (see Figure 4.5). Owners have unrestricted access to all functionalities, while admins share similar access privileges with the additional capability of including multiple individuals. Family members are granted access to all features except for system settings, whereas guests have limited access and can only perform specific functions, such as playing music.

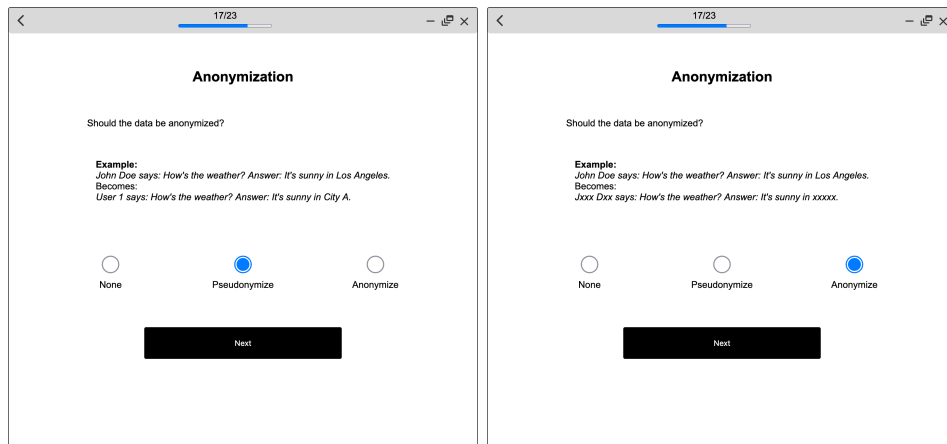


Figure 4.4: Anonymization screens for adjusting speaker settings.

Finally, as part of the setup process, the light bulb and speaker are connected to enable communication and data sharing between the two devices, thereby extending their functionalities. Initially, users are prompted to input the password for the light bulb, ensuring secure access to the device's settings. Subsequently, users are presented with options for configuring data exchange

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

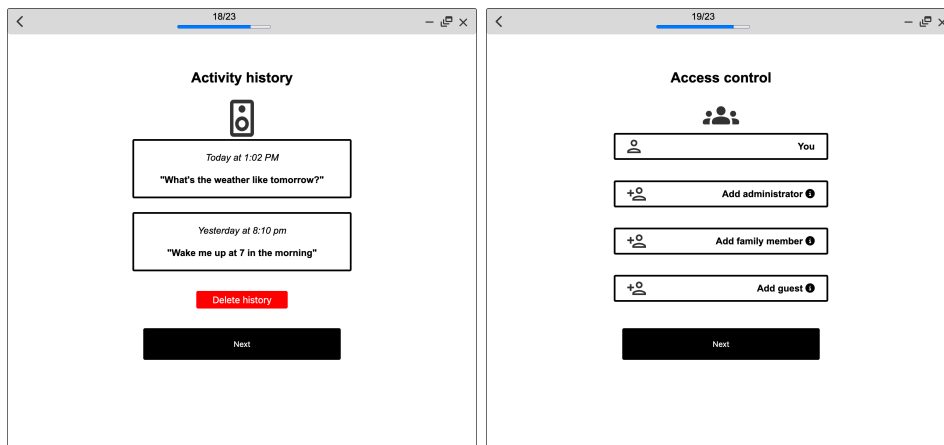


Figure 4.5: Users view an activity log on the left with options to delete recorded entries. At the same time, on the right, they set up access controls, assigning roles such as owner, admin, family member, and guest, each with specific access privileges.

settings between the light bulb and speaker. They can choose from three levels of data sharing: full data sharing, anonymized data sharing, or no data sharing. Opting for full data sharing enables the speaker to access all available data from the light bulb, maximizing functionality. Conversely, selecting anonymized data sharing restricts certain features, as some data is masked for privacy purposes. Alternatively, users can opt not to share any data, resulting in limited functionality while offering maximum privacy. This flexibility empowers users to tailor their data-sharing preferences according to their privacy concerns and desired level of functionality.

Furthermore, users are given the opportunity to select the communication protocol to be used between the devices. They can choose from WLAN, Zigbee, and Z-Wave protocols, each with advantages and limitations. For users who are indifferent to the protocol choice, there is an option to leave it unspecified. This decision-making process allows users to align the device setup with their specific needs and preferences, considering data security, network stability, and interoperability with other devices (see Figure 4.6).

User Evaluation

Study Design In order to address our research questions, we invited 20 participants to configure smart home devices within a laboratory and controlled environment, taking into account potential differences in their knowledge levels. Participants utilized a web page interface smart home setup wizard, which systematically guided them through configuring three smart home devices. These steps closely mimicked typical user interactions with

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

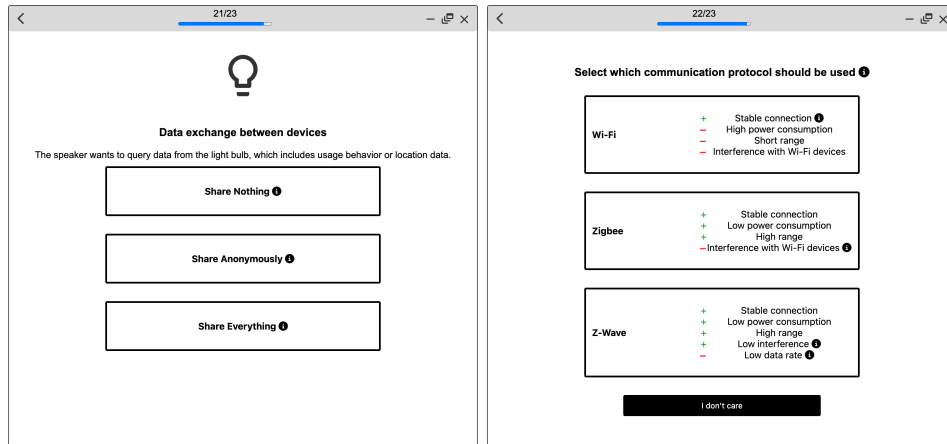


Figure 4.6: On the left, users configure their data-sharing preferences between the light bulb and speaker service providers, while on the right, they select communication protocols for the smart home devices.

new smart home devices. On average, participants dedicated 5.23 minutes to completing the wizard process. Additionally, participants were required to answer pre- and post-questionnaires as part of the study protocol.

Materials The data collection process utilized standardized questionnaires and customized items designed to elicit participant responses.

- *Baseline Insight:* Our self-designed questions encompass multiple facets of participants’ technological engagement and concerns, structured around a 5-point Likert scale. The initial inquiry delves into participants’ utilization of smart home technologies to gauge their familiarity and level of engagement. Following this, the subsequent question explores participants’ comprehension of smart home data protection and security issues related to smart home devices. Finally, the questionnaire concludes by exploring participants’ concerns regarding the privacy and security of their smart home devices.
- *Affinity for Technology Interaction:* We employed the 9-item Affinity for Technology Interaction (ATI) questionnaire to gauge participants’ inclination towards technology interaction (Attig et al., 2017; Franke et al., 2019). This questionnaire utilizes a 6-point Likert scale, with responses ranging from “Completely Disagree” (1) to “Completely Agree” (6). Notably, responses must be reversed during analysis for the three negatively worded items (3, 6, 8). Subsequently, we calculate the mean score by averaging responses across all nine items, providing an overarching measure of participants’ affinity for technology interaction.

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

- *Privacy Concerns:* The Internet Users' Information Privacy Concerns (IUIPC) questionnaire is designed to assess users' privacy concerns, focusing on software companies that provide online services and collect user data (Malhotra et al., 2004). The questionnaire comprises three dimensions: control, awareness, and collection. The control dimension measures the extent to which users desire control over disclosing and transferring their personal information. The awareness dimension assesses the degree to which users want to be informed about how and to whom their personal information is disclosed. Finally, the collection dimension examines how important it is for users to know which personal data is being collected.

In our questionnaire, we integrate trusting beliefs and risk beliefs to understand an individual's inclination to disclose personal information to software companies. Trusting beliefs gauge the level of trust individuals place in a firm's ability to protect consumers' personal data. Conversely, risk beliefs pertain to the anticipation of potential losses linked with sharing personal information with firms. All items used a seven-point Likert-type scale ranging from "Strongly Disagree" (1) to "Strongly Agree" (7).

- *Understanding Security Concepts:* One key focus of this study is to understand how users perceive privacy and security technical terms and concepts within smart homes. We pose a series of questions for each term to explore this area effectively. Initially, participants rate their familiarity with the term on a 5-point Likert scale, ranging from "Very" to "Not at all." Subsequently, when encountering each term, participants are prompted to specify their source of familiarity, whether derived from the smart home context or elsewhere, using two text fields. Finally, participants demonstrate their understanding by providing a definition of the term or elucidating its functionality. These terms, drawn from our analysis, include Authentication, Password, Multi-factor Authentication, Access Control, Third-party Login, Privacy Policy, Privacy, Encryption, Anonymization, Pseudonymization, Physical security, Firmware, Security update, and Communication protocol.
- *Well-Informed and Behavior Intention:* We have designed a set of questions to explore participants' post-wizard comprehension and their intention toward protecting their smart home data. We start by asking participants whether they now feel competent (or well-informed) about

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

the steps necessary to secure their smart home data and account (Q1). Following this, we inquire about their intention to avoid smart home services that require their name or email address due to uncertainty regarding how their personal data will be used (Q2).

Next, we delve into participants' proactive measures by asking whether they plan to modify the default settings of smart home apps to enhance their data security (Q3). We then ask about their intention to review the privacy policies of smart home apps before installing them as a precautionary measure (Q4).

Moving forward, we explore participants' preferences regarding cloud-based smart home services. Specifically, we ask whether they intend to avoid such services and opt for establishing a local smart home network to minimize the risk of data compromise (Q5).

Finally, based on participants' experiences with smart home settings, we seek to understand the importance they attribute to changing their security behavior to enhance protection against various smart home security threats, including data misuse, identity theft, device takeover, and spoofing (Q6).

- *Sketching Task and Conceptual Knowledge:* Following the setup of smart homes through the wizard interface, participants engage in a drawing task and respond to survey questions. The primary objective is to assess their conceptual understanding of smart home concepts, particularly focusing on fundamental security and data management principles. Initially, participants are prompted to illustrate their understanding of the smart home system by visually depicting the setup. Following this, they are presented with questions regarding data collection, exchange, inference, storage, and risk mitigation techniques. The questions were adapted from Tabassum et al. (2019) and adjusted to align with our research objectives. Participants respond using text fields in this study.

Procedure The study initiates by gathering background information from participants through baseline insight questions. Additionally, we evaluate participants' understanding of security concepts. With varying levels of knowledge, participants are then immersed in a controlled environment to configure smart home devices. This interactive exercise facilitates device setup and refreshes participants' comprehension of privacy and security concepts. At the heart of this process lies the wizard, systematically guiding users through the sequential setup of three smart home devices and linking two of

them. This structured sequence closely emulates typical user interactions with new smart home devices. Subsequently, participants provide responses to post-questions, which include inquiries about their level of information and their behavioral intentions. Furthermore, we assess participants' comprehension of network connections through a sketching task and evaluate their conceptual knowledge.

Participants The study included a total of 20 participants, with 15 males and five females. Their average age was 26 years ($SD = 8.3$), ranging from 20 (youngest participant) to 60 (oldest participant). Participation was voluntary, and respondents were not compensated. Recruitment methods encompassed mailing lists, social networks, word-of-mouth, and personal contacts.

Empirical Findings

Baseline Insight We initiated the data collection process by administering inquiries concerning participants' backgrounds. These questions were crafted to gather crucial information and set a foundation for our study.

- *Smart Home Usage:* Among the participants, seventeen owned at least one smart home device. In terms of smart home usage duration, 3 participants reported having less than one year of experience, while 11 participants indicated using it for 1 to 4 years. Furthermore, 6 participants claimed to have over four years of experience with smart home technology.
- *Smart Home Security Understanding:* As part of our study, we asked participants about their knowledge of security issues related to smart home devices. Two participants admitted to having no knowledge at all, while seven mentioned having only minimal understanding. Furthermore, five participants claimed to possess moderate knowledge, and six reported having advanced knowledge. None of the participants indicated having expert-level knowledge.
- *Smart Home Security Concerns:* When questioned about their concerns regarding privacy and security in their own smart homes, 3 participants expressed no concerns whatsoever, while eight indicated having only a few. Four participants stated having neither few nor many concerns, 3 reported having more, and two expressed having a significant number of concerns.

ATI The findings from the ATI questionnaire revealed an average score of 4.44 ($SD = 0.82$) across all participants, indicating a predominantly favorable

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

attitude toward technology. Furthermore, the questionnaire exhibited high reliability, as evidenced by a Cronbach’s α coefficient of 0.88, suggesting strong internal consistency among the scale items.

IUIPC The mean score across the Control, Awareness, and Collection dimensions of the IUIPC questionnaire for participants was 5.66 (SD = 1.50), with a Cronbach’s α coefficient of 0.71. Detailed scores for the IUIPC dimensions and context-specific factors (Trusting Beliefs and Risk Beliefs) are provided in Table 4.2.

Table 4.2: IUIPC Dimensions and Context-Specific Factors

| | Cronbach’s α | Mean | Std. Deviation |
|------------------|---------------------|------|----------------|
| Control | 0.61 | 5.53 | 1.43 |
| Awareness | 0.66 | 6.38 | 1.01 |
| Collection | 0.95 | 5.20 | 1.66 |
| Trusting Beliefs | 0.83 | 2.84 | 1.34 |
| Risk Beliefs | 0.76 | 4.00 | 1.50 |

Understanding Security Concepts We employ a structured approach with three inquiries per term to assess participants’ comprehension of the terms. These encompass an individual’s self-assessment regarding their familiarity with the term, identifying where the term is typically encountered, and a brief definition elucidating its meaning. The final question serves as a test to verify the participant’s understanding (see Figure 4.7).

Participants were tasked with providing either a definition or a functional description for each term. These responses were then classified into four categories: “satisfactory,” “inaccurate,” “invalid,” or “left blank.” A definition was considered satisfactory if it demonstrated a clear understanding of the term. For instance, for “Authentication,” a response such as “Verification of user identity” would be categorized as satisfactory. Alternative responses were deemed acceptable as long as they captured the fundamental aspects of the term, which, in the case of “Authentication,” includes identity verification, access authorization, and the use of specific methods like usernames and passwords. Inaccurate definitions indicated some grasp of the term but lacked the precision required for an accurate definition or description. For example, a definition like “Can be used for authentication” for the term “Password” would be considered inaccurate. Lastly, invalid definitions clearly showed a lack of understanding of the term, while blank responses indicated that the question was unanswered (see Table 4.3).

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

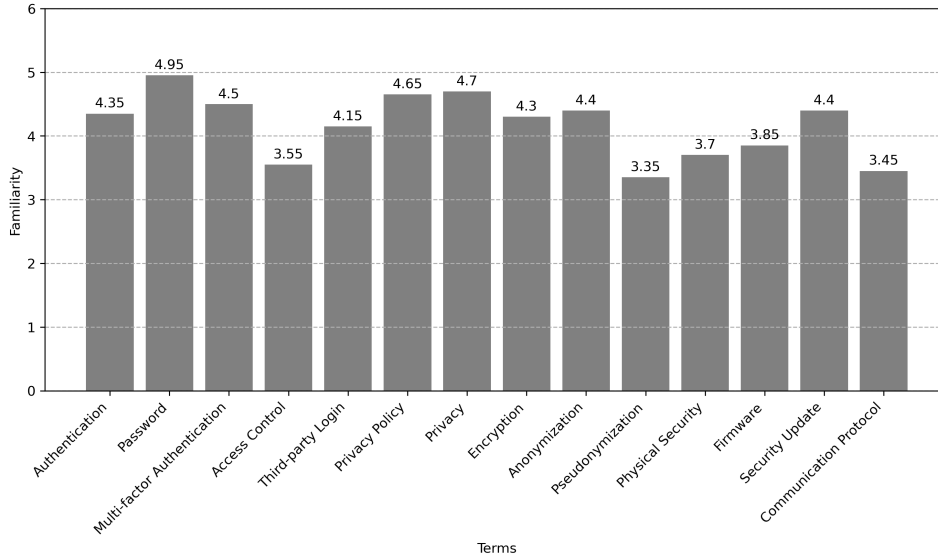


Figure 4.7: Each term is allocated a familiarity rating on a scale ranging from 1 to 5, providing a spectrum of familiarity levels (1 representing “Not familiar at all” and five indicating “Very familiar”)

Well-Informed and Behavior Intention We assessed participants’ degree of being well-informed (Q1) as they engaged with the wizard’s tasks and explored whether the wizard influenced their intentions for future behavior (Q2-Q5), along with their perception of the importance of behavior change (Q6), as shown in Table 4.4. Additionally, the behavioral intention questions displayed high reliability, as evidenced by a Cronbach’s α coefficient of 0.80, suggesting strong internal consistency among the scale items.

Model Testing In this study, we investigate the effect of privacy concerns, trust beliefs, and risk beliefs on the security behavioral intentions of smart home users. To achieve this, we conducted a detailed analysis, examining the correlations and R-squared values between these variables. We began by calculating the correlation coefficients to understand the strength and direction of the relationships between privacy concerns, trust beliefs, risk beliefs, and security behavioral intentions. Our Pearson correlation coefficient analysis revealed that:

- There is a moderate negative correlation between privacy concerns and trusting beliefs ($r(18) = -0.34, p = 0.14$), indicating that higher privacy concerns are associated with lower trust in data handling entities.
- There is a moderate to strong negative correlation between privacy concerns and risk beliefs ($r(18) = -0.55, p = 0.01$), suggesting that

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

Table 4.3: Security Terms Descriptive Statistics

| | Valid | Empty | Invalid | Inaccurate | Mean | Std. Deviation |
|-----------------------------|-------|-------|---------|------------|------|----------------|
| Authentication | 19 | 1 | 0 | 0 | 4.35 | 1.09 |
| Password | 17 | 2 | 0 | 1 | 4.95 | 0.22 |
| Multi-Factor Authentication | 17 | 2 | 0 | 1 | 4.50 | 0.76 |
| Access Control | 11 | 7 | 2 | 0 | 3.55 | 1.43 |
| Third-Party Login | 18 | 2 | 0 | 0 | 4.15 | 1.09 |
| Privacy Policy | 19 | 1 | 0 | 0 | 4.65 | 0.59 |
| Privacy | 13 | 3 | 1 | 3 | 4.70 | 0.47 |
| Encryption | 16 | 2 | 0 | 2 | 4.30 | 0.98 |
| Anonymization | 19 | 1 | 0 | 0 | 4.40 | 0.75 |
| Pseudonymization | 11 | 8 | 0 | 1 | 3.35 | 1.42 |
| Physical Security | 6 | 7 | 3 | 4 | 3.70 | 1.22 |
| Firmware | 12 | 6 | 1 | 1 | 3.85 | 1.31 |
| Security Update | 16 | 3 | 1 | 0 | 4.40 | 0.82 |
| Communication Protocol | 10 | 7 | 2 | 1 | 3.45 | 1.54 |

Table 4.4: Being Informed and Participants' Behavior Intention

| | Mean | Std. Deviation |
|------------|------|----------------|
| Question 1 | 3.30 | 0.86 |
| Question 2 | 2.70 | 1.17 |
| Question 3 | 3.85 | 1.27 |
| Question 4 | 2.90 | 1.33 |
| Question 5 | 3.40 | 1.57 |
| Question 6 | 3.25 | 1.12 |
| Q2-Q5 | 3.21 | 1.39 |

as privacy concerns increase, perceived risks decrease, potentially due to users taking proactive measures to mitigate privacy risks.

- Trusting beliefs and risk beliefs are strongly positively correlated ($r(18) = 0.61, p = 0.004$), implying that users who have higher trust are also more aware of the risks involved.
- There is a weak negative correlation between trusting beliefs and behavioral intention ($r(18) = -0.24, p = 0.30$), indicating that higher scores on Behavior Overall (Q2-Q5) are associated with lower Trusting Beliefs. However, this relationship is not statistically significant.
- There is a moderate negative correlation between risk beliefs and behavioral intention ($r(18) = -0.43, p = 0.059$), suggesting that higher scores on behavior intention are associated with lower Risk Beliefs. This relationship is marginally significant, indicating that

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

it is approaching statistical significance but does not quite meet the conventional threshold ($p < 0.05$).

Following, we calculated the R-squared values to determine the proportion of variance in security behavioral intentions explained by these factors. Our regression model showed that privacy concerns alone accounted for a significant portion of the variance in security behavioral intentions ($R^2 = 0.425$, $p = 0.002$). In contrast, trusting beliefs ($R^2 = 0.059$, $p = 0.3$) and risk beliefs ($R^2 = 0.183$, $p = 0.06$) were not significant predictors of behavioral intentions in this model.

The R-squared value of 0.425 for the regression of Privacy Concerns on Security Behavioral Intentions indicates that Privacy Concerns explain 42.5% of the variance in Security Behavioral Intentions. Similarly, the R-squared value of 0.059 for the regression of Trusting Beliefs on Security Behavioral Intentions implies that Trusting Beliefs explain 5.9% of the variance in Security Behavioral Intentions. Although the p-value is not significant, this suggests a minor role of Trusting Beliefs in predicting behavioral intentions. Additionally, the R-squared value of 0.183 for the regression of Risk Beliefs on Security Behavioral Intentions suggests that Risk Beliefs explain 18.3% of the variance in Security Behavioral Intentions. Despite the non-significant p-value, this indicates a modest influence of Risk Beliefs on behavioral intentions (see Figure 4.8).

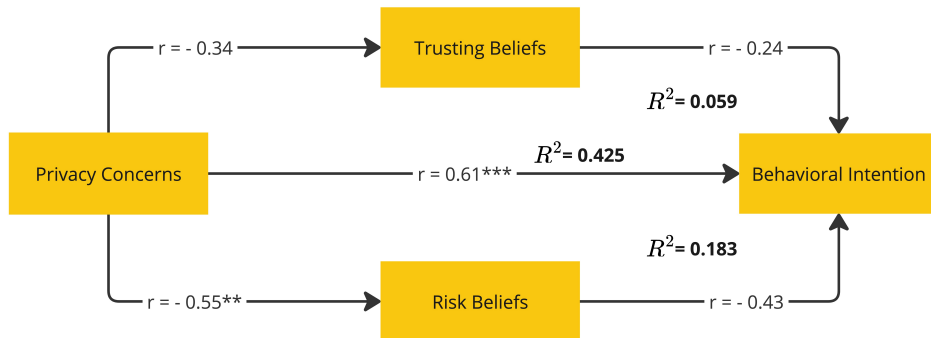


Figure 4.8: The diagram illustrates the research model employed in this study, with arrows denoting their influence on the subjects.

Participant Mental Model: Sketching Task After completing the wizard, participants were asked to create a diagram illustrating how the devices in the wizard interface communicate. The prompt specified which devices should be visible, such as the smartphone, speaker, light, and camera, while also considering invisible devices like the router and the manufacturers'

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

server. Figure 4.9 showcases a visual representation of the accurate data flow within the smart home system intended for this part of the study.

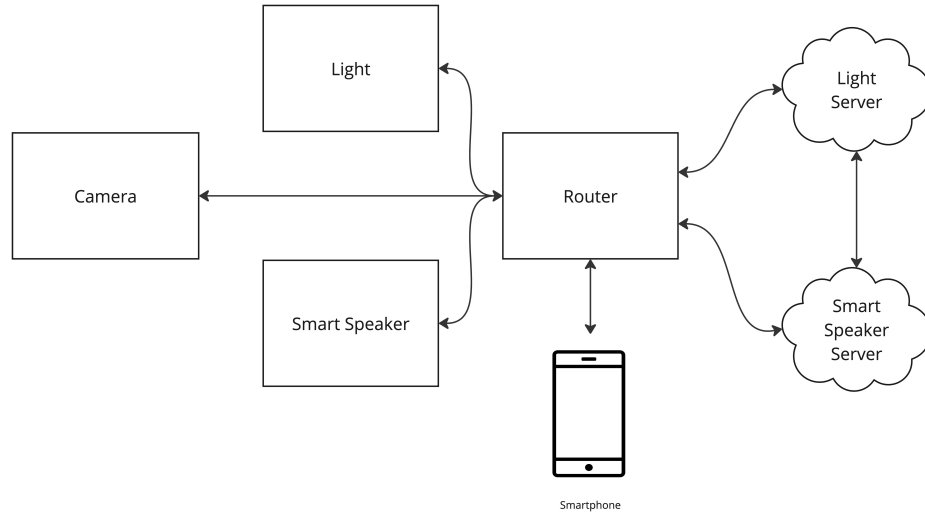


Figure 4.9: The accurate data flow model of the study

The resulting drawings can generally be categorized into two groups: those with simple representations and those with complex representations. Simple representations included only the fundamental smart home devices, whereas complex representations included devices like routers and the manufacturer’s server. Out of the total drawings, 14 accurately depicted the basic elements (camera, smartphone, speaker, and light bulb), whereas 6 had missing components, as detailed in Table 4.5. Most commonly, the manufacturer’s server, including the cloud server, was omitted in 12 drawings. Furthermore, nine drawings did not include the router, and the connection between the speaker and the light bulb was missing in 8 drawings.

| Mistakes Category | Description | Number |
|-------------------|---|--------|
| Camera | Camera not depicted | 1 |
| Smartphone | Smartphone not depicted | 3 |
| Router | Router not depicted | 9 |
| Server | Manufacturer’s server not depicted | 12 |
| Connection | Connection between speaker and light bulb not depicted | 8 |
| Connection | Incorrect connections between speaker and other devices drawn | 3 |

Table 4.5: Category of Mistakes and Number of Errors in the Sketches

Participant Mental Model: Conceptual Knowledge

- *Data Collection:* When participants were questioned about the types

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

of data their smart home devices gather, most respondents offered insights. Specifically, 15 participants discussed the light, 16 the camera, and 18 the speaker. They delved into specifics such as recording the times when the devices are turned on or off, as well as adjustments made to brightness and color settings for the light. For the camera, participants mentioned capturing both image and sound data. As for the speaker, they highlighted the collection of voice data.

Interestingly, only a handful of users demonstrated awareness of network data, which can reveal valuable insights such as the location of the devices and the identities of other gadgets connected to the network. For instance, participant Id79 provided a detailed explanation, stating, “Network data, including IP addresses, which can be used to determine location, logs of commands sent to devices, and potentially logs of interactions, particularly relevant for smart speakers with microphones, as well as data from other interconnected smart devices for coordination purposes.” Moreover, 5 participants directly referenced the importance of location data, indicating its relevance in the context of smart home operations. Additionally, 5 participants speculated that the camera might employ object recognition technology to gather relevant information.

Regarding the perceived necessity of data collection, 14 participants argued in favor of it for the light bulb, citing reasons such as marketing insights, enhancement of user experience, and troubleshooting purposes. Conversely, 4 participants deemed such data collection unnecessary, while two remained undecided. Similarly, 13 participants advocated for data collection for the camera, primarily for reasons related to security monitoring and enhancing the device’s functionality. However, 6 participants expressed reservations about the necessity of data collection for the camera, while one remained undecided. Interestingly, the perceived need for data collection was even lower for the speaker, with only 11 participants supporting it. Conversely, 6 participants questioned its necessity, while three were unsure, reflecting a greater degree of skepticism toward data collection in this context.

- *Data Storage:* Concerning data storage, most respondents ($n = 17$) were aware that the data is stored on the manufacturer’s servers. A small number ($n = 4$) also noted that data is stored within the local smart home network. Two participants mentioned third-party servers as storage locations. Notably, these responses were consistent across all devices.

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

- *Data Sharing:* All 20 respondents indicated that the device manufacturer has access to the collected data. Users themselves were mentioned 11 times as having access, and third parties were mentioned another 11 times. These third parties include advertisers, researchers, and governments. The most commonly mentioned reasons for sharing the data are monetary gain, advertising, or product improvement.
- *Data Inference:* Nine participants expressed concerns regarding data inference, emphasizing worries about the possible exploitation of their data by external parties. They fear that such misuse could lead to invasive surveillance, with two participants specifically mentioning this apprehension. Additionally, two participants highlighted concerns about manipulating user behavior based on their data. Another prevalent concern mentioned by seven participants was the creation of detailed advertising profiles, raising apprehensions about privacy invasion and targeted marketing tactics. Surprisingly, one participant even expressed concerns about the potential use of their data for planning burglaries, reflecting a heightened sense of security risk.

In contrast, the seven unconcerned participants exhibited confidence in their ability to manage data privacy or viewed data sharing as a means to enhance product functionality. Two participants expressed trust in the effectiveness of their control measures to protect their data against misuse. Furthermore, these individuals recognized the potential benefits of data sharing, particularly in optimizing product features and user experiences.

- *Data Control Perspectives:* The respondents agreed regarding the critical need for data control. However, they express dissatisfaction with the existing options, deeming them cumbersome and difficult to navigate, as highlighted by 12 participants. In adherence to EU regulations, 3 participants emphasize the necessity for provisions allowing users to request access to and delete their data. Furthermore, 2 participants mention the alternative option of abstaining from smart home devices altogether as a means of exerting control over their data privacy.

Moreover, respondents express a desire for additional control mechanisms, such as enhanced transparency regarding the collection and usage of their data. They also advocate for simpler and more user-friendly settings that empower individuals to manage their data preferences effectively.

Discussion and Limitations

The study aimed to investigate two primary questions: the degree to which users comprehend privacy and security terms related to smart home technology (Q1) and how exposure to these technical terms influences their behavioral intentions (Q2). The findings provide significant insights into the participants' understanding, concerns, and behavioral intentions regarding smart home technology and privacy.

The empirical findings revealed varying levels of familiarity and understanding among participants regarding key privacy and security terms. Participants displayed a broad spectrum of knowledge, from minimal to advanced levels, with no one indicating expert-level knowledge. This suggests that while some users have a basic or moderate grasp of these concepts, there is a clear gap in deep, technical understanding (Zwilling et al., 2022).

The structured approach to assessing comprehension showed that terms like "Authentication," "Password," and "Privacy Policy" were well understood, with most participants providing satisfactory definitions. However, terms such as "Access Control," "Pseudonymization," and "Communication Protocol" were less understood, with higher rates of inaccurate or invalid definitions. This disparity highlights the need for targeted educational efforts to improve user comprehension of more complex privacy and security concepts (Karagiannis et al., 2020). The familiarity ratings and the categorization of definitions indicate that while users may recognize these terms, their ability to accurately describe and understand them varies significantly. This partial understanding can lead to misconceptions about the security measures and privacy implications associated with smart home devices.

The study also explored how exposure to technical terms influences users' behavioral intentions. The behavioral intention questions demonstrated high reliability, indicating consistent responses among participants. The analysis of behavioral intentions revealed mixed levels of intended changes, with mean scores ranging from moderate to slightly above average. The correlation analysis provided further insights into the relationships between privacy concerns, trusting beliefs, risk beliefs, and behavioral intentions. The moderate negative correlation between privacy concerns and trusting beliefs suggests that higher privacy concerns are associated with lower trust in data handling entities. This is crucial as trust significantly influences users' willingness to engage with smart home technology (Shuhaiber and Mashal, 2019). Interestingly, there was a strong positive correlation between trusting beliefs and risk beliefs, implying that users who trust the data handling entities are also more aware of the associated risks. This awareness might

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

stem from a better understanding of the technology or more informed decision-making processes. The regression analysis showed that privacy concerns significantly predict security behavioral intentions, explaining 42.5% of the variance. In contrast, trusting beliefs and risk beliefs were not significant predictors, although they still accounted for some variance. This finding underscores the critical role of privacy concerns in shaping users' behavioral intentions toward smart home security practices (Guhr et al., 2020).

Participants' mental models, as illustrated through the sketching task and conceptual knowledge questions, revealed a mix of strengths and gaps in their understanding of the smart home ecosystem. Out of 20 participants, 14 correctly depicted the basic elements (camera, smartphone, speaker, and light) in their diagrams. This indicates that most participants had a good grasp of the fundamental components of their smart home systems. However, many participants omitted crucial elements such as routers and manufacturers' servers, indicating a limited understanding of the full data flow and communication pathways within smart home networks. This incomplete mental model can lead to underestimating the complexity and potential vulnerabilities of their smart home systems. Specifically, the omission of elements like the manufacturer's server, which was missing in 12 drawings, and the router, which was missing in 9 drawings, highlights areas where users' understanding can be enhanced. Moreover, participants' responses about data collection, storage, sharing, and inference highlighted their concerns and awareness levels. While most users were aware that data is stored on manufacturers' servers and recognized the potential for data sharing with third parties, there was considerable concern about data inference and the misuse of collected data. These concerns ranged from targeted advertising to more severe implications like surveillance and security breaches.

These findings can help explain the strong positive correlation between trusting beliefs and risk beliefs. Users who trust the data handling entities tend to have a more informed understanding of the risks involved, which might be attributed to their better grasp of the smart home ecosystem. Their awareness of data flows, potential vulnerabilities, and data handling practices likely informs their trust and perception of risks. This indicates that trust and risk beliefs are not mutually exclusive but rather interlinked through users' understanding and awareness of the technology.

While the study provides valuable insights, several limitations need to be acknowledged. First, the sample size was relatively small, and the participants might not represent the broader population of smart home users. Second, the study relied on self-reported data, meaning that participants provided information based on their recollections and perceptions. This

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

approach can introduce biases, such as social desirability bias, where participants provide answers they believe are more socially acceptable, and recall bias, where participants might not accurately remember past behaviors or experiences. Third, the wizard interface used in the study might not accurately reflect the real-world experience of using a smart home application. The simulated environment may have limited participants' ability to understand the interactions and data flows between devices fully. Moreover, there was no actual data sharing between devices in the study, which could impact participants' perceptions of smart home security. Future research should incorporate real smart home devices and data interactions to provide a more realistic assessment of users' comprehension and behavioral intentions.

Acknowledgments

This section is based on the bachelor's thesis:

Jonas Zoellner. 2024. *Influence of Understanding Security and Privacy Concepts on User Behavior in Smart Home Systems*. Unpublished bachelor's thesis. University of Bremen.

My contribution to this work: Conceptualization, data curation, formal analysis, investigation, methodology, project administration, resources, partial software development, supervision, validation, and visualization.

4.1.2 Study 11: Data Protection Compliance in Health Apps

Introduction and Background In our modern digital landscape, alongside the rise of smart homes, the significance of fitness & health apps is steadily growing. They aid individuals in achieving their health objectives and provide easy access to tailored training and health guidance. Nevertheless, as their relevance expands, concerns arise regarding protecting personal data and the transparency of privacy practices, given the sensitive nature of the information these applications handle (Papageorgiou et al., 2018; Schroeder et al., 2022). In our previous study, we underscored the necessity for service provider companies and developers to adhere to stringent standards set by regulations like the GDPR in the European Union. One essential requirement mandates obtaining explicit consent from users before initiating services, particularly concerning privacy policies. Additionally, we tackled usability concerns related to privacy policies and proposed condensing them into one-pager designs to facilitate the hurdle of navigating dense text. Nonetheless, one aspect we overlooked is how well the privacy policy texts align with the actual behavior of the applications. Concerning data transparency requirement in fitness & health apps, this study illuminates this field through interdisciplinary inquiry, connecting topics from information security to human-computer interaction and regulation.

Huckvale et al. (2019) examined the privacy practices of popular depression and smoking cessation apps by comparing their privacy policies to actual data transmission behavior. Among the 36 apps they analyzed, 25 had privacy policies, while only 22 disclosed primary data uses, and 16 mentioned secondary uses. Despite 23 apps stating data sharing with third parties, data transmission was observed in 33 apps. Moreover, it was found that 29 apps transmitted data to Google and Facebook for advertising. Interestingly, only 12 explicitly disclosed this data transmission to Google in their privacy policies, while merely 6 mentioned the transmission to Facebook. In a related study, Claesson and Bjørstad (2020) conducted a study on ten popular Android apps, examining the transmission of personal data to advertising companies. They monitored data traffic during app usage and found that while turning off ad-tracking settings, specific data like the Advertising ID and GPS location continued to be transmitted. This study revealed that all tested apps shared user data with multiple third parties, including sensitive information like IP addresses and personal attributes.

While prior studies have delved into the possibility of data being shared with third parties (Grundy et al., 2019; Bauer et al., 2020), our research takes a more targeted approach. We aim to thoroughly examine the data

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

transmission process, particularly focusing on data sent to specific countries outside the user’s home country. Additionally, we seek to investigate whether any such transmission occurs before users provide their consent to the privacy policies. Therefore, our initial research questions in this study are: 1) *To what extent do the recipients of data listed in the privacy policies and third-country recipients align with the data transmission patterns observed?* and 2) *Is there any evidence of data transmission occurring before users provide consent to the privacy policies?*

Furthermore, in this study, we explore the existence of dark patterns in designing privacy policies within fitness & health apps. Dark patterns are deceptive design tactics that intentionally undermine users’ ability to make informed decisions when interacting with digital systems (Mathur et al., 2021). These manipulative techniques may include misleading prompts, hidden costs, or confusing interfaces, all of which obstruct the user’s autonomy and clarity of choice. Despite the designer’s intentions, dark patterns have the effect of coercing users into actions or agreements they might not have chosen otherwise (Bongard-Blanchy et al., 2021). Our analysis draws upon relevant categories from existing literature. For instance, *Missing Consent Notices* dark pattern refers to the absence of expected interface elements such as checkboxes for personal data consent, thus depriving users of choice (Gunawan et al., 2021). *Disguised Data Collection* involves the covert collection of data without explicit user consent (Greenberg et al., 2014). *Obfuscation* hides essential information among less important details, often necessitating users to navigate through layers to access critical data, typically hidden behind the “Learn More” button (Conti and Sobiesk, 2010). *Forced Action* is another category of dark pattern that manipulates users into specific actions, often by omitting options to decline (Gray et al., 2018). *Privacy Zuckering* is a variant that tricks users into sharing more data than necessary, often through pre-filled checkboxes or additional prompts (Gray et al., 2018). *Misdirection* redirects user attention through elements like colored or enlarged buttons, making options like the “Accept All” button prominent (Gray et al., 2018). Lastly, *Forced Registration* mandates account creation for app usage, facilitating data collection (Bösch et al., 2016).

Many studies have observed the growth of dark patterns in mobile applications. A comparative study conducted by Di Geronimo et al. (2020) examined the prevalence of dark patterns and their influence on user perception. The researchers categorized dark patterns and analyzed 240 popular Google Play Store apps, revealing their ubiquity in 95% of the sampled apps. Specifically, the analysis showed that 10% of the apps exhibited 0-2 dark patterns, 37% contained 3-6, and 49% featured 7 or more. Additionally, an online survey

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

conducted as part of this study found that many respondents struggled to identify Dark Patterns: 55% could not recognize them, 20% were uncertain, and only 25% could accurately identify these deceptive design elements. The findings suggest a noteworthy lack of user awareness regarding dark patterns in mobile applications. While this study contributes valuable insights into the prevalence of dark patterns in apps, Van Kleek et al. (2017) pursued a distinct objective, which was to bolster user awareness regarding data usage before app download. Their research aimed to enhance transparency by developing “Data Controller Indicators” within a simulated app store environment, illustrating data flows, the rationales behind data collection, and the entities receiving collected data. Through rigorous user testing, they discerned a clear preference among participants for apps with minimal data processing. They observed a heightened sense of confidence among users when presented with transparent data usage information. Thus, the findings from Van Kleek et al. (2017) underscore the pivotal role of pre-download transparency in empowering users to make well-informed decisions. In addition to transparency, this study focuses on dark patterns, which pose IT security risks by tempting users to disclose personal data or consent to risky data practices within sensitive applications. As a result, we pose the next research question: *3) What is the prevalence of dark patterns in the privacy policy forms of fitness & health apps?* Furthermore, this study intends to leverage the findings from the previous research questions to explore whether the information transparency provided in the privacy policies of fitness & health apps is satisfactory and to what degree users grasp how their data is employed and distributed. Therefore, the fourth research question is: *4) How comprehensively do privacy policies of fitness & health apps delineate information about data recipients, transfers to other countries, and the utilization of personal data?*

To address our research questions, we structure the methodology of this study into three key components. Firstly, we curate a selection of relevant fitness & health applications, adhering to predefined criteria for selection, which will be elaborated on in the subsequent section. Secondly, we thoroughly analyze the privacy policies of the chosen apps. These findings are then juxtaposed with the outcomes of the technical analysis of these apps, facilitating an evaluation of the alignment between the privacy policy and the actual behavior of the apps. Additionally, we give particular attention to examining consent forms for dark patterns and design elements that may sway user actions or obscure information. This holistic approach aims to assess the transparency and informational integrity of apps in protecting user privacy.

Methodology

Concept This study employed a multifaceted methodology to meticulously analyze a curated set of mobile applications available in Germany, focusing on their underlying codes, detecting dark patterns, and evaluating compliance with privacy policies. The technical analysis was conducted using a hybrid approach, combining static and dynamic methods. The static analysis delves into the APK files of the applications without execution, employing tools such as MobSF to dissect their code and structural components. On the other hand, dynamic analysis involves the active execution of apps to observe real-time behaviors and user interactions, especially concerning the transmission of personal data. This process was facilitated by network monitoring software, enabling detailed observation and data collection. In order to prepare for the dynamic analysis, an Android smartphone was rooted and configured with specific permissions activated and monitoring tools installed, creating a controlled environment conducive to a thorough examination.

In addition to technical analysis, the privacy policy user interfaces of the apps were scrutinized for the presence of any dark patterns or manipulative design elements intended to deceive or drive users into certain actions. Finally, the privacy policies of the selected apps underwent a thorough review to identify involved third parties, types of collected personal data, and potential data transfer destinations. These findings were systematically tabulated to facilitate comprehensive comparison and analysis, enabling a thorough understanding of the apps' privacy practices and potential risks to users.

App Selection For this study, we selected 20 mobile applications from the Google Play Store, concentrating on the "Health & Fitness" and "Medical" categories due to their handling of sensitive data, emphasizing the need for transparent and secure communication with users (Wykes and Schueller, 2019). To ensure a comprehensive study, we chose apps that appeal to a diverse audience and represent various user demographics. Moreover, accessibility played a pivotal role in our selection process. Therefore, All chosen applications had to be provided for free, ensuring that users could download and use them without any cost. Our experimental design prioritized independent analysis, avoiding the necessity for input from medical professionals. Hence, apps requiring interaction with medical personnel, such as appointment scheduling or video consultations, were excluded. Similarly, apps focused on medical personnel training were also omitted. We excluded specific categories of apps to maintain a focus on general health and fitness. These included COVID-19 apps, especially those affiliated with the Robert Koch Institute, as well as apps associated with DiGA (Digitale Gesundheit-

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

sanwendungen, translated as “Digital Health Applications”), which target managing specific health conditions and are typically used by individuals covered by statutory health insurances. Furthermore, service apps of statutory health insurance companies in Germany were excluded to provide relevance to a broader public audience.

With reference to our selection criteria, the apps were determined based on their download count using AndroidRank¹ data. The chosen apps from the “Health and Fitness” and “Medical” categories are presented in Table 4.6.

Table 4.6: Health & Fitness and Medical Apps

| Rank | Name | Developer | Downloads |
|-----------------------------|--------------------------------|--|-----------|
| Health & Fitness | | | |
| 1. | Samsung Health | Samsung Electronics Co., Ltd | 1B |
| 2. | Period Calendar Period Tracker | Simple Design Ltd. | 100M |
| 3. | Home Workout – No Equipment | Leap Fitness Group | 100M |
| 4. | Zepp Life (MiFit) | Anhui Huami Information Technology Co., Ltd. | 100M |
| 5. | MyFitnessPal: Calorie Counter | MyFitnessPal, Inc. | 100M |
| 6. | Six Pack in 30 Days | Leap Fitness Group | 100M |
| 7. | Google Fit: Activity Tracking | Google LLC | 100M |
| 8. | Flo Ovulation & Period Tracker | Flo Health Inc. | 50M |
| 9. | Sweatcoin | Sweatco Ltd. | 50M |
| 10. | Lose Weight App for Men | Leap Fitness Group | 50M |
| Medical | | | |
| 1. | My Calendar - Period Tracker | SimpleInnovation | 10M |
| 2. | amma: Pregnancy & Baby Tracker | PERIOD TRACKER & PREGNANCY AND BABY CALENDAR | 10M |
| 3. | Blood Pressure | Klimaszewski Szymon | 10M |
| 4. | Ada – check your health | Ada Health | 5M |
| 5. | Pregnancy Tracker | Amila | 5M |
| 6. | Period and Ovulation Tracker | SMSROBOT LTD | 5M |
| 7. | MyTherapy Pill Reminder | MyTherapy | 5M |
| 8. | Ladytimer Ovulation Calendar | Vipos Apps | 5M |
| 9. | Medscape | WebMD, LLC | 5M |
| 10. | Ovia Pregnancy & Baby Tracker | Ovia Health | 1M |

Static Analysis We employed the Mobile Security Framework (MobSF) in the static analysis stage to investigate the selected apps. MobSF is a versatile tool designed for penetration testing, malware analysis, and static security assessments. While MobSF boasts a wide array of functionalities, we focus here on elucidating the pertinent features we utilized. One key aspect of MobSF is its capability to inspect the permissions requested by an app extracted from the “AndroidManifest.xml” file. These permissions delineate the actions an app may seek the user’s consent for, such as accessing location information or camera functionality. Our goal is to determine whether these permissions imply the collection of personal data, which can then be cross-referenced with disclosures in privacy policies.

Moving forward, we explore network security within the “Security Analysis” section of MobSF for each individual app. The findings may flag potential vulnerabilities necessitating further investigation. For example, as illustrated

¹<https://www.androidrank.org/>

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

in Figure 4.10, the initial entry indicates that the app transmits unencrypted messages, prompting a deeper probe into potential risks to user data security.

| NO ↕ | ISSUE ↕ | SEVERITY ↕ |
|------|---|------------|
| 1 | Clear text traffic is Enabled For App [android:usesCleartextTraffic=true] | high |
| 6 | Activity (com.myfitnesspal.feature.recipes.ui.activity.RecipesAndFoods) is not Protected. [android:exported=true] | high |
| 7 | Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true] | high |

Figure 4.10: Overview of the permissions determined for an app using MobSF

Furthermore, MobSF facilitates the identification of communication channels between apps under scrutiny and distributed servers. It includes details such as server location, IP address, and domain name, aiding in pinpointing server operators and their industry affiliations, whether it involves advertising or providing services. This information is crucial for assessing whether data transmission occurs across borders. Figure 4.11 provides a snapshot from the analysis of a healthcare app, revealing communication with the Indian-based advertising firm Inmobi. Static analysis also examines the libraries employed, laying the groundwork for subsequent steps, notably dynamic analysis.

Dynamic Analysis The technique employed in the dynamic analysis draws inspiration from the approach outlined by Claesson and Bjørstad (2020). To create our testing environment, we utilized a Google Pixel 2 XL running Android 10 within a home network setting. During the dynamic analysis stage, we looked at app network communications in real-time using Burp Suite², a comprehensive tool developed by Portswigger for web or application security testing and analysis of HTTP traffic. In order to set up our analysis, we configured Burp Suite’s proxy server with port 8082. This configuration enables us to intercept and inspect outgoing messages from the mobile device within the Burp Suite interface. Finally, the network settings on the mobile phone must be set so that all outgoing network messages from the mobile phone also run via the same port.

The majority of outgoing network traffic is indeed encrypted using the HTTPS protocol. However, it is essential to decrypt encrypted messages for

²<https://portswigger.net/burp>

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

| | | |
|------------------------------------|----|---|
| config.inmobi.cn | ok | IP: 39.105.228.126 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map |
| config.inmobi.com | ok | IP: 104.45.180.93 Country: United States of America Region: Virginia City: Washington Latitude: 38.713451 Longitude: -78.159439 View: Google Map |
| configuration-api.myfitnesspal.com | ok | IP: 54.208.251.183 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map |

Figure 4.11: Advertising firm and IP address identified via MobSF analysis

the purpose of this study. One method involves utilizing the Burp Suite tool to install a self-signed certificate, facilitating a Man-in-the-Middle attack. This process installs a certificate that allows the examined app to trust Burp Suite as an intermediary, enabling the decryption of the network traffic. Despite Android 10 permitting the installation of self-signed certificates, it segregates them into two distinct storage areas. These certificates are stored in the user certificate storage, yet apps installed on the device solely trust certificates from the Trusted Credential Storage³.

Therefore, the decryption of network messages becomes impossible. In order to bypass this security measure, we rooted the Android smartphone. A rooted device grants users the ability to execute privileged actions typically inaccessible. This is achieved by running processes with UID zero, causing all privileged processes to disregard permission checks from the system's kernel. Additionally, users gain the capability to manipulate system files,

³<https://developer.android.com/privacy-and-security/security-ssl>

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

including adding, editing, or deleting them. Preparing the device for rooting is a necessary step. Android complicates direct alterations to the kernel system, prompting users to modify the bootloader⁴ instead. The bootloader initializes and launches the kernel on a device while monitoring its status. In order to acquire separate permissions, a program must be installed on the bootloader, necessitating the initial unlocking of the bootloader to allow the initiation of third-party programs directly. This step can be accomplished through the developer option provided by Android.

Upon unlocking the bootloader, Magisk⁵ was installed. Magisk serves as a tool for modifying Android devices without altering the core system, known as systemless rooting. This approach affords users complete control over their devices without directly impacting the system itself. Unlike traditional rooting methods, Magisk is initialized directly by the bootloader upon device startup, avoiding direct system modifications. Notably, this technique circumvents detection by various apps designed to identify rooted devices, including Google's SafetyNet⁶. Installing Magisk on the bootloader facilitates the detection of rooted devices, potentially influencing app execution and analysis results.

Following installation on the bootloader, a fully privileged Magisk daemon with UID:0 is executed during the booting process. This daemon can grant root privileges to any process requiring them. Moreover, Magisk supports the installation of extensions. For analytical purposes, the Magisk Trust User Certs extension⁷ was installed. This module enables the installation of all user-installed certificates into the trusted certificate storage during system startup, ensuring that all apps on the device trust these certificates. Consequently, in conjunction with Burp Suite, all encrypted outgoing and incoming HTTPS messages can be decrypted directly from the device.

After the device has been prepared, network activities are monitored using Burp Suite. Serving as an intercepting HTTPS proxy, Burp Suite renders encrypted TLS data in a comprehensible format, as illustrated in Figure 4.12. Among the transmitted data, certain personally identifiable information such as local IP address, country, and language can be observed coming from the host *branch.io*. Burp Suite facilitates the interception and decryption of these transmissions.

It is necessary to note that many of these transmitted messages are further encoded in an unreadable format. While encoding differs from encryption, it

⁴<https://source.android.com/docs/core/architecture/bootloader>

⁵<https://topjohnwu.github.io/Magisk/>

⁶<https://developer.android.com/privacy-and-security/safetynet>

⁷<https://github.com/NVISOsecurity/MagiskTrustUserCerts>

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

| Host | Method | URL | Params | Status | Length | MIME type | Title |
|------------------------|--------|----------|--------|--------|--------|-----------|-------|
| https://api2.branch.io | POST | /v1/open | ✓ | 200 | 780 | JSON | |
| https://api2.branch.io | GET | /v1/open | | | | | |

| Request | Response |
|---|---|
| <pre>"brand": "Google", "model": "Pixel 2 XL", "screen_dpi": 560, "screen_height": 2712, "screen_width": 1440, "wifi": true, "ui_mode": "UI_MODE_TYPE_NORMAL", "os": "Android", "os_version": 29, "cpu_type": "aarch64", "build": "OP1A.190711.020", "locale": "en_US", "connection_type": "wifi", "os_version_android": "10", "country": "US", "language": "en", "local_ip": "192.168.178.40", "app_version": "22.22.0", "facebook_app_link_checked": false, "is_referrable": 0, "debug": false,</pre> | <pre>1 HTTP/2 200 OK 2 Content-Type: application/json 3 Content-Length: 289 4 Access-Control-Allow-Origin: * 5 Cache-Control: no-cache 6 Date: Wed, 23 Nov 2022 17:55:22 GMT 7 Strict-Transport-Security: max-age=31536000; includeSubDomains 8 X-Branch-Request-Id: 8d98520efd0749139f41ba584fc8b2e8-2022 112317 9 X-Cache: Miss from cloudfront 10 Via: 1.1 d050e2738eeca6f287a6d79edd9743de.clou dfront.net (CloudFront) 11 X-Amz-Cf-Pop: HAM50-C1 12 X-Amz-Cf-Id: Z3f580PARMcDzbaR9DH7B1DbxjnSvXbtE3vEI OgpKOO_9M2gFXoIOA== 13 14 {</pre> |

Figure 4.12: Monitored network communication using Burp Suite

is commonly utilized to minimize the file size of transmitted data. Common encoding methods found in HTTPS messages encompass URL, Base64, ASCII Hex, Octal, Binary, or GZIP. Decoding messages usually involves identifying the encoding method, often omitted during transmission, complicating the decoding process. Burp Suite offers tools to identify the encoding format and decode accordingly. Although frequently utilized in the analysis, it is worth mentioning that some messages, primarily those from Google, could not be decoded, rendering them unreadable.

A test persona named *Petra Muster* was created to facilitate dynamic analysis. We have generated various health data points for this person, including weight, age, gender, temperature, and date of birth. Further, technical data such as the Google Advertising ID and the Device ID were collected to facilitate locating them in the data stream of network transmissions.

At the outset of the dynamic analysis, the app is freshly installed and left to run for 5 minutes without any interaction. Throughout this period, network transmissions are closely monitored. Next, the app is executed until consent to a privacy policy is required. If personal data is found to be transmitted at this stage, it would be considered a breach of the privacy policy, as consent has not yet been obtained. Additionally, an examination is conducted to ensure that the language of the displayed privacy policy matches the language of execution. Following this, consent is granted, and the app is put through all functionalities to determine whether the transmitted data and the destinations of these transmissions align with the terms outlined in the privacy policy. Lastly, it is verified whether the app offers a mechanism for users to revoke consent to the privacy policy within its interface.

Dark Patterns Analysis In this study, one of our focuses was uncovering dark patterns embedded within user-facing consent agreements. We captured screenshots of all privacy policy agreement interfaces through dynamic analysis, subjecting them to detailed scrutiny afterward. Initially, we conducted an exhaustive examination to identify potential dark patterns and documented their occurrences. Subsequently, we synthesized a comprehensive list of recurring dark patterns, streamlining the classification process for apps privacy policy agreements. This compiled inventory encompassed a variety of potential dark patterns, including Misdirection, Forced Action, Obfuscation, Disguised Data Collection, Missing Notices and Options, and Forced Registration (Luguri and Strahilevitz, 2021).

Privacy Policies Analysis We examined the privacy policies of selected applications through a systematic process. Firstly, we thoroughly reviewed each privacy policy, carefully examining the disclosed information regarding third-party recipients, third countries involved in data processing, and the types of personal data collected. Next, we meticulously cataloged all third-party recipients mentioned in the privacy policies. These entities ranged from specific corporations like Google or Facebook to more general designations such as “Business Partners” or “Companies for purposes of analytics.” Subsequently, we analyzed the section about data processing outside the originating country.

We identified all mentioned foreign countries and determined the legal basis associated with data processing in these jurisdictions. Whether explicitly named or described using terms like “Outside the European Economic Area,” we documented these instances. Lastly, we cataloged all types of personal data and health-related information mentioned in the privacy policies. We then compared our findings with data obtained from both static and

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

dynamic analyses. This comparative analysis allowed us to highlight any inconsistencies or discrepancies between the disclosed privacy policies and the actual operational practices of the respective applications. Figure 4.13 visually summarizes the investigation process.

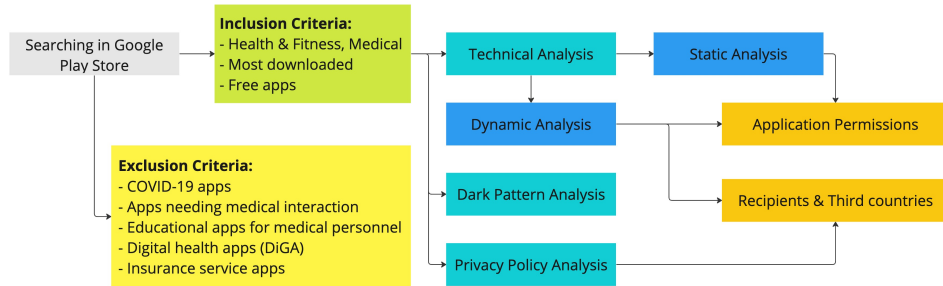


Figure 4.13: Overview of analysis steps and objectives

Empirical Findings

Recipients of Transmitted Data One of the essential parts of our analysis was examining the data recipients with whom communication was established. We categorized these recipients by analyzing the outcomes of static and dynamic analyses, evaluating the privacy policies, and conducting subsequent Whois searches online. Notably, a recipient may belong to multiple categories, reflecting the multifaceted nature of their involvement. The identified recipients fell into distinct groups:

- *Advertising Companies*: Specialized entities leveraging data for targeted advertising.
- *Analytical Services*: Providers that collect, measure, and analyze user behavior within the apps for insights and personalized marketing.
- *Information Providers*: Offering users valuable information, such as dietary habits, sleep patterns, and crisis assistance.
- *Governmental Bodies*: Dispensing information and standards at the governmental level.
- *Service Providers*: Offering a range of technical services for apps, including cloud computing, development tools, and artificial intelligence.
- *Social Media Platforms*: Facilitating social interactions on networks like Facebook, Twitter, and Instagram.

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

- *Potentially Malicious Entities*: Hosts posing security risks, such as fraudulent activity or malware distribution.
- *Partners*: Likely contractual collaborators contributing to app development or functionality.

Figure 4.14 illustrates the categorization of recipients in the analysis. Remarkably, recipients categorized as “advertising companies” were frequently encountered, totaling 49 instances. This finding highlights a widespread dependency on numerous advertising entities, averaging 2.45 per app. Moreover, our analysis of the “Sweatcoin” app revealed communication with potentially harmful hosts, “dewrain” and “akisinn,” flagged as possible malware by MobSF. Nevertheless, no definitive outcomes were yielded for these hosts in the subsequent Whois search.

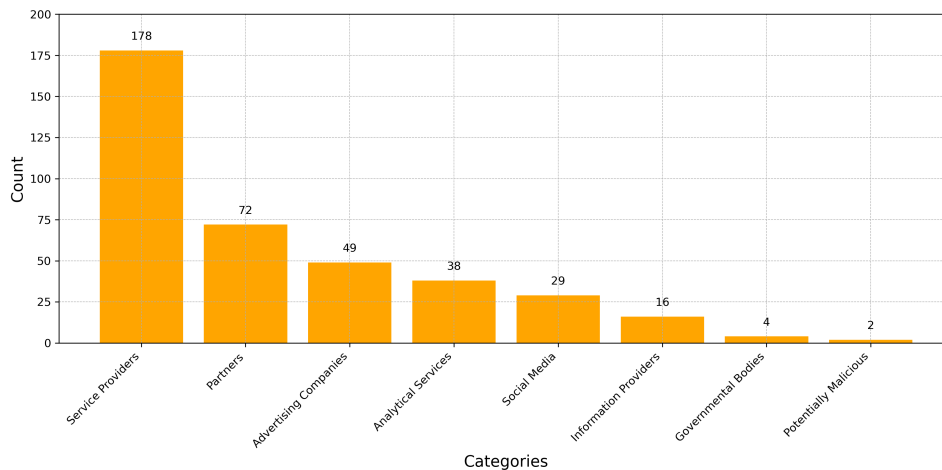


Figure 4.14: Number of recipients found in the respective categories

Data Transfers to Third Countries Most of the analyzed apps were developed in the USA or designed for users from the USA. Furthermore, each app communicates with Google in different capacities, whether as an advertising company or an analytical service. While Google’s locations are distributed, they all have at least one base in the USA. As a result, all 20 examined apps send their data to the USA. Additionally, Figure 4.15 indicates that 40% of the communications are sent to Ireland. Ireland is favored as a headquarters for many major industries in Europe due to its favorable climate for server cooling and low corporate tax rates (Fox, 2022; Dodd, 2023).

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

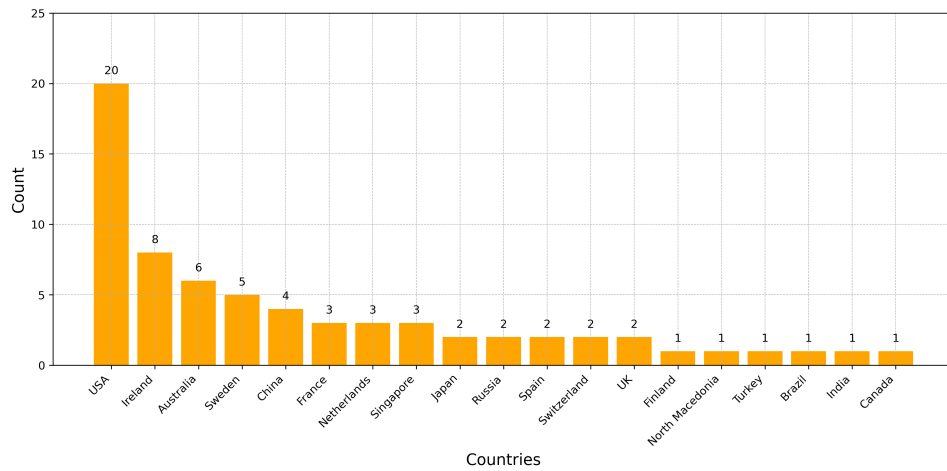


Figure 4.15: Server locations of third-party recipients

Transmitted Data without Consent Our static analysis revealed that most of the examined applications communicate with servers outside the EU. Another critical aspect involves observing the transmission of personal data, mainly focusing on data sent before obtaining consent for its processing. Additionally, the destination of the transmitted data is significant, as the GDPR mandates consent for data transmission to third countries. This aspect of the analysis was carried out using dynamic analysis. However, it is essential to note that the identified data may present a partial result, as only the data found or decrypted during the investigation are represented. Figure 4.16 illustrates all data that were transmitted before users consented to the privacy policies in our analyzed apps.

According to the GDPR, “personal data” is defined as information that can lead to the identification of an individual (Voigt and Von dem Bussche, 2017). Figure 4.16 illustrates that the Google Advertising ID was identified in 13 of the analyzed apps. This ID serves as a unique identifier for advertising purposes, assigned to each Android device via Google Play. While it can be reset, deactivation is not an option (Google, 2024). The European Commission classifies this information as personal data, referring to it as “the advertising identifier of your phone” (European Commission, 2024). Additionally, hardware details were detected in 13 apps, while data about the country, languages, or time zones were found in 9 apps. For instance, hardware information was transmitted to a Facebook server in the My Calendar app (developed by SimpleInnovation). The transferred message included an indication labeled “ROOTED:1,” suggesting that the app may detect a rooted smartphone, along with details about the device model.

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

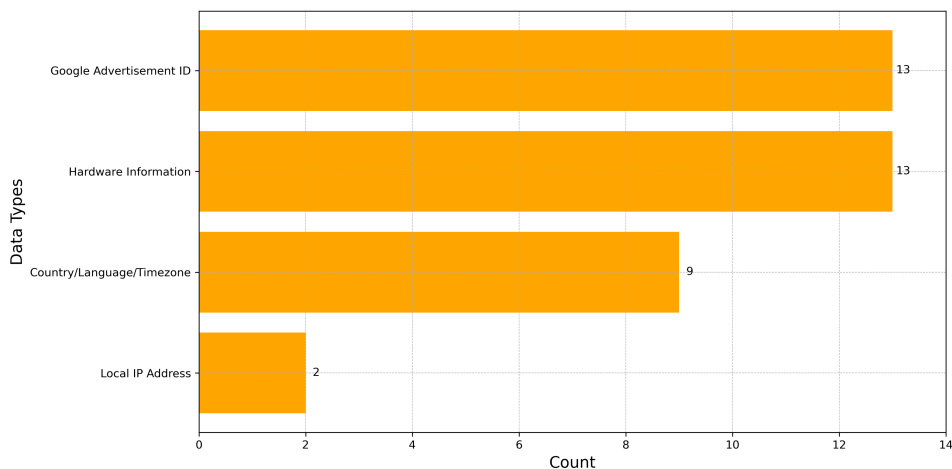


Figure 4.16: Data sent before consent to the privacy policy was obtained

Although a Magisk module was intended to conceal the rooted status, our analysis revealed that certain apps could still detect it.

Furthermore, the investigation revealed the transmission of local IP addresses. A local IP address, also known as an internal or private IP address, is a numerical label assigned to devices within a local network, such as a home or office network. Nonetheless, when users move outside a home network, they typically switch to mobile data, where a dynamic IP address is assigned to facilitate communication between servers and mobile devices. However, evidence indicates dynamic IP addresses may be categorized as personally identifiable information (Borgesius, 2017).

Consent Dialogs and Dark Patterns: We examined the privacy policies of the apps to identify potential dark patterns. In the case of “Blood Pressure” (Developed by K. Zsymon) and “Ladytimer Ovulation Calendar” (Developed by Vipos Apps), users were not provided with an option to consent to the privacy policy. No window was displayed to inform users about the processing of personal data or to obtain consent. Access to the privacy policy was only possible through the settings of the respective apps.

Consequently, these apps were excluded from this aspect of the analysis. Although the app “My Calendar-Period Tracker” (Developed by Simple Design Ltd.) did present a consent window for the privacy policy, it appeared only upon the second launch of the app, indicating a potential software issue. Nevertheless, data processing was observed during the first launch.

Despite this discrepancy, the app was still examined for dark patterns, and the results were documented during the second launch. In total, 18

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

out of 20 apps underwent analysis to identify the presence of dark patterns. Figure 4.17 illustrates the study outcomes, revealing that every app analyzed exhibited at least one instance of a dark pattern.

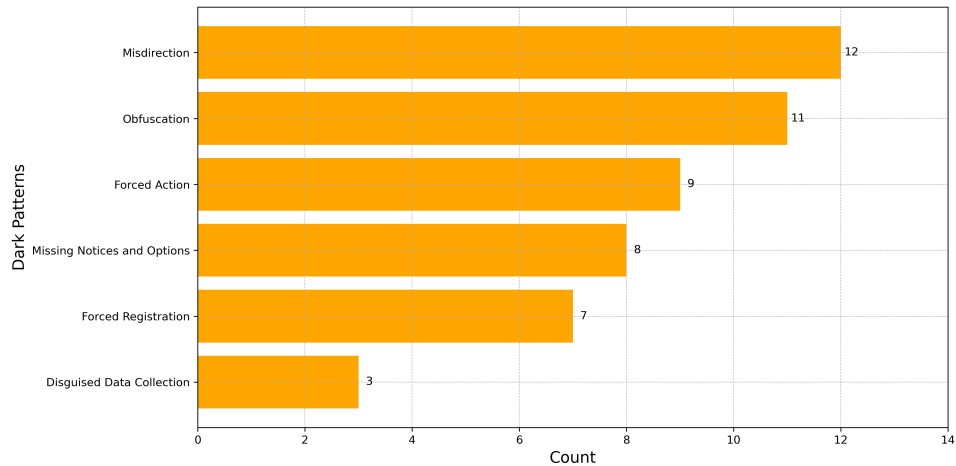


Figure 4.17: Dark patterns found in the user interface of privacy policies

The most prevalent dark pattern identified was Misdirection, which uses design elements to distract users’ attention from crucial information. For instance, in Figure 4.18, example (a) shows a screenshot from the Sweatcoin app (developed by Sweatco Ltd.), where different colors are used for various buttons. The “Registrieren mit Google” (translated as “Register with Google”) button is prominently highlighted with a white background, making it more visually appealing and likely to be selected by users, even though they also have the option to register with other accounts. Below these two options is the privacy policy explanation, rendered in a gray font without additional design elements, making it less noticeable.

A similar manipulation is seen in example (c), where users are prompted to click the “Einwilligen” (translated as “Consent”) button. Another variation of Misdirection appears in example (b), where sensitive data collection details are listed, whereas an “Accept All” checkbox is provided to encourage users to skip reading the details. This design nudges users to consent to all options directly, thus bypassing the detailed information about the collected data.

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

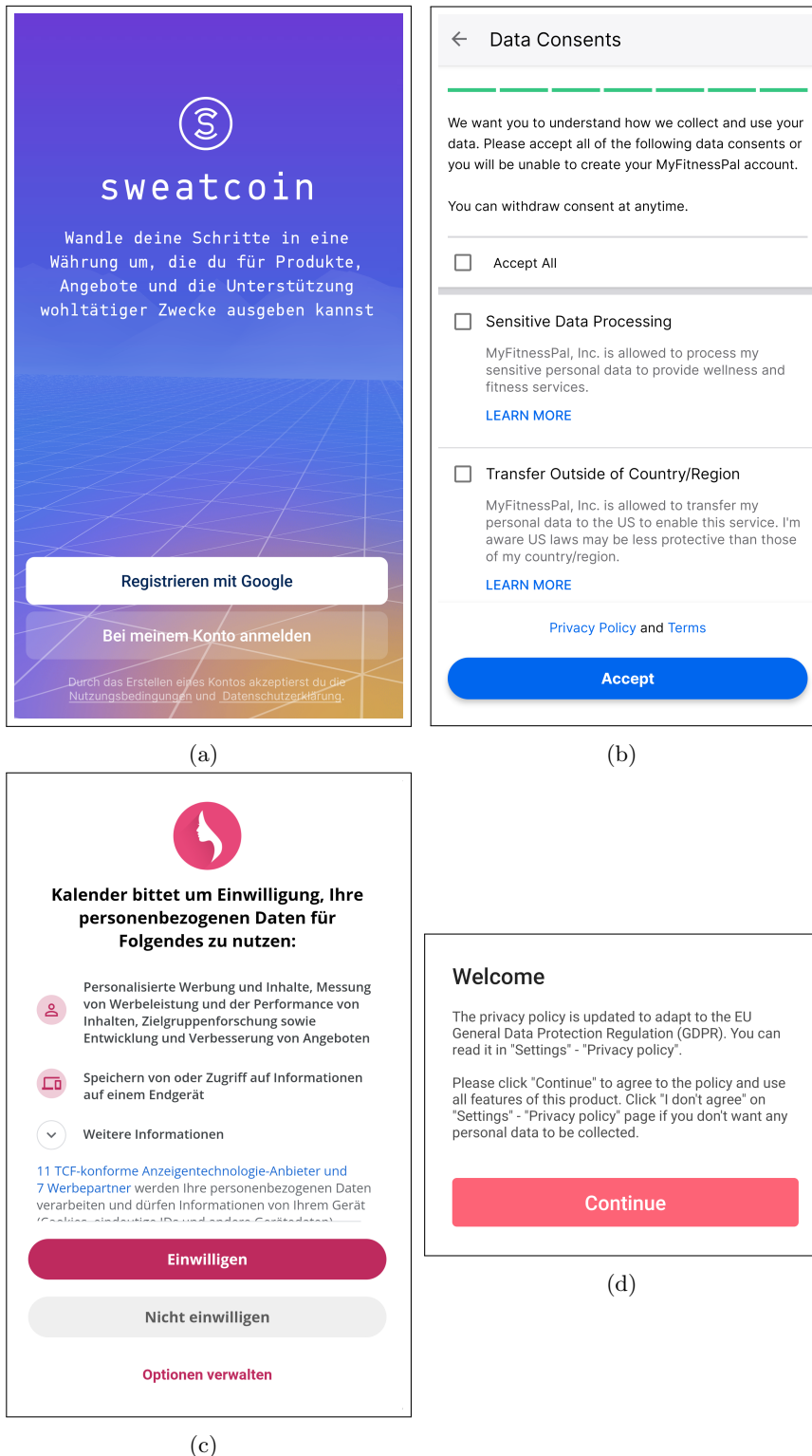


Figure 4.18: Privacy policy screenshots

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

In the case of Obfuscation, important information is deliberately withheld from the user. In example (a), the privacy policy screen design provides no information directly to the user, requiring them to open a link to read the privacy policy and learn about handling their personal data. Similarly, example (d) fails to present any information within the dialog. It does not allow access to the privacy policy, leaving the user without any means to obtain the necessary information. Additionally, important information is only partially displayed. In examples (b) and (c), while some details are listed, users must click the “LEARN MORE” button in example (b) and the “Optionen verwalten” (translated as “Manage options”) button in example (c) to access comprehensive information. However, neither example (b) nor example (c) provides a complete picture of all collected sensitive data.

In the case of Forced Action, users are not given the option to decline, compelling them to perform a specific action to continue using the app. examples (a), (b), and (d) do not allow users to refuse the collection of personal data while still using the app. In examples (a) and (d), there are no design elements that permit rejection. Although example (b) includes checkboxes that users can leave unchecked, the app becomes unusable if they do so. On the other hand, example (c) offers an option to decline the collection of sensitive data while continuing to use the app.

Moreover, some apps, such as “MyFitnessPal” (developed by MyFitnessPal, Inc.), inform users during account creation and consent to the privacy policy so that they can revoke their consent. However, they fail to mention that this requires deleting the account. By this point, users may have become habituated to the app, making it more challenging to delete their accounts.

Among the 18 apps analyzed, eight neglected to offer privacy choices, provide checkboxes for distinct personal data categories, or empower users to govern their data rights. With the exception of example (b), none of the showcased apps permit users to specifically consent to categories of information such as health, fitness, or location data. Instead, users are merely prompted for broad consent, lacking the capacity to tailor their consent for different data types.

In the case of Forced Registration, users are required to register and create an account. This dark pattern often appears alongside Forced Action, yet they are distinct. While examples (a), (b), and (d) illustrate instances of Forced Action, Example (d) does not require an account to use the app. The app functions without an account as long as consent to the privacy policy is given. However, seven apps mandated account creation, allowing the developer to store data about the users.

Finally, we examined the scenario of Disguised Data Collection, where

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

the user's personal data is collected without explicit consent to the privacy policy. Example (a) indicates that the user agrees to the privacy policy by creating an account. However, when combined with other dark patterns like Misdirection, users may not fully grasp that they are consenting to the privacy policy during this stage of app usage. Additionally, it was noted that the design of consent dialogs varies even among apps from the same company. Three distinct apps from the Leap Fitness Group were thoroughly analyzed. While the consent dialogs of the apps "30 days sixpack" and "Lose Weight for App for Men" (both developed by Leap Fitness Group) remained consistent and provided users with some information regarding the use of their data, the confirmation dialog for the app "Home Workout - No Equipment" (also developed by Leap Fitness Group) appeared outdated and offered no information to the user (refer to Figure 4.19).

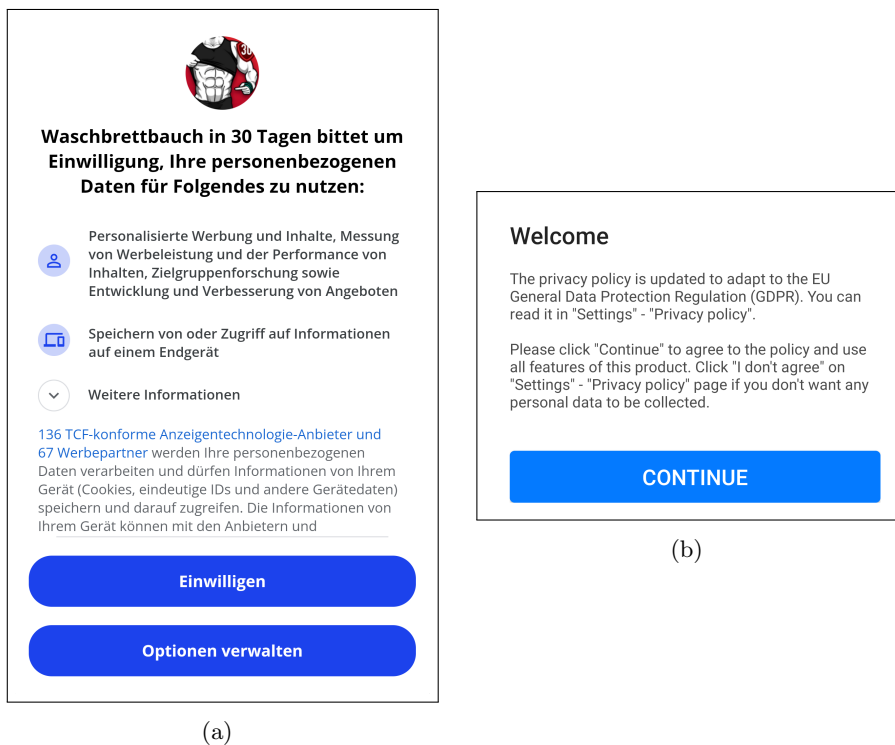


Figure 4.19: Privacy policy interfaces within apps developed by Leap Fitness Group

In the analysis of the applications "Home Workout - No Equipment" (refer to Figure 4.19 - (b)) and "My Calendar" (refer to Figure 4.18 - (d)), it was observed that although users are presented with an interface element to consent to a privacy policy, they are not offered an option to access the privacy policy (e.g., via a link). In these applications, users are required to

consent to the privacy policy before being given the chance to review it.

Revocation and Language Another dimension of our analysis delved into the presentation of privacy policies across different languages and the extent to which users could retract their consent. Among the 20 analyzed applications, two did not allow users to access the privacy policy, narrowing our evaluation down to 18 apps. Remarkably, seven apps lacked mechanisms for users to modify or retract their consent once granted. Subsequently, we thoroughly examined the language used in presenting these privacy policies. Of the remaining 18 apps, only two were exclusively available in English, necessitating their exclusion from this linguistic analysis.

Interestingly, all 16 apps in this analysis offered German language support, with their interface elements exclusively presented in German. However, it is noteworthy that the privacy policies of 10 of these apps were solely articulated in English. This discrepancy underscores a potential language barrier for German-speaking users, particularly those with limited proficiency in English, who may need help comprehending the handling of their personal data in the majority (63%) of the apps studied, except during the initial consent dialogue.

Privacy Policy Analysis In this part of the study, we compared information obtained from static and dynamic analyses with the disclosures in privacy policies to evaluate their accuracy and transparency.

- *Data Transfers to Third Countries:* Data transfers to third countries were compared through static analysis with the corresponding privacy policy disclosures. In two instances, privacy policies did not mention data transfers despite evidence of such transfers in the static analysis. Overall, 55% of the examined apps did not specify particular countries, opting instead for general categories like “European Union” or “operating offices.” Moreover, combinations of third countries and categories were common, such as repeated mentions of the USA alongside the European Union, making it challenging for users to track data transfers accurately. Despite efforts to catalog identified countries and compare them with defined categories and explicitly named countries, only a 75% match was achieved. This discrepancy indicates that in five apps, users could not learn about data transfers to third countries. The lack of precise or missing information about data transfers significantly hampers transparency, as vague or evasive language leaves users uninformed about the actual destinations of their personal data.
- *Recipients of Transmitted Data:* The recipients of transmitted data

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

were also categorized. Although each privacy policy listed names or categories of potential recipients, an 85% overall match was found between static analysis results and privacy policy disclosures. Privacy policies tended to list recipients primarily in categories, with 60% of the apps using categories instead of explicitly naming recipients. These categories often employed broad terms like “Service Partners,” “Analytics Partners,” or “Advertisement Partners.” Interestingly, 55% of these categories included more than ten potential recipients, raising questions about whether these categories might be overly broad. Conversely, 40% of the privacy policies listed only two or fewer recipients in a category, suggesting that individual recipients could be named for clarity. Moreover, 55% of the apps listed more categories than exactly identified recipients, mentioning categories for recipients that may not exist, potentially undermining transparency. We also examined whether prominent and frequently used companies related to data sharing, especially in advertising networks or tracking services like “Google Analytics,” were explicitly named. Such companies were explicitly named in only 75% of the examined cases, raising the question of whether capturing widespread advertising companies and tracking services in more general categories instead of explicitly naming them enhances user transparency.

- *Requested Personal Data:* The requested personal data was analyzed, revealing challenges in comparing them with the corresponding apps. Permissions obtained through static analysis and MobSF provided minimal information about personal data, often limited to the user’s location information. However, this finding could not be confirmed in the dynamic analysis. Permissions defined in the `AndroidManifest.xml` do not cover personal data, making it impossible to detect potential personal data transmission in the static analysis. Additionally, no flow of personal data was identified during app operation. This could be because the data is encoded or encrypted, making bypassing the applied analysis methods impossible. Therefore, no definitive conclusion could be drawn regarding the conformity of the personal data requested in the privacy policies compared to the actual app execution.
- *Consent Dialogs and Dark Patterns:* The study demonstrated that personal data, particularly the Advertising ID, was identified even before consent in 13 of the examined apps. This finding raises questions about the definition and protection of personal data. Furthermore, privacy policy consent dialogs were examined for dark patterns, revealing their

presence in each examined app. These dark patterns, primarily forms of Forced Action and Obfuscation, suggest that users are often coerced into agreeing without sufficient information.

Discussion and Limitations

This study employed an interdisciplinary approach to examine the privacy policies and actual data transmission practices within health & fitness apps. By integrating insights from information security, human-computer interaction, and regulation, the research aimed to comprehensively understand the complex dynamics of protecting user privacy in mobile and ubiquitous digital health applications.

Our analysis unearthed significant gaps between the information provided in privacy policies and the actual practices regarding the disclosure of third countries and data recipients. Notably, 65% of privacy policies opted to categorize countries rather than explicitly naming them, leaving users uncertain where their data might end up. This ambiguity presents a challenge for users trying to pinpoint the destination of their data. While the legality of categorizing third countries remains a topic of debate (Wagner, 2018; Juliussen et al., 2023), it is evident that clearer data transfer to third countries is imperative for enhancing transparency and user understanding (Minssen et al., 2020).

Similarly, privacy policies often lumped data recipients into broad categories such as “Advertising Partners” and “Service Partners,” obscuring the specific entities involved. Despite an 85% alignment with the technical analysis concerning data recipients, the lack of specificity erodes user trust and transparency. Furthermore, while all apps transmitted data to the USA, only 75% of privacy policies explicitly acknowledged this, often resorting to vague terms like “operating offices,” further complicating users’ comprehension of data handling practices. Thus, there is a critical need for consistent standards or guidelines to ensure more explicit disclosure and more precise identification in privacy policies. Such measures are essential for empowering users to make informed decisions about their data, ultimately fostering trust in the digital health ecosystem (LaMonica et al., 2021).

The dynamic analysis results unveiled how apps operated before users consented to their privacy policies, particularly concerning the transmission of personal data to third parties. Notably, the Google Advertising ID emerged as a prevalent piece of personal information. Similar findings were also noted by Claesson and Bjørstad (2020), which identified additional transmissions of personal data such as GPS location, gender, and age to third parties. Grundy et al. (2019) found comparable results in the medical sector, where personal

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

data like birth dates and gender were transmitted. While our study revealed the transmission of user data such as time zone, hardware specifics, local IP address, and Advertising ID without explicit consent to privacy policies, it prompts a debate on whether such information aligns with the criteria for personal data outlined in the GDPR. The complexity of this matter stems from multiple factors contributing to the uncertainty surrounding its classification (Borgesius, 2017). Moreover, we did not observe any other personal data transmission. This absence raises several potential arguments as well. One argument is that personal data might initially be sent to the app operator’s main servers before being transferred to third parties, a process not accounted for in the study’s design. Additionally, data could be further encrypted or encoded; indeed, most transmissions to Google were encoded and inaccessible. Nonetheless, the discovery of the Google Advertising ID in 65% of the examined apps before consent suggests a need for a clearer definition of what constitutes personal data. Although GDPR specifies this, a lack of unified implementation in practice remains (Finck and Pallas, 2020).

Our study took another angle, aiming to explore the prevalence of dark patterns within consent agreements of fitness and health apps. Our goal was to illuminate issues of user coercion and transparency. Throughout our analysis, we encountered various forms of manipulation. Misdirection stood out as the most prevalent, utilizing design elements to conceal crucial information. Additionally, we observed widespread use of forced action tactics and obfuscations, often leading users to consent to data collection without fully grasping the consequences. Moreover, certain apps compelled users to create accounts, enforcing registration to access fundamental features. These findings resonate with existing research, such as Di Geronimo et al. (2020), which similarly highlighted the pervasiveness of dark patterns in app consent agreements. These practices undermine the principle of informed consent and prioritize data collection at the expense of user rights and transparency. Consequently, users may unwittingly agree to terms they do not fully understand, raising significant privacy concerns (Luguri and Strahilevitz, 2021).

The analysis of privacy policies for 20 health and fitness apps revealed significant gaps in transparency and detail, especially when compared to static and dynamic analysis results. The privacy policies often failed to provide specific information about data transfers to third countries, with many using vague terms like “operating offices” instead of naming particular countries. For example, while all apps sent data to the USA, only 75% of the policies mentioned this explicitly, and 40% of data communications to Ireland were not clearly reflected in the policies. The privacy policies also

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

broadly categorized data recipients, such as “Service Partners” or “Analytics Partners,” which obscures the specific entities involved. This contrasts with the detailed findings from static analysis, which identified numerous instances of communication with advertising companies and other services. Additionally, the policies did not adequately detail the types of personal data collected, as dynamic analysis revealed the transmission of data like Google Advertising IDs without user consent, highlighting a lack of transparency in actual data practices. Furthermore, dark patterns in consent dialogs, such as misdirection and forced action, were prevalent but not addressed in the privacy policies. This manipulation further diminishes user control and informed consent, contravening data protection principles. Overall, privacy policies lacked the specificity and transparency necessary for users to understand and control their data usage. These deficiencies suggest a need for stricter regulatory oversight to ensure that privacy policies accurately reflect actual data practices and comply with data protection laws (Zaeem and Barber, 2020).

Our investigation and experimental setup revealed numerous challenges and limitations that demanded careful consideration. We primarily relied on MobSF for static analysis, as alternative tools were scarce. Although the JADX⁸ decompiler was available, its cryptic output made it impractical, prompting us to dismiss this option. In dynamic analysis, rooting the mobile device was necessary, albeit risky. While initial considerations included device emulation through platforms like the Android Studio Simulator and Genymotion⁹, their unreliability led us to favor physical devices despite MobSF offering dynamic analysis options for both. Moreover, some apps could detect rooted or emulated devices, potentially altering their behavior. Despite installing a Magisk module to conceal root access, detection remained possible, compromising data transmission reliability.

The identification of personal data beyond the Google Advertising ID posed challenges due to encoded transmissions, particularly to Google servers, impeding our assessment of personal data handling during technical analysis. During the experiment setup, isolating app activities from background system transmissions proved daunting despite monitoring outgoing network activities with Burp Suite. While efforts were made to minimize background activity influence, we could not guarantee distortion-free results. These challenges underscore the intricacies of mobile app analysis, highlighting the critical importance of meticulous experimental setups and analysis techniques.

⁸<https://github.com/skylot/jadx>

⁹<https://www.genymotion.com/>

Acknowledgments

This section is based on the master's thesis:

Alexander Herbst. 2024. *Dark Patterns and Privacy Policy Compliance in (Health & Fitness) Apps - An Analytical Study*. Unpublished master's thesis. University of Bremen.

My contribution to this work: Conceptualization, data curation, formal analysis, investigation, methodology, project administration, resources, partial software development, supervision, validation, and visualization.

Additional advisors: I would also like to acknowledge the contributions of Merle Freye and Matthias Kohn, whose guidance and expertise supported the development of this thesis.

4.1.3 Key Insights of the Imperative for a Paradigm Shift

Study 10: Security Literacy and Behavioral Intentions

This study investigated users' comprehension of privacy and security terms related to smart home technology and the impact of these terms on behavioral intentions. The findings revealed a broad spectrum of understanding among participants, with a clear gap in deep technical knowledge. Terms like "Authentication," "Password," and "Privacy Policy" were generally understood, while more complex terms such as "Access Control," "Pseudonymization," and "Communication Protocol" were less well understood.

This gap in comprehension is critical because it can lead to misconceptions about security measures and privacy implications. Users' partial understanding can result in inadequate privacy practices and a false sense of security. The study also found that higher privacy concerns were associated with lower trust in data handling entities, which in turn influenced users' behavioral intentions. Privacy concerns significantly predicted security behavioral intentions, highlighting the need for better education and clearer information to build trust and empower users to make informed decisions.

Study 11: Data Protection Compliance in Health Apps

This study examined the privacy policies and actual data transmission practices of health & fitness apps. The study found significant gaps between the information provided in privacy policies and the actual practices regarding data transmission to third countries and recipients. Many privacy policies used vague categories, leaving users uncertain about where their data might end up. Additionally, the dynamic analysis revealed that many apps transmitted personal data, such as Google Advertising IDs, without user consent, raising significant privacy concerns.

The study also highlighted the prevalence of dark patterns in consent dialogs, which manipulate users into making decisions without fully understanding the consequences. These practices undermine informed consent and compromise user autonomy. The discrepancies between privacy policies and actual practices, combined with manipulative consent dialogs, underscore the need for clearer, more transparent information to help users navigate their privacy rights effectively.

The Imperative for a Paradigm Shift

The findings from Studies 10 and 11 underscore the critical need for a paradigm shift towards empowering users to navigate their privacy rights effectively within mobile and ubiquitous applications. This shift is essential from the perspectives of users, developers, and legislators. Each stakeholder

4.1. THE IMPERATIVE FOR A PARADIGM SHIFT

group plays a unique role in fostering a privacy-conscious and secure digital ecosystem. From the user's perspective, receiving clear, transparent, and accessible information builds trust and enhances self-efficacy, enabling informed decision-making. From the developer's perspective, designing ethical, user-friendly interfaces and providing accurate privacy policies align with best practices in the Fogg Behavior Model and self-efficacy theory, fostering user confidence and compliance. Lastly, from the legislator's perspective, enforcing regulations that ensure transparency and guard against manipulative practices is essential for creating a secure digital environment. By integrating the Fogg Behavior Model and self-efficacy theory, this paradigm shift can be effectively implemented, ensuring that users are not only informed but also confident in navigating their privacy rights. This approach is essential for fostering a more privacy-conscious and secure digital ecosystem, addressing our fourth research question in this dissertation comprehensively.

RQ4

Do users understand the basic components of security, and do apps implement transparent mechanisms to support this understanding?

By addressing Research Question 4, this dissertation examines the challenges users face in making informed privacy and security decisions stemming from a lack of deep technical knowledge and the presence of unethical design practices. This question also focuses on whether users understand relevant security terms and interface elements, which are essential for confidently navigating complex security tasks.

4.2 Informed Behavior Using Interactive Interfaces

In the last two studies, we recognized the necessity of a paradigm shift to empower users with an understanding of their security practices and the ability to make informed decisions. Interactive experiences, such as Augmented Reality, have been shown to effectively transfer knowledge across various domains by overlaying virtual information onto the physical world, enhancing learning through visual engagement. In smart home contexts, where security configurations can be complex, AR offers a promising avenue to simplify these concepts, making them more accessible and actionable. Consequently, this section explores how AR interactions can enhance user empowerment, facilitate procedural knowledge, and improve the management of security practices. Additionally, a comparative study with classic 2D interfaces assesses their impact on users' informed behavior.

The first study investigates the integration of AR technology into smart home environments to enhance user understanding and perception of security measures. It examines whether visual elements, such as data flow lines combined with textual and iconic indicators, can improve users' comprehension of the security status of their smart home devices. The study also considers how users' prior technological experience and security concerns affect their interaction with these AR interfaces.

The second study builds upon the findings of the first, focusing on the tasks and challenges smart home users face beyond the initial setup. While visual representations can enhance security perceptions, practical challenges remain in managing interconnected devices. These challenges include ensuring data security and privacy as devices exchange information with each other and external servers. This study provides a holistic view of user motivation and ability in smart home environments, emphasizing the need for intuitive interfaces and robust security measures.

The third study replicates the second, with the prototype and context redeveloped to ensure consistency. This replication aims to test the same questions and goals, yielding additional insights into the effectiveness and reliability of the findings in varied conditions.

Together, these studies highlight the role of interactive interfaces in empowering users through improved understanding and proactive decision-making in smart home security. By leveraging technologies like AR to make security concepts more accessible, we aim to contribute to developing more intuitive and secure smart home environments where users can confidently manage and protect their digital spaces.

4.2.1 Study 12: AR Visualization Raises Security Perception

Introduction and Background

In the rapidly evolving world of smart home technology, user interface designs are crucial in shaping usability, enhancing user experience, and guiding interaction dynamics (Pyae and Joelsson, 2018; Chalhoub et al., 2020). These interfaces serve as the primary means through which individuals interact with and control various aspects of their smart home systems. Despite their significance, research shows that users often overlook privacy and security concerns when using smart home technologies (Zeng et al., 2017). This oversight underscores the need to integrate solutions into smart home devices that enhance data security, providing users with greater awareness and control over their personal information (Tabassum et al., 2019). Moreover, improving transparency, exploring ways to incorporate clear visual indicators, and educating users about their controls during device interactions are essential to building a solid foundation of trust and promoting the widespread acceptance of smart home technology (Zimmermann et al., 2019).

Transparency is generally defined as removing secrets or barriers to allow clear observation and examination (Meijer, 2009). It involves making information and processes visible and accessible to the public or those affected. Regarding human-computer interactions, transparency is necessary in fostering shared intent and awareness. It involves providing relevant information without overwhelming users (Lyons and Havig, 2014). The level of transparency in the design and implementation of user interfaces enables end-users to understand the workings of a desired system, consequently building their trust in technology (Kizilcec, 2016). Displaying security mechanisms, like encryption processes, enhances user trust and understanding while potentially introducing challenges in usability due to increased complexity (Distler et al., 2019). On the other hand, the absence of transparent privacy controls poses a significant barrier to adopting smart devices such as smart speakers (Lau et al., 2018). Language selection also profoundly shapes users' perceptions, particularly among non-experts, where terms like “encrypt” and “secure” convey a stronger sense of security than alternatives (Distler et al., 2020). Following this, incorporating indicators such as a green lock icon alongside these terms has proven to be the most effective method for conveying security to users (Felt et al., 2016). Studies indicate that homeowners increasingly seek greater transparency and control over their data usage within smart home systems (Tabassum et al., 2019). Data transparency and control are also relevant for bystanders in smart homes (Yao et al., 2019).

In recent years, integrating augmented reality and the Internet of Things

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

has reshaped interactions within smart home systems (Jo and Kim, 2019). AR applications represent an innovative interface design tailored for smart home environments, enabling personalized user experiences and interaction within the home (Oh et al., 2009). AR interfaces enhance users' experiences managing and controlling smart home devices (Ullah et al., 2012), offering users a deeper understanding of their surroundings (Seo et al., 2016). Essentially, augmented reality is a technology that seamlessly integrates virtual content with the real world, offering users an interactive experience and enhancing users' perception in real time (Caboni and Hagberg, 2019). AR systems blend elements from the physical and digital realms, allowing users to interact with virtual objects or information as if they were part of their immediate environment (Billinghurst et al., 2015). Augmented reality offers diverse instructional approaches like game-based learning, place-based learning, and participatory simulations (Squire and Klopfer, 2007; Squire and Jan, 2007; Rosenbaum et al., 2007). These methods engage learners through roles, physical interactions, and task designs, promoting skill acquisition, enhancing spatial abilities, and increasing motivation (Klopfer, 2008; Sotiriou and Bogner, 2008; Baragash et al., 2022). AR also addresses learning challenges by visualizing abstract concepts and providing tailored experiences for special needs (Kerawalla et al., 2006), indicating its transformative potential in education (Schmidt and Tang, 2020). Furthermore, research has demonstrated the positive effect of AR transparency in helping users increase their privacy awareness and make appropriate privacy decisions. Bermejo Fernandez et al. (2021) introduced the Privacy Augmented Reality Assistant (PARA), which enables users to visualize data disclosure and control privacy settings on compatible devices. Their findings notably influenced users' perceptions of privacy risks associated with smart devices. Building on this research, Kaiser et al. (2022) investigated the role of AR in facilitating informed decision-making during shopping activities. They highlighted the potential of AR visualizations to showcase privacy details during shopping experiences. In parallel to these investigations, research has investigated the impact of AR icons on privacy awareness and decision-making within smart environments. Preliminary findings from a study using AR technology revealed significant changes in user awareness, particularly highlighting the impact of AR icons and interfaces (Knutzen et al., 2021). Participants expressed increased discomfort and awareness regarding the data collected by smart devices, emphasizing the importance of educating users about data flows and privacy risks. Additionally, concerns were raised about manufacturers' intentions and the loss of anonymity, suggesting a growing need for transparent privacy policies and user education initiatives.

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

Furthermore, the study highlighted the potential risk of overtrust, where users may rely too much on manufacturers' assurances of privacy protection, potentially leading to a false sense of security.

The potential of AR extends beyond user experience and training. Its role in enhancing smart home security through the overlay of real-time security alerts and the visualization of network activity in the physical space proves crucial (Böhm et al., 2021). This capability allows users to easily identify and respond to digital vulnerabilities, fostering a more secure smart home environment. Despite the promise of these applications, it remains unclear how AR can create transparent security configurations in smart homes and influence users' perceptions of security, as research in this area is currently lacking. To address this gap, we explore the integration of augmented reality into smart home technology and assess how visual elements such as data flow lines, alongside textual and iconic indicators, enhance the user experience by improving the comprehension of security measures within smart home environments. This study aims to determine *RQ1) whether the inclusion of these AR features can aid users in better understanding the security status of their smart home devices, potentially leading to increased trust and engagement with these technologies and influencing users' comprehension of network security statuses in smart home environments*. Additionally, we seek to investigate *RQ2) how users' previous technological experiences and security concerns influence their interaction with and perceptions of these advanced interfaces*.

We developed an Android-compatible application designed to overlay virtual representations of a Google Nest Cam and a Google Home onto the physical world, connecting these to a virtual router. The prototype includes two versions, *Linker* and *Connector*, which follow the same functional flow but differ in their AR visual presentation. Both versions display the security status of the connected devices using text, along with green locks for secure connections and red warning icons for insecure ones. The *Connector* version enhances this with a color-coded line that visually represents the security status of the connection paths between devices. In contrast, the *Linker* version lacks this visual element, offering a more abstract representation of connectivity. Our approach adopts the recommendation proposed by researchers, which advocates for easy-to-understand user interfaces to control information flow concepts in smart connected homes (Bugeja et al., 2016; Henze et al., 2016).

Our study's findings reveal that augmented reality interfaces, specifically the visualization of data flow lines, significantly enhance user security perception in smart home settings by improving clarity and understanding of device

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

interconnectivity. Users responded favorably to the *Connector* version, which includes visual lines indicating the security status of connections, suggesting that such visual cues greatly aid in comprehension and increase the perceived security of the system. This enhancement was particularly notable among men, who valued the explicit visual representation of data flows more than women. The contributions of this research are substantial, providing valuable insights for the development of AR technology in smart home applications. It emphasizes the importance of visual elements in user interfaces for enhancing the functionality and security perceptions of smart home systems.

Prototype Description

Concept We have developed a prototype to visually illustrate the interconnection between two virtual smart home devices to a virtual router, namely a Google Nest Cam and a Google Home. These devices were chosen because they represent common, widely-used smart home products that highlight diverse functionalities such as security monitoring and voice control, which are enabled through networked connectivity in a smart home environment (Ammari et al., 2019; Chakraborty et al., 2023). We opted for virtual representations instead of real devices because our focus is on demonstrating the network architecture and data flow rather than the actual functionalities of the devices. This approach allows for a more precise and controlled presentation of the interconnections without being distracted by the physical setup or the specific behaviors of the actual devices. Augmented reality technology was implemented to superimpose virtual representations of devices onto the physical world. Since the prototype is meant to feel like a typical smart home app, the Google Home app’s setup process served as a reference. The prototype has two versions with the same flow, including a user registration page, logging in, selecting the room where the desired smart home device is located, and connecting the device to the router (see Figure 4.20). The applications differed only in the presentation of the connections in AR. The version with the connecting line is called *Connector*, and the one without the connecting line is *Linker*. The prototype was developed in Unity for Android devices.

Design Users initiate access to the prototype by authenticating with the provided credentials. Once logged in, they select a preferred room and add the router, the Google Nest Cam, and Google Home into their simulated smart home environment. Virtual devices can then be strategically positioned on an actual table within an augmented-reality scene. The placement process is supported by the AR Foundation framework, which employs plane detection abilities to identify optimal horizontal surfaces for object placement in Unity.

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

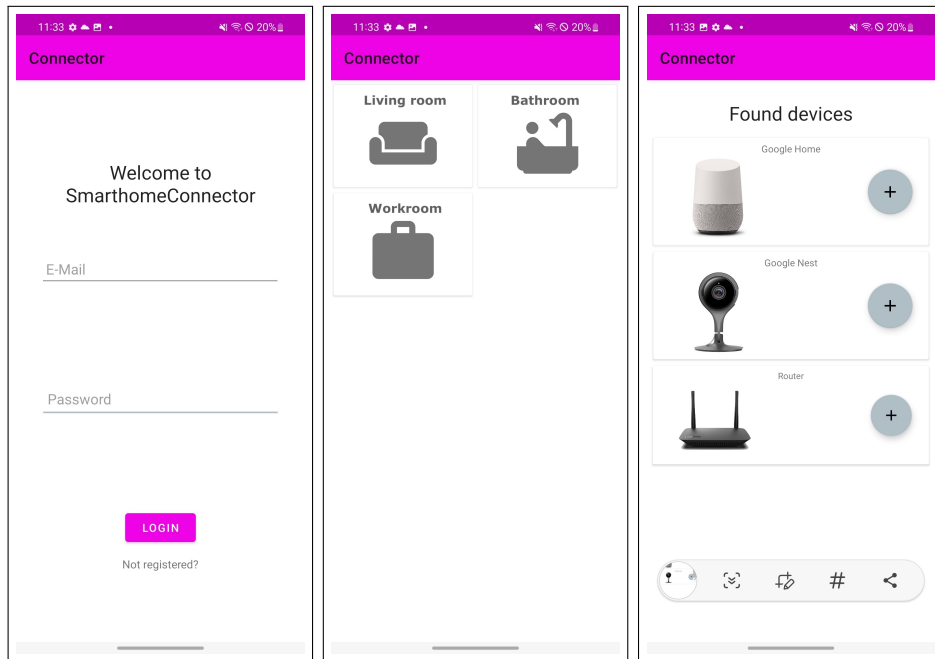


Figure 4.20: A user’s journey starts through three stages. On the left, the user registers by entering provided data. In the middle, they select their preferred room. On the right, the user can place devices on a table by tapping the plus buttons and utilizing the AR function.

Once a suitable surface is identified, the system facilitates precise alignment and instantiation of virtual objects on these planes.

A pop-up window appears when an individual device is selected, providing contextual information and interaction options. In both variants, establishing a connection between each device and the router requires the user to press the “connect” button. Upon doing so, a notification appears stating that the connection is being established, which subsequently updates to “connection established.” This action in the *Connector* version results in a visible colored line, whereas in the *Linker* version, no line appears (see Figure 4.21). In our scenario, we have assumed that the connection of the IP camera is unsecured while that of the voice assistant is secure.

Both prototypes use intuitive icons, a green lock for secure connections, and a red warning for insecure, supplemented by explanatory text. This approach, which incorporates insights from existing studies (Felt et al., 2016; Distler et al., 2020; Prange et al., 2021), clearly communicates the security status of each connection. The *Connector* version emphasizes security statuses with green and red lines indicating secure and unsecured connections, respectively. This visual distinction is absent in the *Linker* version.

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

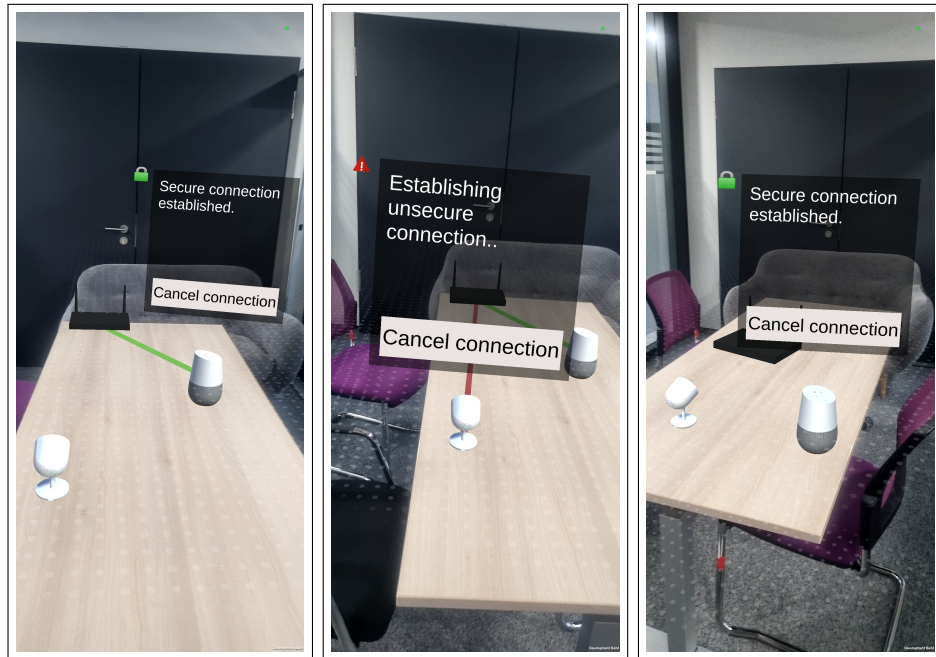


Figure 4.21: The *Connector* version (left and middle) demonstrates two distinct levels of connection security. On the left, a user establishes a secure connection between the voice assistant and the router, indicated by a green line and lock icon, with a pop-up confirming security. In the middle, an IP camera connection to the router displays a red line and warning icon, highlighting an insecure connection with a corresponding pop-up. On the right, the *Linker* version shows the voice assistant connected to the router without the green line visual, yet a lock icon and pop-up still provide the connection's security status.

User Evaluation

Study Design A within-subject design lab study was conducted to evaluate users' perceptions of the developed AR app designed to simulate the setup of smart home devices. The study involved testing two prototype versions of the app. The conditions were counterbalanced using Latin squares to mitigate learning effects, ensuring an equal number of responses for each questionnaire. The experiment sessions lasted approximately 45 to 60 minutes.

Materials The data collection process involved standard questionnaires and tailored items to gather participant answers.

- *Advanced User Experience Assessment:* The UEQ+ is an enhanced version of the User Experience Questionnaire (UEQ) (Laugwitz et al., 2008), offering an expanded set of scales to assess user experience comprehensively. In our study, we carefully selected items from the UEQ+

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

that align with our research approach, focusing on scales highly relevant to our investigation. The chosen scales encompass attractiveness, efficiency, intuitive use, transparency, reliability, usefulness, stimulation, and trust. Each scale within the UEQ+ comprises four pairs of terms, allowing participants to rate their perception using a seven-point Likert scale.

- *Affinity for Technology Interaction:* Considering the importance of Affinity for Technology Interaction (ATI) in user-centered design and human-computer interaction, the 9-item ATI questionnaire was employed to measure participants' affinity for technology interaction, as described in Section 4.1.1 on page 207.
- *Privacy Concerns:* In this study, the Internet Users' Information Privacy Concerns (IUIPC) questionnaire was used to evaluate users' privacy concerns, focusing on three key dimensions: control, awareness, and collection, as well as context-specific factors, including trusting beliefs and risk beliefs, as described in Section 4.1.1 on page 208.
- *Prototype Feedback:* The self-designed questions included in the study aimed to gather participant feedback on the two prototypes. Participants are asked to provide their responses in text format to evaluate the use of such security visualizations, indicate their preferred prototype, provide detailed reasons for their choice, share specific likes and dislikes about each presentation, and offer constructive suggestions for improvement. By encouraging participants to provide textual responses, the questionnaire facilitates in-depth qualitative feedback collection to assess participant perceptions about each prototype.
- *Baseline Insight:* The self-designed questions cover various aspects of participants' technological engagement and concerns, all structured around a 5-point Likert scale. The first inquiry explores participants' experiences with AR, while the second focuses on their smartphone knowledge and expertise with these widely used devices. Afterward, participants are asked about using smart home technologies to assess their familiarity and engagement. The subsequent question addresses participants' understanding of smart home data protection and security measures, while the next evaluates their perceived importance of data protection and security in smart home device usage. Participants then rate the extent of their security concerns related to smart home devices. Finally, the last question assesses participants' comprehension of secure

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

connections, specifically their awareness of HTTPS abbreviations and their ability to provide descriptions.

Statistical Analysis Statistical methods were used to analyze the data collected with the questionnaires. Specifically, paired t-tests (Student, 1908) were performed to examine significant differences in UEQ+ scores between the two conditions, while unpaired t-tests examined gender differences across prototype versions. Additionally, we conducted a repeated measures ANOVA (Fisher, 1970) to examine the effects of interface type and individual factors (e.g., gender, ATI, IUIPC) on KPI scores, assessing both main and interaction effects. All tests were conducted with an alpha level of 0.05. The ATI score was calculated and analyzed by gender, and IUIPC mean scores were calculated for each category.

Procedure The study was conducted anonymously, and the participants gave informed consent. The study director then welcomed the participants and provided an introduction to the app. The participants were briefed about the application's functionalities and how to interact with it. They were also given specific information regarding their registration in the application, which was provided beforehand by the experimenter in an attempt to keep anonymity. During the study, the participants were given step-by-step tasks to complete. These tasks included registering in the application, logging in, navigating to choose the desired room, adding Google Nest Cam and Google Home, and connecting the devices to the router. Upon finishing each prototype version, participants completed the UEQ+ questionnaires. Subsequently, having completed both versions and the associated UEQ+ questionnaires, participants were prompted to respond to a series of inquiries encompassing ATI and IUIPC assessments, along with their opinions on the two representations. They were asked which representation was better and why. In the end, participants answered baseline insight and demographic questions.

Participants The study involved recruiting 33 participants, including 16 men and 16 women, and one did not provide gender information. The respondents ranged from 19 to 42 years, with an average of 28.42 ($SD = 5.03$). Participation was voluntary, and no compensation was offered to respondents. The acquisition was made through various methods, including mailing lists, social networks, word-of-mouth, and personal contacts.

Empirical Findings

Baseline Insight We initiated the data collection process by administering a preliminary participant survey. This survey was designed to gather essential

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

background information and establish a baseline for our study.

- *AR Experience:* Among the 33 participants, 26 individuals were already familiar with AR. Specifically, 16 participants reported gaining AR experience through Pokémon Go, while seven acquired it through university projects. Additionally, two participants had AR experience in a professional context, two utilized AR for room measurements, and two had experience with AR in navigation apps. Furthermore, five participants mentioned being familiar with AR without direct experience, while two stated that they had no prior experience.
- *Smartphone Experience:* The participants demonstrated a sufficient level of knowledge of smartphone utilization. Merely two respondents indicated that they had a basic understanding of smartphones. In contrast, the following four participants described their backgrounds as average. A substantial number of thirteen participants expressed possessing advanced knowledge, while fourteen considered themselves experts in smartphone usage.
- *Smart Home Usage:* Among the participants, thirty owned at least one smart home device. The experience with these devices varies significantly. Ten participants have one year of experience, fifteen have between two and four years of experience, and eight have over four years of experience.
- *Smart Home Security Understanding:* Participants provided varying ratings for their understanding of smart home data protection and security. Three participants indicated that they did not possess any understanding in this area. In contrast, eight participants rated their understanding as basic, while nine considered it average. Additionally, ten participants classified their understanding as advanced, and three described their knowledge as expert-level regarding smart home data protection and security.
- *Smart Home Data Protection Importance:* When asked to evaluate the significance of data protection and security in using their smart home devices, three respondents indicated that it held no importance to them. Eight participants expressed it as relatively unimportant, while nine participants considered it neither important nor unimportant. In contrast, nine participants rated it as rather important, and four deemed it very important.

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

- *Smart Home Security Concerns:* As part of our exploration, we inquired about participants' security concerns related to smart home devices. Among the respondents, three reported having no concerns, while two indicated having relatively few concerns. Eight participants expressed having neither few nor strong concerns, while twelve had rather more concerns. Additionally, eight participants conveyed significant levels of concern regarding smart home device security.
- *HTTPS Comprehension:* Lastly, participants' comprehension of secure connections was evaluated by questioning their familiarity with the abbreviation HTTPS and requesting them to provide a description. Of the respondents, twenty-four expressed confidence in their knowledge of the abbreviation, while nine indicated they were unfamiliar with it. However, when asked to explain HTTPS, six participants either provided incorrect responses or failed to mention the encrypted connection. On the other hand, seventeen respondents demonstrated a precise understanding of HTTPS functions, even if the abbreviation was not explicitly explained.

ATI The ATI questionnaire demonstrated a mean score of 4.24 ($SD = 0.89$), indicating a generally positive attitude toward technology. The questionnaire demonstrated good reliability with a Cronbach's α coefficient of 0.82.

IUIPC The overall mean score of the IUIPC questionnaire (Control, Awareness, and Collection) for participants was 5.68 ($SD = 0.81$) with a Cronbach's α coefficient of 0.80. The IUIPC dimensions and context-specific factors (Trusting Beliefs and Risk Beliefs) scores are collected in Table 4.7.

Table 4.7: IUIPC Dimensions and Context-Specific Factors

| | Cronbach's α | Mean | Std. Deviation |
|------------------|---------------------|------|----------------|
| Control | 0.56 | 5.78 | 1.34 |
| Awareness | 0.66 | 6.19 | 1.28 |
| Collection | 0.88 | 5.08 | 1.75 |
| Trusting Beliefs | 0.86 | 2.78 | 1.48 |
| Risk Beliefs | 0.80 | 4.19 | 1.65 |

A Pearson correlation analysis was conducted to examine the linear relationships between the mean IUIPC score and three variables: Risk Beliefs, Trusting Beliefs, and the Importance of Data Protection and Security. The results indicated a significant positive correlation between IUIPC and Risk Beliefs ($r(31) = 0.44, p = 0.0099$), and between IUIPC and the Importance

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

of Data Protection and Security ($r(31) = 0.52, p = 0.0019$). However, no significant correlation was observed between IUIPC and Trusting Beliefs. Table 4.8 displays all correlation coefficients among the variables analyzed.

Table 4.8: Correlations among Variables Related to Privacy Concerns

| Variable Pair | Pearson's r | p-value |
|-----------------------------------|-------------|---------|
| Awareness vs. IUIPC | 0.8065 | < .001 |
| Collection vs. IUIPC | 0.8107 | < .001 |
| Control vs. IUIPC | 0.5649 | < .001 |
| IUIPC vs. Trusting Beliefs | 0.0754 | 0.6767 |
| IUIPC vs. Risk Beliefs | 0.4424 | 0.0099 |
| IUIPC vs. Importance | 0.5212 | 0.0019 |
| Trusting Beliefs vs. Risk Beliefs | -0.3224 | 0.0673 |
| Trusting Beliefs vs. Importance | -0.0474 | 0.7933 |
| Risk Beliefs vs. Importance | 0.5348 | 0.0013 |

UEQ+ (*Linker & Connector*) The *Linker* representation achieved an overall user experience Key Performance Indicator (KPI) of 1.33 ($SD = 0.85$). Meanwhile, the *Connector* representation attained a higher user experience KPI of 1.66 ($SD = 0.67$). Table 4.9 shows the eight scales from the UEQ+ questionnaire for both versions. These scales include attractiveness, efficiency, perspicuity, dependability, intuitive use, usefulness, trust, and stimulation. For each scale, means, standard deviations, and confidence scores were calculated based on the mean scores of the respective items. Additionally, to maintain consistency with the reporting format of the original UEQ, the mean scores were transformed from a range of 1 – 7 to a range of –3 to +3.

Table 4.9: UEQ+ (*Linker & Connector*)

| | <i>Linker</i> | | | <i>Connector</i> | | |
|----------------|---------------|----------------|------------|------------------|----------------|------------|
| | Mean | Std. Deviation | Confidence | Mean | Std. Deviation | Confidence |
| Attractiveness | 0.92 | 1.39 | 0.47 | 1.42 | 1.26 | 0.43 |
| Efficiency | 1.63 | 1.45 | 0.49 | 1.89 | 1.26 | 0.43 |
| Perspicuity | 1.49 | 1.44 | 0.49 | 1.97 | 1.23 | 0.42 |
| Dependability | 1.32 | 1.42 | 0.48 | 1.87 | 1.07 | 0.36 |
| Intuitive Use | 1.66 | 1.40 | 0.48 | 2.06 | 1.03 | 0.35 |
| Usefulness | 1.14 | 1.33 | 0.45 | 1.39 | 1.26 | 0.43 |
| Trust | 0.91 | 1.81 | 0.62 | 0.98 | 1.76 | 0.60 |
| Stimulation | 1.27 | 1.47 | 0.50 | 1.27 | 1.44 | 0.49 |

UEQ+ (Comparison) We applied a paired t-test to analyze KPI scales of the UEQ+ questionnaires. The results revealed a significant difference ($t(32) = 3.51, p = 0.001, Cohen'sd = 0.61$) in KPI values between the *Linker*

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

prototype ($M = 1.33$, $SD = 0.85$) and the *Connector* prototype ($M = 1.66$, $SD = 0.67$). Table 4.10 shows paired t-test results for UEQ+ subscales.

Table 4.10: UEQ+ Paired Samples T-Test

| | t | df | p | Cohen's d |
|----------------|-------|----|-------|-----------|
| Attractiveness | -3.59 | 32 | 0.001 | -0.63 |
| Efficiency | -1.58 | 32 | 0.124 | -0.28 |
| Perspicuity | -3.01 | 32 | 0.005 | -0.52 |
| Dependability | -3.05 | 32 | 0.005 | -0.53 |
| Intuitive Use | -2.20 | 32 | 0.035 | -0.38 |
| Usefulness | -1.63 | 32 | 0.112 | -0.28 |
| Trust | -0.58 | 32 | 0.569 | -0.10 |
| Stimulation | -0.04 | 32 | 0.970 | -0.007 |

Significant changes were observed between the two prototypes in the Attractiveness, Perspicuity, Dependability, and Intuitive Use dimensions. These results highlight meaningful differences in user perceptions of these aspects, as depicted in Figure 4.22.

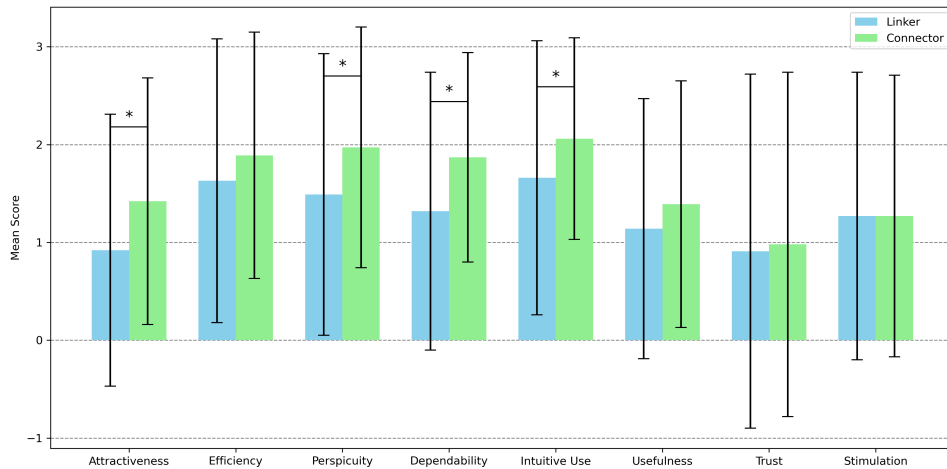


Figure 4.22: Comparison of UEQ+ subscales for *Linker* and *Connector*

Gender Differences Through our data analysis, we uncovered notable variations between men and women in their responses, which prompted us to delve deeper into this aspect. Nearly all participants identified themselves as either men or women, with only one choosing not to disclose their gender. Given this, our gender-focused analysis is limited to men and women, as the dataset does not include enough representation from non-binary individuals to allow meaningful comparisons. We recognize this limitation but aim to

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

provide clear insights based on the available data, emphasizing transparency in reporting the demographic context and associated findings.

- *Baseline Insight:* We chose the Mann-Whitney U test as a statistical analysis method due to the non-normal distribution of the baseline insight data (Shapiro-Wilk test p-values < 0.05). The results revealed no gender disparities in smartphone knowledge, comprehension of smart home privacy and security, and security concerns regarding smart home devices ($p > 0.05$). However, men ($M = 4.25$, $SD = 1$) displayed a significantly higher score regarding the importance of data protection and security for their smart home devices ($Z = 2.40$, $U = 189.5$, $p = 0.016$) than women ($M = 3.38$, $SD = 1.03$). Concerning understanding of HTTPS, approximately half of the women surveyed expressed unfamiliarity with the HTTPS abbreviation ($Z = -2.68$, $U = 72$, $p = 0.007$).
- *ATI:* The ATI scale was assessed separately for women and men, and the scale's internal consistency was evaluated using Cronbach's α coefficient. The ATI scale showed high internal consistency for women, with a Cronbach's α coefficient of 0.89. The mean score for women on the ATI scale was 3.91 ($SD = 1.58$), indicating a moderate affinity for technology interaction. The ATI scale exhibited lower internal consistency for men, with a Cronbach's α coefficient of 0.63. The mean score for men on the ATI scale was 4.56 ($SD = 1.16$), indicating a slightly higher level of affinity for technology interaction than women. To further investigate potential gender differences in the ATI scale, a Mann-Whitney U test was conducted due to the non-normal distribution of the men's data (Shapiro-Wilk test p-value = 0.013). The test results indicated no significant difference in affinity for technology interaction between women and men ($p > 0.05$).
- *IUIPC:* The IUIPC questionnaire (Control, Awareness, and Collection) demonstrated good internal consistency for both women and men, with Cronbach's α coefficients of 0.76 and 0.83, respectively. Among female participants, the mean score on the IUIPC scale was 5.76 ($SD = 0.75$), indicating a relatively high level of privacy concerns. Similarly, among male participants, the mean score on the IUIPC scale was 5.70 ($SD = 0.84$), suggesting a comparable level of privacy concerns to that of women (see Table 4.11). An independent t-test revealed no statistically significant difference in privacy concerns between women and men ($t(30) = 0.22$, $p > 0.05$).

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

We conducted a Pearson correlation coefficient analysis to assess the linear association between the mean score of the IUIPC and the importance of data protection and security measures among both women and men. The results demonstrated a positive correlation within each gender group, with a correlation coefficient of $r(14) = 0.63$, and a significance level of $p = 0.009$ for women, and a correlation coefficient of $r(14) = 0.53$, and a significance level of $p = 0.035$ for men. However, no significant correlation was observed between the mean score of the IUIPC and Risk Beliefs.

Table 4.11: IUIPC Scores and Privacy Concerns by Gender

| | | Mean | Std. Deviation |
|------------------|-------|------|----------------|
| Control | women | 6.04 | 0.95 |
| | men | 5.54 | 0.97 |
| Awareness | women | 6.12 | 0.98 |
| | men | 6.38 | 0.65 |
| Collection | women | 5.11 | 1.34 |
| | men | 5.17 | 1.56 |
| Trusting Beliefs | women | 3.03 | 1.29 |
| | men | 2.52 | 1.06 |
| Risk Beliefs | women | 4.13 | 1.58 |
| | men | 4.25 | 1.72 |

- *UEQ+ (Linker)*: The user experience of the Linker representation was evaluated separately for women and men. Women exhibited a KPI score of 1.79 ($SD = 0.88$), indicating a promising user experience. In contrast, men had a KPI score of 0.87 ($SD = 0.57$), reflecting a comparatively lower user experience. The normality assumption for the women's data was violated according to the Shapiro-Wilk test ($p = 0.022$). Therefore, a non-parametric Mann-Whitney U test was conducted. The results showed a significant difference in KPI scores between women and men ($Z = -3.15$, $U = 44$, $p = 0.002$), suggesting gender-related differences in user experience. Table 4.12 presents the results of the subscales of the UEQ+ questionnaire, highlighting significant variations between men and women across the dimensions of Attractiveness, Efficiency, Perspicuity, and Usefulness. Figure 4.23 provides a visual comparison of these results.

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

Table 4.12: Gender Comparison of UEQ+ Subscales with T-Test (*Linker*)

| | | Mean | Std. Deviation | t | df | p | Cohen's d |
|-----------------------|-------|------|----------------|-------|----|-------|-----------|
| Linker-Attractiveness | women | 0.63 | 0.13 | 2.96 | 30 | 0.006 | 1.05 |
| | men | 0.48 | 0.16 | | | | |
| Linker-Efficiency | women | 0.81 | 0.17 | 3.26 | 30 | 0.003 | 1.15 |
| | men | 0.64 | 0.13 | | | | |
| Linker-Perspicuity | women | 0.83 | 0.19 | 2.67 | 30 | 0.012 | 0.94 |
| | men | 0.66 | 0.16 | | | | |
| Linker-Dependability | women | 0.71 | 0.23 | 1.25 | 30 | 0.221 | 0.44 |
| | men | 0.61 | 0.21 | | | | |
| Linker-Intuitive Use | women | 0.75 | 0.25 | 0.55 | 30 | 0.585 | 0.19 |
| | men | 0.71 | 0.17 | | | | |
| Linker-Usefulness | women | 0.74 | 0.22 | 2.06 | 30 | 0.048 | 0.73 |
| | men | 0.59 | 0.21 | | | | |
| Linker-Trust | women | 0.72 | 0.30 | 1.22 | 30 | 0.232 | 0.43 |
| | men | 0.59 | 0.30 | | | | |
| Linker-Stimulation | women | 0.59 | 0.22 | -0.05 | 30 | 0.963 | -0.02 |
| | men | 0.59 | 0.23 | | | | |

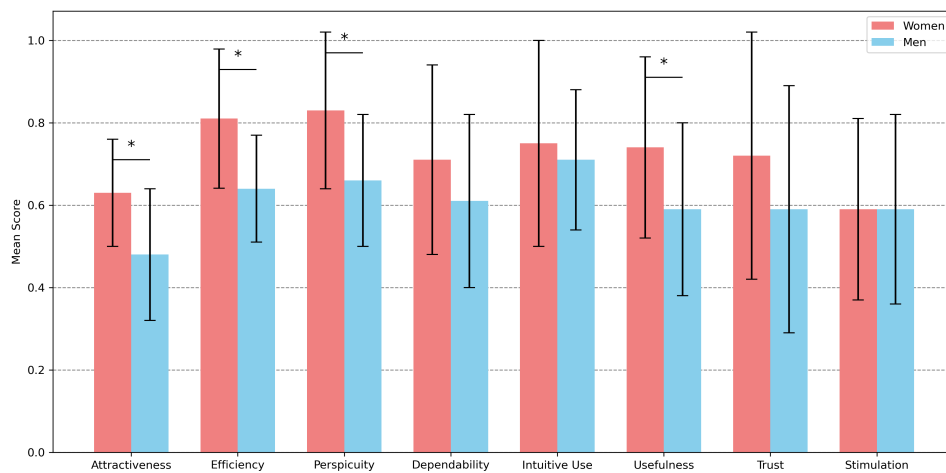


Figure 4.23: Gender Comparison of UEQ+ subscales (*Linker*).

- *UEQ+ (Connector)*: We analyzed genders to assess users' experiences with the *Connector's* representation. Women revealed a good user experience, with a KPI score of 1.95 ($SD = 0.71$). In contrast, men had a relatively lower user experience, as indicated by a KPI score of 1.40 ($SD = 0.52$). The Shapiro-Wilk test was performed for both women ($p = 0.021$) and men ($p = 0.003$) to examine the normality of the data distribution. The results demonstrated violations of the normality assumption. Consequently, a non-parametric Mann-Whitney U test was employed. The test indicated a significant difference in KPI

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

scores between women and men ($Z = -2.81$, $U = 53$, $p = 0.005$), suggesting gender-related disparities in user experience. Regarding the subscales of UEQ+, the t-test analysis indicated that there was only a significant difference in the Perspicuity subscale between genders ($t(30) = 2.41$, $p = 0.02$, $Cohen'sd = 0.85$). Table 4.13 presents the means and standard deviations of the UEQ+ subscales.

Table 4.13: UEQ+ Subscales by Gender (*Connector*)

| | | Mean | Std. Deviation |
|--------------------------|-------|------|----------------|
| Connector-Attractiveness | women | 0.65 | 0.19 |
| | men | 0.55 | 0.17 |
| Connector-Efficiency | women | 0.85 | 0.16 |
| | men | 0.73 | 0.16 |
| Connector-Perspicuity | women | 0.88 | 0.22 |
| | men | 0.73 | 0.12 |
| Connector-Dependability | women | 0.77 | 0.17 |
| | men | 0.77 | 0.24 |
| Connector-Intuitive Use | women | 0.86 | 0.20 |
| | men | 0.83 | 0.30 |
| Connector-Usefulness | women | 0.70 | 0.21 |
| | men | 0.58 | 0.23 |
| Connector-Trust | women | 0.67 | 0.28 |
| | men | 0.63 | 0.36 |
| Connector-Stimulation | women | 0.56 | 0.27 |
| | men | 0.59 | 0.21 |

User Factors in Interface Interaction We conducted a repeated measures ANOVA to assess the effects of interface type and individual factors (gender, IUIPC, ATI, and the Importance of Data Protection and Security) on KPI scores. Unlike a paired t-test, this analysis also examines interactions between individual factors and interface type, allowing for a more comprehensive view of user differences. The within-subjects effects showed no significant main effect of interface type on KPI scores ($F(1, 27) = 2.14$, $p = 0.155$). However, a significant interaction was observed between the interface type and gender ($F(1, 27) = 4.60$, $p = 0.041$), indicating that responses to the interfaces varied by gender. Furthermore, the between-subjects effects revealed no significant main effects for individual factors:

- ATI ($F(1, 27) = 1.29$, $p = 0.266$)
- Importance of Data Protection and Security ($F(1, 27) = 0.47$, $p = 0.499$)

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

- IUIPC ($F(1, 27) = 0.86, p = 0.363$)
- Gender ($F(1, 27) = 3.17, p = 0.086$)

In summary, while interface type alone did not significantly affect KPI scores, the significant interaction between interface type and gender suggests differential engagement with the interfaces based on gender.

Prototype Feedback Specific questions provided respondents with choices or numerical values, while others allowed them to offer free-text responses. The free-text answers were assessed by grouping them based on their proximity to the content, enabling their quantification. The participants were initially asked: “What are your thoughts on a smart home vendor incorporating security indicators in their apps, including text, icons, and visual representation of the connection?” In analyzing the responses from 33 participants, several insights emerge across five distinct areas. First, there is broad approval of security features, with 10 participants expressing positive sentiments like “I find it sensible” and “I would highly support it.” Specific features such as icons, text, and color-coded lines were particularly favored, noted by 28 participants for their clarity and efficiency in conveying security status; responses like “Icons: Very good, Text: Good, Line: Very good” demonstrate appreciation for each element. However, about 7 participants suggested improvements, particularly advocating for more comprehensive information and including a button for detailed explanations. Further, 8 participants emphasized the importance of transparency and user-friendliness, highlighting the need for easily understandable security indicators, especially for less tech-savvy users. Lastly, the need for clarity and intuitiveness was a frequent theme, with several mentions of the desire for security features to avoid confusion and be more intuitive, as illustrated by concerns about unclear icons and the need for additional contextual information.

Participants were subsequently queried about their preferred version. Twenty-two participants leaned towards the *Connector* version, while two opted for the *Linker* version. Eight participants found both versions equally satisfactory, while one expressed dissatisfaction with both options. We asked them about the reasons for their preferences. Twenty-four participants mentioned that the lines helped in understanding. One participant mentioned, “The lines clarified which devices were connected and how.” Another participant said, “I found the visual representation provided by the lines intuitive.” Additionally, a participant stated, “The lines helped me quickly identify device connections.” Four participants felt the security indicators were adequate without the lines. For instance, one mentioned, “The text

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

and icons alone were enough for me to determine the connection status; the lines didn't add much value for me." One participant deemed the entire AR view unnecessary. Another participant admitted to confusion caused by the lines and misunderstanding the red color's significance. Three participants found both versions equally satisfactory.

Furthermore, we inquired with participants regarding both versions, asking, "What aspects did you appreciate and find lacking in the prototypes?" As for the connector version, approximately 17 respondents praised features such as colored lines, icons, and clear visual indicators like green locks, appreciating their contribution to user clarity and interface effectiveness. For instance, one participant stated, "The clarity in showing what connections were made was appreciated, pointing out the effectiveness of the interface in making transparent connections." The other one said, "The lines help to recognize that there are security problems. It is perhaps better if an insecure connection is prevented directly." Conversely, 16 of the feedback highlighted areas for improvement, including the perceived redundancy or confusion caused by some visual elements and interface design issues. For instance, some respondents found features like the red line confusing, initially mistaking it as a sign of a failed connection. In contrast, others criticized the small size of warning triangles and the clutter caused by unnecessary visual elements. Additional concerns included the excessive size of dialogue boxes on camera views, which obscured important content until the user adjusted the interface scale, and ambiguous text that needed to be more clearly differentiated between secure and insecure connections.

Concerning the *Linker* version, respondents frequently valued the interface's simplicity and overall effectiveness, recognizing these attributes for improving user interaction. For example, three respondents mentioned that they found the icons beneficial. However, several drawbacks were noted, such as missing lines and elements, highlighted 12 times by users expecting to see them, resulting in confusion and challenges in understanding how to engage with the system. Additionally, concerns about the small size of specific user interface components, highlighted by one participant, indicate that these elements were not adequately visible, potentially affecting usability.

The last question was about the improvements the participants would make if they could. Nine participants would have liked the opportunity to access more information, especially regarding the meaning of warnings or what precisely the red-colored line signifies. Four participants would have preferred a different color for the line instead of red, assuming that red meant the connection was not functioning at all. Two participants wished for an intermediate status during connection establishment. One

participant expressed a desire to be guided through the application via a wizard without exerting mental effort. Seven participants had no suggestions for improvement. Four participants wished they could recognize that the devices were clickable or have a call to action prompting them to click. Two participants would have preferred an outline around the dialogue box in the corresponding color instead of the line. One participant wished for more icons. One participant found the lines leading to the router confusing because the connection to the router, the secure part of their network, was not visible, while the connection to the cloud, which was problematic, needed to be more apparent. Two participants would have liked to see a reflection of the status (No connection, connection in progress, connection established) visually represented in the button's color, not just textually.

Discussion and Limitations

Our study explored the application of AR technology in smart home setups, focusing on how visualizing device connections influences user security perception. We created an Android-compatible app to overlay virtual smart home devices onto the real environment, connecting them to a virtual router. Using a within-subject design, we evaluated participants' responses to both versions: one without visual data flow lines (*Linker*) and one with (*Connector*).

The results of the baseline insight questions, ATI, and IUIPC questionnaires provide an overview of the participants' mental models. Most participants had some level of familiarity with AR technologies, primarily through casual or academic experiences. The distribution of AR experience suggests that while many participants were not experts, they were not entirely naive about AR technology either. This familiarity and experience imply a moderate willingness to engage with AR technologies in various contexts (Nikhashemi et al., 2021). The data shows a relatively high adoption of smart home technologies among the participants, with a spread across beginners to experienced users. This adoption and the variety in the duration of usage indicate a perceived ease of use and increasing integration of smart home technologies in daily lives (Nikou, 2019). Additionally, the high level of smartphone proficiency (with a majority describing their knowledge as advanced or expert) among participants suggests that they were technologically savvy. This high proficiency may also influence their interactions and expectations from other technology-based tools and systems, like AR and smart home devices (Mishra et al., 2021).

The understanding of smart home security among our participants ranges from no knowledge to expert levels. However, a majority report their understanding as between average and advanced, showing a reasonable awareness

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

of security issues that may influence their trust in and use of technology (Zeng et al., 2017). Further, the question about the importance of data protection and security measures in smart home usage elicited various views. Significantly, many participants regard data protection as crucial, underscoring a heightened awareness of privacy concerns that could shape their protective behaviors with technology (Tabassum et al., 2019). This awareness is critical as it aligns with their overall proficiency with technology and emphasizes the role of data protection in their acceptance and integration of smart home systems (Guhr et al., 2020).

The concerns about the security of smart homes vary, with many participants indicating moderate to significant concerns. However, while most claimed familiarity with the HTTPS abbreviation, there seems to be a gap between recognizing the term and comprehending its function. This indicates a divide between superficial knowledge and a deeper understanding of cyber security practices (Catal et al., 2023).

The positive ATI score implies a generally favorable attitude towards technology among the participants, complemented by good internal consistency of the questionnaire. The IUIPC results, showing higher mean scores in awareness and control but lower in trusting beliefs, suggest that while participants feel in control and are aware of privacy concerns, they may not necessarily trust service providers fully. In terms of correlation, it is noteworthy to clarify that the mean of the IUIPC scores represents participants' concerns regarding companies' handling of personal information. When these concerns increase, there is a corresponding rise in risk beliefs, which pertain to the anticipation of potential losses associated with sharing personal information with firms. This escalation in risk beliefs further heightens the perceived importance of data protection and security measures among participants, particularly in the context of smart home environments. This finding underscores the importance of the relationship between individual perceptions of privacy risks and the implementation of robust data security practices by manufacturers (Haney et al., 2020).

The UEQ+ results established that the *Connector* interface surpasses the *Linker* in crucial user experience dimensions such as Attractiveness, Efficiency, Perspicuity, Dependability, and Intuitive Use, evidenced by a higher overall KPI. This quantitative assessment is supported by participants' feedback, which vividly highlights the *Connector's* effectiveness in utilizing visual elements like color-coded lines and icons to enhance clarity and user interaction. Participants particularly praised these features for their ability to depict connections and security statuses, making the interface intuitive and engaging and improving users' perceptions of security. However, despite

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

these positive responses, the trust indices measured did not show significant improvements, suggesting a gap between understanding and trust. AR interfaces need to ensure that visual indicators are intuitive and accurately interpreted, avoiding symbols or colors that might be misunderstood (Knutzen et al., 2021). The feedback also suggests significant room for improvement in both interfaces. Users recommended reducing visual redundancies, enhancing the interpretability of security indicators such as color-coded lines, and providing more detailed explanatory content to avoid confusion. Additionally, suggestions for more interactive elements like clickable devices and guided navigation indicate a demand for informative, engaging interfaces that are easier to navigate.

The study also investigated how participants' prior technological experiences and security concerns influence their interactions with and perceptions of AR interfaces. Upon analyzing the data, a notable disparity was observed in KPI scores between male and female participants when evaluating both AR interfaces. Men exhibited a higher enhancement in KPI scores, suggesting potential differences in their interaction experiences with the interfaces compared to women. Further examination of correlations revealed a positive relationship between the IUIPC mean score and the perceived importance of data protection and security measures among participants of both genders.

However, further analysis using repeated measures ANOVA, which considered individual factors like gender, privacy concerns (IUIPC), and technological attitude (ATI), showed no significant effect of interface type on KPI scores. This lack of a main effect in the ANOVA suggests that while participants may show a general preference for one interface when examined in isolation, the impact of the interface itself may be influenced by other factors, particularly gender. Indeed, the ANOVA revealed a significant interaction between interface type and gender, indicating that men and women responded differently to the two interfaces. Men demonstrated a stronger preference for one interface, potentially explaining the difference detected in the paired t-test. These findings highlight that while individuals who prioritize security concerns (as measured by IUIPC) value security measures as important, this does not necessarily translate into a more favorable interaction with the interfaces themselves. Such insights underscore the significance of considering the diverse mental models of participants to ensure the inclusivity and efficacy of technology interfaces and understanding of smart home systems (Zeng et al., 2017).

The study has limitations that should be acknowledged when interpreting the findings. Firstly, while the data suggests that displaying visualized connections may positively impact users' perception of security, the study cannot

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

definitively establish whether this enhances security perception. Although many users preferred security notices, the study lacks direct evidence of a clear improvement in security perception. However, strong trends are evident from the free responses and the observed enhancement in user experience. Additionally, the sample consists of users with at least one year of smart home experience, indicating a tech-savvy population. Therefore, the findings may not be directly generalizable to users with less technical proficiency.

The study does not provide conclusive evidence to support the claim that AR user interfaces instill more trust than traditional 2D interfaces, as this aspect falls outside the scope of the research. The study's limited device selection involving the Google Nest Cam and Google Home does not fully capture the complexity of a typical smart home environment. This limited scope may affect the generalizability of the findings to setups involving multiple devices and connections. Additionally, the study was conducted with virtual smart homes, which raises concerns about the external validity of the results when applied to real-device AR settings.

Scalability is another limitation, as the study's fixed scenario with two devices does not address how the visualization method would perform with a larger number of devices, potentially leading to cluttered or confusing displays in more complex environments. The study's design also may have introduced bias, particularly due to the consistent use of an insecure camera connection, which could influence participants' perceptions of security importance. Finally, the comparison between the two AR interfaces, one with and one without colored connection lines, might not have been entirely fair, as the interface with more features was likely to perform better, potentially skewing the results.

Acknowledgments

This section is based on the master's thesis:

Jannis Fritsche. 2023. *Impact of Connection Line Visualizations in Augmented Reality on User Experience in Smart Home Devices*. Unpublished master's thesis. University of Bremen.

My contribution to this work: Conceptualization, data curation, formal analysis, investigation, methodology, project administration, resources, partial software development, supervision, validation, and visualization.

4.2.2 Study 13: AR Visualization Drives Security Decisions

Introduction and Background

Our prior study demonstrated that incorporating visual representations of data flow lines into AR interfaces substantially bolstered users' perception of security within smart homes. This improvement was attributed to the heightened clarity and understanding of device interconnectivity, achieved through visual elements like data flow lines accompanied by textual and iconic indicators within the visualizations. Participants strongly favored AR interfaces that visually illustrate the security status of connections. However, in reality, smart home users are required to perform various tasks like accepting privacy policies, granting permissions, configuring security, and customizing device settings to use their devices effectively. In a typical smart home setup, multiple devices are connected internally and to the internet. This connectivity allows data exchange between devices and cloud service providers, raising user concerns regarding data security and privacy risks (Zeng et al., 2017).

Research findings underscore the common scenario where users express privacy concerns; nevertheless, they voluntarily assume associated risks in exchange for perceived benefits (Kokolakis, 2017). They readily adopt privacy-compromising technologies, seldom engaging in risk mitigation strategies, while simultaneously acknowledging responsibility for their choices and usage patterns. These behaviors encapsulate the essence of the privacy paradox, highlighting a tendency towards inaction despite concerns. This reluctance may stem from various factors, including users' limited confidence in managing security and privacy, resulting in experiences of security fatigue and resignation. Moreover, the complexity of configuring settings or the absence of viable alternatives further restricts users' ability to take proactive measures (Mourey and Waldman, 2020).

Non-technical users may find it challenging to grasp the flow of interconnected smart home data and its destinations. They often rely on prior knowledge from experiences with settings on devices like smartphones to get how smart home technology operates. This conceptual knowledge offers users the flexibility to access and utilize information effectively, assisting in their understanding of the principles and logic behind various concepts. However, it may not suffice to grasp the precise workings of a smart home device. While some users may have a basic understanding of concepts such as how a voice assistant functions, they may struggle to address security issues effectively due to a lack of procedural knowledge. Procedural knowledge involves understanding how to perform specific tasks or actions, in this case,

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

enabling users to implement practical steps to protect their data security when using smart devices. For instance, with Alexa, these measures include actions like manually muting the microphone when necessary, regularly reviewing and deleting voice recordings through the Alexa app, adjusting wake word detection sensitivity, and managing third-party skills and permissions.

As conventional manufacturing applications do not provide conducive environments for cultivating this knowledge, researchers have explored effective strategies to impart conceptual and procedural security knowledge to users. They have also examined how these approaches might influence user behavior. When individuals possess a solid understanding of a task and the know-how to execute it, they tend to have greater confidence in their ability to succeed. This belief in one's capabilities, known as self-efficacy, is a fundamental motivator. Boosting self-efficacy can enhance users' intrinsic motivation, leading them toward desired behaviors. In the context of protecting personal data within smart homes, this can inspire users to regularly review and make informed decisions in accordance with their objectives and priorities.

Research Objectives & Theoretical Model In order to fill the identified research voids, this study aims to explore how the visualization of the data flow of smart homes through augmented reality influences the security behavior of smart home users. To achieve this goal, we have developed an AR application that visually represents the data flow among smart home devices and actuators. Users can configure hypothetical security and privacy settings, which are reflected in the AR visualization of the smart home environment. The primary objective of the application is to establish users' procedural knowledge of smart home security settings by providing interactive tasks and visualizations that immerse users in the experience. To assess our research goal, we constructed a theoretical model that declares conceptual and procedural knowledge impact users' self-efficacy concerning privacy and security settings in smart homes (see Figure 4.24). This knowledge influences users' motivation and ability to execute security-related tasks and ultimately determines whether users can make informed decisions in this domain.

The proposed theoretical model draws from two foundational concepts. The first is rooted in the Technology Threat Avoidance Theory (TTAT), which explains the behavior of individual IT users in avoiding the threats posed by malicious information technologies (Liang and Xue, 2009). The TTAT underscores the difference between avoidance and adoption behaviors in response to malicious information technology threats. It overcomes the shortcomings of cybernetic (Edwards, 1992) and coping theories (Lazarus and Folkman, 1984) by introducing a dynamic feedback loop that includes

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

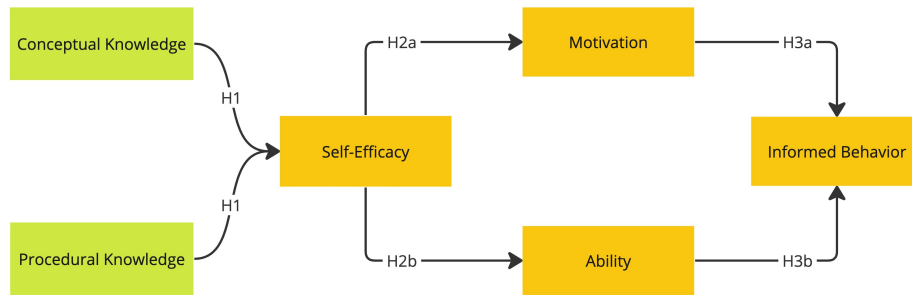


Figure 4.24: The diagram illustrates the research model employed in this study, with arrows denoting their influence on the subjects.

threat and coping appraisals. Users initially measure the threat’s severity and their vulnerability. If they perceive a substantial threat, they assess the effectiveness, cost, and self-efficacy of protective measures. Additionally, TTAT acknowledges using emotion-focused coping when threats appear unavoidable. In contrast to the TTAT, our approach in the realm of smart home security distinguishes itself by strongly emphasizing procedural knowledge and proactive user empowerment. While TTAT primarily focuses on users’ emotional responses and the dynamic feedback loop of threat and coping appraisal, our strategy prioritizes establishing procedural knowledge. We believe that equipping users with concrete knowledge and utilizing visual aids can significantly enhance their decision-making abilities in smart home security scenarios. Instead of relying solely on users’ feelings, we strive to empower them with the tools and understanding they need to protect their smart homes effectively.

The second concept of our approach originates from the research conducted by Arachchilage and Love (2014), which aimed to assess the influence of conceptual and procedural knowledge on computer users’ self-efficacy in mitigating phishing attacks. Their study demonstrates that combining conceptual and procedural knowledge significantly enhances users’ self-efficacy, leading to more effective avoidance of phishing threats. Our approach extends and enriches this framework by incorporating insights from the Fogg Behavior Model (Fogg, 2009). According to the Fogg Behavior Model, converging three factors (Motivation, Ability, and Triggers) is necessary for a desired behavior. Within the Fogg Behavior Model, the absence of adequate motivation and ability renders prompts ineffective in driving target behaviors. Our approach emphasizes explicitly enhancing motivation and ability, leveraging visual aids to achieve this goal, and examining their collective impact on users’ informed

security behaviors while deliberately abstaining from direct intervention in the realm of triggers. This seamless integration of the Fogg Behavior Model into our framework offers a profound insight into the intricate mechanisms that shape users' responses to security challenges in the context of smart homes. Our holistic perspective harmoniously combines the TTAT-based theoretical model and the Fogg Behavior Model, substantially contributes to understanding the multifaceted factors influencing users' security behaviors, and underscores the critical role of well-structured end-user security education. Accordingly, this study investigates *RQ) How can providing procedural knowledge and fostering a sense of achievement through AR visualization enhance self-efficacy, motivation, and ability and promote informed behavior in smart home security settings?* Based on this question, our hypotheses (H) are outlined below (illustrated in Figure 4.24).

H1. Conceptual and Procedural knowledge affect self-efficacy differently.

H2a. Self-efficacy positively affects motivation.

H2b. Self-efficacy positively affects ability.

H3a. Motivation positively affects informed behavior.

H3b. Ability positively affects informed behavior.

Prototype Description

Concept We developed an AR app that overlays smart home devices in their everyday environment with additional visualizations and information, including data flow tracking and privacy and security configuration. The AR app was created with the Unity 2022.1 game engine and is planned for mobile AR supporting ARKit¹⁰ and ARCore¹¹. The app allows users to integrate their smart home devices by scanning a corresponding QR code in front of them. The QR code provides the app with information on the device, its position, and its rotation. For QR code scanning, the ZXing library¹² is used. Furthermore, a database with predefined information for selected smart home devices integrates the device into the AR app.

Device Scenarios In order to simulate a diverse range of scenarios typical for smart home users, we meticulously selected a representative set of widely used devices. As a foundational component, we included a Netgear R6220 WLAN router AC1200, given that routers are ubiquitous in modern homes and essential for device connectivity. To facilitate the management and automation of smart devices, we integrated a Bosch smart home controller,

¹⁰<https://developer.apple.com/documentation/arkit>

¹¹<https://developers.google.com/ar>

¹²<https://github.com/zxing/zxing>

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

which interfaces with a motion detector. Additionally, we incorporated an Alexa Echo Plus 2nd generation to enhance the smart home experience for participants. We included a Google Nest camera to address privacy concerns associated with sensitive personal data, such as video streaming. Lastly, to complete our lineup, we selected an IKEA table lamp that smart home devices can remotely manage. These devices were included purely for their ability to create a realistic smart home setting. They were not intended to be functional or provide connectivity or service during the study.

Design After scanning a QR code, a visual representation of the selected smart home device is displayed within the AR app. This digital projection showcases the device's features, covering its functionality status and configuration options. Each visual representation has a status indicator, employing a color-coded system to convey its current status. The green check box icon indicates the device is secure and functioning correctly; the yellow exclamation mark signals a warning or potential issue that may require attention, and the red exclamation mark denotes a critical problem that needs immediate resolution (see Figure 4.25). These intuitive icons serve as gateways for additional interaction, enabling users to access essential device settings through a user-friendly 2D interface.



Figure 4.25: Upon scanning a QR code, the AR app displays a visual overlay over the actual physical device.

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

Tapping a device indicator for the first time triggers the appearance of a one-pager privacy policy on the 2D interface, inspired by the research conducted by Bahrini et al. (2022). This statement clarifies key aspects of the related device’s privacy policy and offers users a straightforward and easily understandable summary. The statement is structured into three tabs: “Data”, “Rights”, and “Contact”. Each tab contains multiple sections adorned with distinct icons, highlighting the significance or critical nature of specific information (see Figure 4.26).

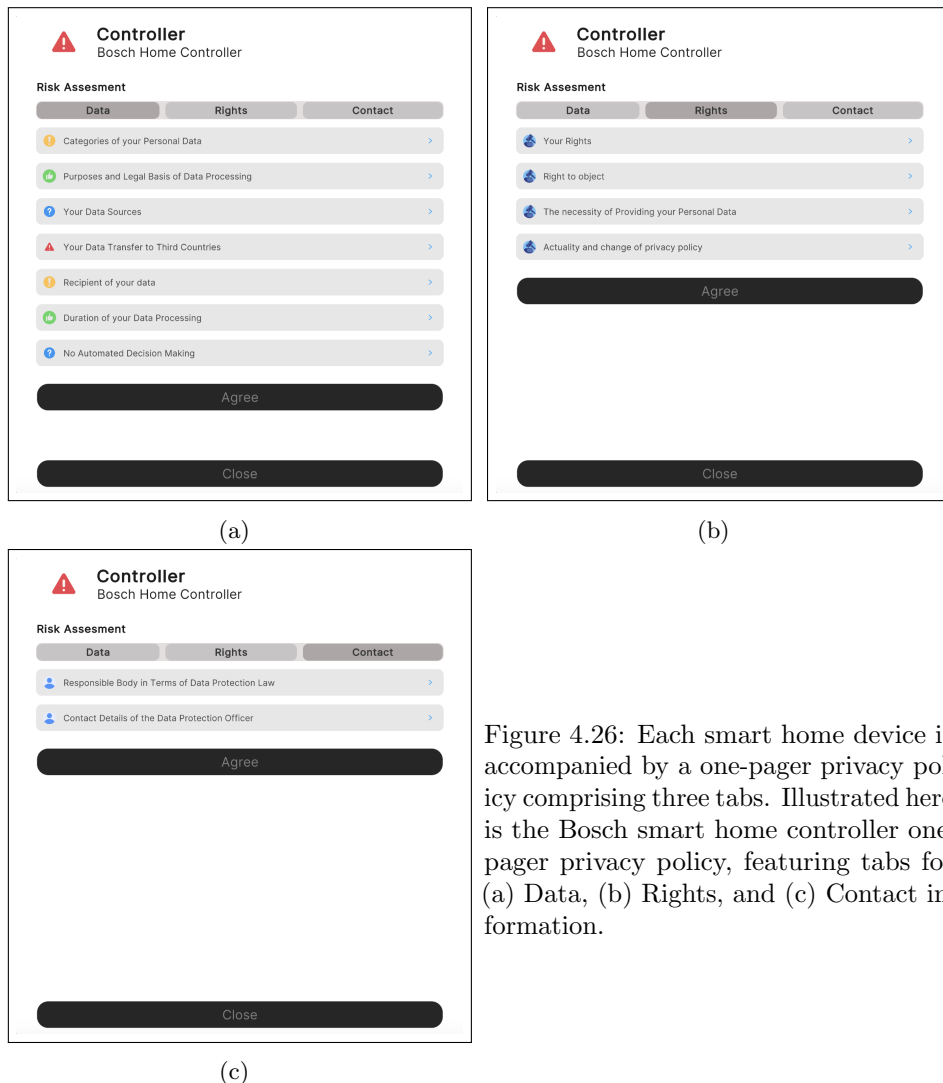


Figure 4.26: Each smart home device is accompanied by a one-pager privacy policy comprising three tabs. Illustrated here is the Bosch smart home controller one-pager privacy policy, featuring tabs for (a) Data, (b) Rights, and (c) Contact information.

We have maintained the same icon design from our previous one-pager study for this one. Generally, a green thumb symbolizes that neither the device nor third parties directly store the user’s personal data. However, if

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

the privacy policy confirms data storage, this icon indicates compliance with legal requirements and transparency regarding time frames. Conversely, a yellow exclamation mark denotes the storage of personal or sensitive user data. This icon also signifies the lack of notifications to users regarding changes in the privacy policy. In contrast, a red exclamation mark flags the transfer of personal data to third parties, whether domestically or internationally. The blue gavel symbolizes user rights, while the person icon represents contact persons. Lastly, a question mark icon indicates the absence of information about this category in the original privacy policy of the related device.

In order to offer a streamlined one-pager privacy policy for each device, we meticulously reviewed and categorized the original privacy policies of our selected devices. Afterward, we integrated the extracted information into each tab as follows.

The “Data” tab encompasses information about 1) categories of user personal data, 2) purposes and legal basis for data processing, 3) sources of user data, 4) recipients of user data, 5) data transfer to third countries, 6) the duration of user data processing, and 7) the presence or absence of automated decision-making for privacy settings. The “Rights” tab includes information about 1) users’ rights, 2) the necessity of providing user personal data, and 3) actuality and privacy policy changes. Lastly, the “Contact” tab encompasses details regarding the body responsible for data protection law and the contact information of the designated data protection officer. Users have the option to tap on any area of interest to access the comprehensive privacy policy text tailored specifically to that particular section. While we preferred privacy statements tailored to specific devices, in cases where only a general statement from the manufacturer was available, we employed it as a substitute. As an example, we utilized the Bosch smart home controller privacy policy for the Bosch motion detector.

Once users agree to the one-pager privacy policy, signifying their acceptance, the integration of their selected smart home device is finalized. Following this, the associated cloud service is prominently displayed at the apex of the physical router, symbolizing the establishment of connectivity. Furthermore, within the AR scene, animated dashed lines dynamically depict the connection between the device and its corresponding cloud service, providing a visual representation of the integration process. We used distinct colors for each device’s connection to its corresponding cloud service, ensuring that users can easily discern and follow the pathways between their devices and the cloud. (see Figure 4.27).

By tapping the indicator again, the AR app provides a range of configurable options categorized into three distinct menus, including: “General,”

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES



Figure 4.27: Upon scanning a device’s QR code and accepting the associated privacy policy, the chosen smart home device is integrated into the system. The corresponding cloud service is displayed prominently above the physical router in the AR scene. Animated dashed lines connect the device to the cloud, using dynamic color coding to enhance visibility and make the device-to-cloud relationships easier to understand and follow. Moreover, tapable icons indicating the communication protocol, such as Wi-Fi and Bluetooth, are displayed along these lines.

“Privacy,” and “User”. The availability of these menus depends on the capabilities of the device. Within the “General” menu, users have the capability to carry out configurations, such as updating the device firmware and verifying its signature. Additionally, this menu in the Bosch smart home controller provides options for establishing connections with devices like the motion detector, Alexa, and Google Nest camera.

The “Privacy” menu contains all settings related to data protection and user privacy. Users can toggle features such as employing encrypted connections, utilizing Virtual Private Network (VPN) services, and ensuring anonymized data transmission. Moreover, users can access and delete their personal data directly from this menu.

Lastly, the “User” menu is exclusively accessible for the smart home Bosch controller. Within this menu, users can add and manage new users within the smart home system, configure detailed settings related to password policies, and adjust the maximum number of allowed authentication attempts (see Figure 4.28).

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

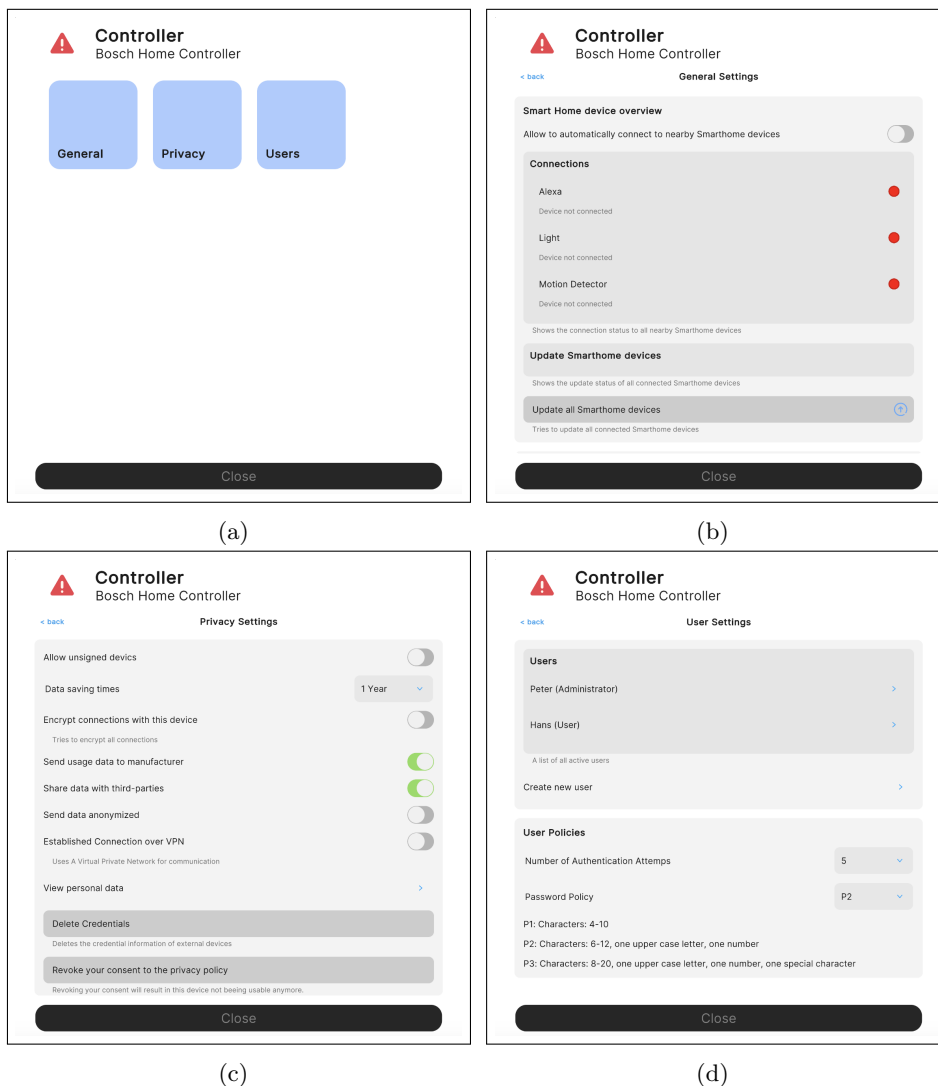


Figure 4.28: Upon agreeing to the privacy policy of the Bosch smart home controller, tapping its indicator triggers the app to reveal a selection of configurable options (a) grouped into three distinct menus: (b) General, (c) Privacy, and (d) User Settings.

Changing a device configuration can affect its status indicator and established connections. For instance, when the privacy policy of a device is revoked, it becomes disconnected from the cloud, and the dotted lines vanish. The device undergoes a reset, and all its data is promptly deleted. Furthermore, in our design, tapping indicators positioned above dotted lines activate a separate 2D interface, revealing details about the device's connection type, whether Wireless, Bluetooth, or ZigBee. Additionally, users gain insights into settings from the "Privacy" menu, such as encrypted connections, VPN

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

usage, anonymized data transmission, and data sharing (see Figure 4.29).

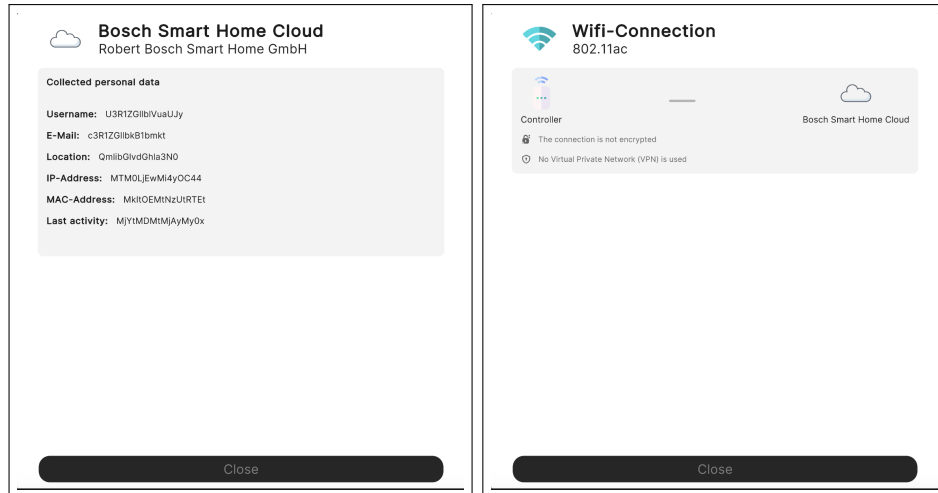


Figure 4.29: The left screen indicates the collected personal information and whether they are anonymized in the Alexa cloud, and the right screen shows a WiFi connection, which provides information encryption and VPN status.

Moreover, the app gives users the capability to interact with smart home clouds situated above the router. Tapping a cloud indicator reveals a 2D screen displaying the collected personal information from the desired smart home device. For instance, if a user opts for data anonymization within the “Privacy” menu, the cloud presents anonymized data, ensuring that personal information is stripped of identifying details before being utilized or shared.

Task Evaluation The AR app includes task and tracking features designed to embed user study and monitor participant actions. Initiating a user test involves scanning a designated QR code, prompting an overlay where participants input their identification, as illustrated in Figure 4.30. The task system sequentially presents users with five tasks: an introductory task, followed by two randomly selected simple tasks, and concluding with two randomly selected challenging tasks (Appendix A.5 contains the list of tasks.). Users can access the task list screen through the AR app. As users progress through tasks, the completion of individual steps is illustrated in the task list. Meanwhile, all user interactions with the app are discreetly recorded in the background and securely stored in an Excel file in the cloud (see Figure 4.30).

User Evaluation

Study Design In order to address our hypotheses, we have formulated a scenario set within a smart home environment aimed at setting up and configuring privacy and security settings. Recognizing the significance of

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

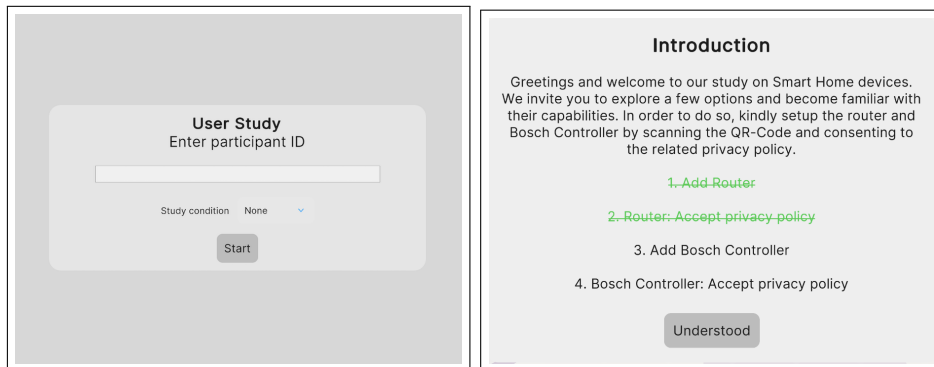


Figure 4.30: User interface for participant identification and task completion Tracking: On the left, participants enter their identification to start the study. On the right, the task list is displayed. When a task is completed, its color changes to green and a line is drawn through the text.

the physical and digital environment and context, as they strongly influence user behavior and interactions with technology, we conducted user tests within a dedicated smart home laboratory situated on our university campus. The Bremen Ambient Assisted Living Lab (BAALL)¹³ encompasses a fully furnished 60m² apartment outfitted with various cutting-edge technical smart systems tailored explicitly for research and development. The lab provides an authentic setting to assess and appraise novel technologies and applications. Figure 4.31 displays the smart home kitchen where our user testing takes place. Throughout the study, participants are asked to immerse themselves in the following scenario: “Envision yourself residing in a smart home for a duration. The home offers you an array of smart devices that have yet to be configured. Your objective is to harness the potential of these smart devices and set them up effectively.”

Materials In this study, we have used both standard questionnaires and custom-designed items to address specific aspects of our research focus.

- *Demographic, Experience, and Knowledge:* We gathered demographic information, including age and gender, from participants. Additionally, we inquired about their prior familiarity with data privacy and security, their experiences and expertise with smart home devices, and their proficiency in utilizing smartphones and augmented reality technology.
- *Affinity for Technology Interaction:* For the purposes of this study, we utilized the 9-item ATI questionnaire to measure participants’ affinity

¹³<https://www.dfki.de/web/anwendungen-industrie/living-labs/bremen-ambient-assisted-living-lab-baall>

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES



Figure 4.31: The smart home’s kitchen is equipped with authentic appliances, including a refrigerator, cooktop, and dining table, creating an actual home environment.

for technology interaction, as described in Section 4.1.1 on page 207.

- *Privacy Concerns:* For this study, we employed the IUIPC questionnaire, which includes three dimensions: Control, Awareness, and Unauthorized Secondary Use. The Control dimension measures the extent to which users desire control over disclosing and transferring their personal information. The Awareness dimension assesses the degree to which users want to be informed about how and to whom their personal information is disclosed. Finally, the unauthorized secondary use dimension examines how important it is for users that online companies must obtain explicit consent before using or sharing personal information. In our questionnaire, we integrate Trusting Beliefs and Risk Beliefs to understand an individual’s inclination to disclose personal information to software companies, as described in Section 4.1.1 on page 208.
- *Practical Setup:* In this part of our study, participants were tasked with setting up a compact smart home system. Initially, they were instructed to configure a Bosch Smart Home controller by installing the Bosch Smart Home app (version 10.16.1) on an iPad Pro 12.9-inch tablet. The Bosch controller served as the central hub for the smart home configuration. Participants then connected a motion detector to the controller. Following this, they linked an Alexa smart speaker to the Bosch controller using the Alexa app (version 2023.15), pre-installed on the iPad. In order to facilitate this process, participants were provided with a document containing login credentials for the smart home devices and their respective accounts. Assistance was available if participants encountered any difficulties during the setup.

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

On average, it took participants 16 minutes to complete this task.

- *Participant Mental Model and Interview:* After setting up the smart homes using manufacturer applications, participants were invited to join a semi-structured interview. The main goal was to evaluate their conceptual knowledge of smart home concepts, including key security and data practice principles. Initially, they were asked to describe their comprehension of the smart home system, visually representing the setup on paper and explaining how devices collected data, connected, and transmitted information. Following this, participants were questioned about various aspects of data management, such as collection, storage, and sharing, as well as their security behaviors and privacy preferences. The interview questions were adapted from research conducted by Tabassum et al. (2019), aiming to understand end-user perceptions of smart home device data practices and risks. We selected questions that aligned with our research objectives for this study. The list of interview questions can be found in Appendix A.5.
- *Self-Efficacy:* Self-efficacy, the belief in one’s ability to achieve specific tasks, is a crucial psychological concept for enhancing individual behavior (Bandura et al., 1999). Various self-efficacy measurement scales have been employed in different contexts, from general ones like the General Self-Efficacy Scale (Schwarzer and Jerusalem, 1995) to technology-focused scales such as the Computer Self-Efficacy Scale (Murphy et al., 1989), Internet Self-Efficacy Scale (Torkzadeh and van Dyke, 2001), and the Self-Efficacy in Information Security (Rhee et al., 2009). In the domain of evaluating self-efficacy related to privacy and security in smart homes, psychologists have developed and validated the Cybersecurity Self-Efficacy in Smart Homes (CySESH) scale (Borgert et al., 2023). This scale aims to assess individuals’ confidence and capability in effectively protecting themselves against cyber threats in smart home environments. With 12 questions, the CySESH scale employs a seven-point Likert scale, ranging from “Strongly Disagree” to “Strongly Agree.”
- *Motivation and Ability:* In order to evaluate the degree of user enjoyment in performing smart home configuration tasks, intrinsic motivation must be evaluated. Intrinsic motivation, rooted in personal interest and the inherent satisfaction from tasks, differs from external influences like rewards (Hennessey et al., 2015). For this purpose, we employed the Task Evaluation Questionnaire extracted from the Intrinsic Mo-

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

tivation Inventory (IMI) (Ryan, 1982). This questionnaire comprises 22 queries, with participants rating each item on a seven-point Likert scale, ranging from “Not true at all” to “Very true.” Key variables measured include *Interest/Enjoyment*, *Perceived Competence*, *Perceived Choice*, and *Pressure/Tension*. We consider that *Perceived Competence* measures the participants’ perceived ability to perform and succeed in the given tasks effectively. This metric provides insight into how capable and proficient the participants feel in managing and completing the smart home configuration activities. In the context of our research, we adapted these questions to align with the specific nuances of smart home scenarios.

- *Informed Behavior*: In order to determine whether participants intend to engage in informed behavior due to their experiences in our study, a set of custom-designed questions was formulated. Participants answered these questions using a five-point Likert scale, ranging from “Strongly Disagree” to “Strongly Agree.” The participants were asked the following questions. The first question is whether they are now extremely knowledgeable (or well-informed) about all the steps needed to keep their smart home data and accounts safe. The second one is whether they will avoid any smart home services that require their name or email address because they are unsure how their personal data will be used. The third question inquires if they will change the default settings of the smart home apps to increase their data security. The fourth question asks whether they will check the privacy policy of the smart home apps before installing them. The fifth question probes whether they will avoid smart home services that rely on cloud storage and instead use a smart home with local networks to minimize the risk of data being attacked while being fetched to the cloud. Finally, the sixth question asks participants, based on their experience with those smart home settings, to what extent it is important for them to change their security behaviors to improve their protection against smart home security threats, such as data breaches, identity theft, device hijacking, and spoofing.
- *User Experience*: The User Experience Questionnaire (UEQ) is a standardized tool designed to quickly assess the user experience of interactive products, such as websites, mobile applications, and software interfaces (Laugwitz et al., 2008). The objective of the UEQ is to enable end users to efficiently provide a comprehensive impression of their user experience. It allows users to express their feelings,

impressions, and attitudes toward the product simply and immediately. The UEQ consists of 26 items grouped into six scales: *Attractiveness*, *Perspicuity*, *Efficiency*, *Dependability*, *Stimulation*, and *Novelty*, each representing a distinct user experience quality aspect. Responses are rated on a scale from “Strongly Disagree” (1) to “Strongly Agree” (7). The UEQ is commonly used during product development to evaluate prototypes or early product iterations and gather user feedback. This approach facilitates quantitative analysis and comparison of results across different studies (Schrepp et al., 2014).

- *AR Setup*: In this stage of the study, participants engage with the AR app, which guides them through a series of five tasks centered around smart home functionalities available in the market. The initial task serves as an introduction to the application. Subsequently, users encounter two straightforward tasks followed by two more challenging tasks, all randomly selected. The AR app monitors user interactions to assess proficiency and includes a task-tracking functionality. Participants begin by scanning a designated QR code, which initiates an overlay prompting the entry of their subject ID. The task system assigns one task to the user at a time. The study director explains the essential features of the AR app before participants begin. The app and assigned tasks are designed to equip participants with procedural knowledge of the processes and security configurations within smart home settings. On average, subjects took 22 minutes to complete the tasks with the AR app.
- *Final Interview*: During the final interview, the interviewer asked participants questions to collect their insights and feedback on the AR interface and its impact on their understanding of smart home systems. They were first asked if they could imagine using such an app privately at home to gauge their interest in personal integration. Participants were then queried on whether they saw an advantage in the AR aspect compared to a traditional 2D visualization, aiming to determine which format they found more beneficial. In order to assess the educational value of the AR app, the interviewer asked participants if they had a better understanding of smart home processes and possible settings after using the AR prototype. Additionally, they were questioned about any differences they noticed in the design of privacy policies between traditional smart home provider apps and the AR prototype. When participants noticed no differences, the interviewer would show the distinctions. If differences were noted, participants were asked

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

for their thoughts on the design of the one-pager privacy policy and their preference between this simplified design and traditional privacy policies, along with their reasons.

Procedure The study commenced with an overview of the entire process, provided to each participant orally and through written documentation. Informed consent was obtained prior to participation. Initially, participants shared demographic information and completed questionnaires assessing their technology affinity and privacy concerns. Participants then proceeded to set up actual smart home devices, with their interactions and challenges meticulously observed. Following this setup, participants engaged in a drawing task to capture their experiences, which was succeeded by a semi-structured interview. After completing the device setup and initial interview, participants filled out self-efficacy, motivation, behavior, and user experience questionnaires. They then undertook augmented reality tasks designed to simulate the setup and configuration of smart home devices. Upon completing the AR tasks, participants were asked to complete the same set of questionnaires again to assess any changes. Finally, a brief follow-up interview was conducted to gather their final reflections. This comprehensive procedure enabled a holistic exploration of the impact of smart home device setup and AR interactions on users' behavior. Figure 4.32 illustrates the study procedure.

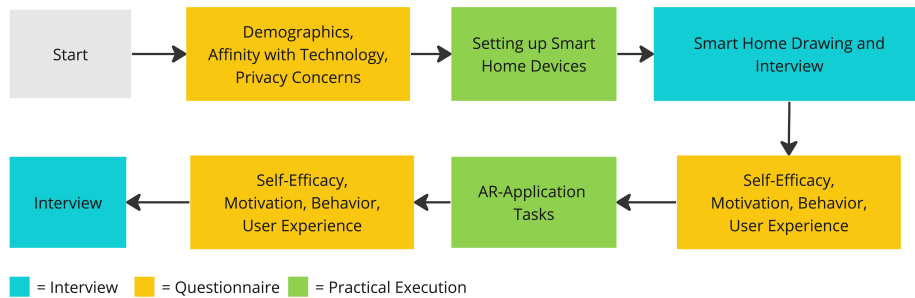


Figure 4.32: User Study Procedure

Pre-Study The preliminary study was conducted in two distinct phases, each with specific objectives to refine the AR app and the entire study process. The first phase, termed the internal preliminary study, focused exclusively on testing the AR app. In this phase, three non-developers from our research group at the university were tasked with evaluating the AR app to identify and rectify prominent user experience issues. They tested the prototype multiple times to accommodate the random assignment of tasks, which led to

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

identifying a few required areas for improvement. It became clear that there was a significant need for clearer task descriptions, more effective feedback mechanisms, and enhanced user instructions. Participants often needed help navigating the prototype, including revisiting task descriptions and interpreting the functionality of various buttons. Additionally, participants found remembering and executing multi-step tasks challenging without frequently referring back to the instructions. These issues underscored the necessity for a more intuitive and user-friendly design. In the second phase of the pre-study, we aimed to test the entire study process in a realistic setting in the living lab. This comprehensive phase involved the setup and interaction with actual smart home devices, providing a holistic view of the study’s logistical and technical aspects. We invited four participants who had no connection to the research project and were guided through the entire experimental procedure, replicating the planned study workflow. This phase also highlighted a few practical challenges, such as the initial setup of smart home devices and connectivity issues, as well as further technical problems with the AR app, which were not apparent in the first phase. Specific issues included the recognition of task completion, where some steps were not acknowledged as completed by the system, leading to participants being unable to progress. The interface overlay of the devices, implemented as a bottom sheet, was difficult to close for participants as they tried clicking outside the overlay rather than using the designated “Close” button. Additionally, a critical issue was found in the data-saving mechanism, where starting the study without a user ID resulted in data not being saved at the end, necessitating a fail-safe to handle empty IDs. These adjustments were crucial in preparing for the main study, ensuring a smooth and effective execution yielding reliable and meaningful results.

Participants We employed a quota sampling strategy to assemble a cohort of participants meeting pre-established criteria. The primary objective of this recruitment methodology was to create a representative sample of individuals adept at using smart home devices. Participation in the study was strictly voluntary, and participants received a 30-euro compensation voucher for their involvement. The recruitment process involved a multi-faceted approach, utilizing mailing lists, engagement through social networks, and word-of-mouth referrals. The final study cohort comprised 26 participants, evenly split between 13 males and 13 females. The average age of the participants was 26.22 years ($SD = 7.02$), with an age range from 19 to 56 years. Regarding their privacy or security background, 12 participants had an educational background, 1 had a professional background, and 14 had no background.

Statistical Analysis Statistical methods were used to analyze the data collected from the questionnaires. Specifically, when scales were administered twice, initially after configuring the smart home using manufacturer apps (SH-Setup) and after performing tasks using the AR application (AR-Setup), paired t-tests were performed to examine significant differences. An alpha level of 0.05 was used for significance testing, and effect sizes were calculated using Cohen's *d* to assess the magnitude of these differences. Furthermore, the ATI score was also evaluated according to the specified instructions, and the UIIPC mean scores were calculated for each category to assess privacy concerns across different dimensions.

Qualitative Analysis The report of the qualitative analyses is structured into two sections: "SH-Setup Interview" and "Final Interview." We employed the Mayring qualitative content analysis technique, renowned for its effectiveness in examining qualitative data (Mayring et al., 2004). This method accommodates both inductive and deductive analysis strategies and is suitable for combining qualitative and quantitative analyses, particularly in mixed methods research (Creswell, 2021). The Mayring method's evaluation process is highly transparent, with each step thoroughly documented to enhance reproducibility and credibility. The method involves several essential steps. Initially, it defines the material, selecting a representative subset relevant to the research question. Then, it analyzes the context of material generation, considering who collected the material, their motives, and the conditions under which it was gathered. The material is formally characterized, and its type and transcription conventions are documented. The direction of the analysis is determined by deciding on the specific aspect of the material to be analyzed, such as the thematic content or dynamic state. The research question is theoretically differentiated to align with scientific rules and theories, ensuring verifiability and integration into broader scientific knowledge. The appropriate analysis technique, such as summarization, explication, or structuring, is selected based on the material and research question. Analysis units are defined, specifying the smallest and largest text units to be analyzed. Finally, the material analysis is conducted using the chosen techniques, applied according to the analysis needs rather than as sequential steps. This approach ensures that findings are credible and reproducible, informed by the data and existing literature.

The initial stages of the content analysis, as outlined by Mayring, were omitted because the data had already been gathered. Therefore, we knew about the material, the circumstances of its collection, and its format and structure. All interview audio recordings underwent transcription with the

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

assistance of researchers involved in the study. For the interviews, the initial step was to determine the relevant information required to address the hypotheses. Subsequently, the subjects' statements for each question were rephrased. An Excel page was created for each subject, with the rephrased responses presented as bullet points. Following this, categories were assigned to these bullet points. This process was tracked in another Excel sheet containing all the categories and the frequency of their occurrence. As part of the inductive approach, cues were analyzed, and categories were incrementally added and refined. Subsequently, the categories were compiled in an overview on a separate Excel sheet, with each respondent assigned a row and their answer categories entered in columns. Finally, the emerging categories were consolidated, and further analysis was conducted to identify high similarities, which led to their combination to prevent double-counting of categories per subject.

Empirical Findings

Experience and Knowledge In response to the inquiry, "How long have you been utilizing smart home systems?" seven participants reported using them for under a year, thirteen participants indicated a usage period of one to four years, and six participants stated a usage duration exceeding four years with smart home systems. When queried, "How would you evaluate your familiarity with smart home privacy and security issues?" three individuals acknowledged having no knowledge, twelve individuals possessed fundamental knowledge, nine individuals possessed intermediate knowledge, two claimed advanced knowledge, and none claimed expertise in this domain. Addressing the query "How much concern do you have for the privacy and security of your own smart home?" all participants demonstrated concern. Seven respondents expressed mild concern, nine held moderate concern, eight held substantial concern, and two exhibited high concern. In reaction to the prompt "How do you assess your familiarity with smartphones?" most participants rated their smartphone knowledge favorably. Two participants possessed foundational knowledge; six held intermediate knowledge; fourteen claimed advanced knowledge and four professed expert knowledge. When queried about their experience with augmented reality applications, fifteen individuals responded affirmatively, and ten responded negatively. However, they indicated they were aware of the AR technology. One individual responded negatively, stating unfamiliarity. Furthermore, participants were surveyed about their ownership of smart home devices. Among the respondents, twenty-three individuals owned at least one smart home device, while three reported not having their own devices but using those belonging to their roommates.

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

ATI Participants achieved an average score of 4.48 ($SD = 0.66$) on the ATI scale, reflecting a high level of technical affinity. The assessment also yielded a Cronbach's α value of 0.84, confirming the reliability of the ATI scale's results.

IUIPC The mean score across the Control, Awareness, and Unauthorized Secondary Use dimensions of IUIPC questionnaire for participants was 5.98 ($SD = 0.62$), with a Cronbach's α coefficient of 0.68. The IUIPC dimensions and context-specific factors (Trusting Beliefs and Risk Beliefs) scores are detailed in Table 4.14. A Pearson correlation coefficient analysis was performed to evaluate the linear relationship between the mean score of the IUIPC and Trusting Beliefs and Risk Beliefs. However, no significant correlations were detected.

Table 4.14: IUIPC Dimensions and Context-Specific Factors Scores

| | Cronbach's α | Mean | Std. Deviation |
|----------------------------|---------------------|------|----------------|
| Control | 0.49 | 5.63 | 0.91 |
| Awareness | 0.42 | 6.00 | 0.75 |
| Unauthorized Secondary Use | 0.65 | 6.22 | 0.85 |
| Trusting Beliefs | 0.79 | 3.47 | 0.97 |
| Risk Beliefs | 0.73 | 4.53 | 0.86 |

Participant Mental Model: Sketching Task Following the setup of smart homes through manufacturer applications, participants were asked to articulate their understanding of the smart home system, illustrating their setup on paper. The initial sketches were then analyzed to grasp their mental models. We paid particular attention to the depiction of data flow among the smart home network components that the participants drew. When certain aspects of the sketches seemed ambiguous, like whether participants grasped the concept of data exchange between Bosch and Amazon symbolized by a cloud icon, we consulted the interview transcripts and considered participants' statements. Figure 4.33 showcases a visual representation of the accurate data flow within the smart home system intended for this part of the study.

The sketches created by the test subjects were categorized into two groups: those with an extended model, including technical elements like routers, and those with a simpler model, focusing solely on the primary smart home devices and their connections. Figure 4.34 displays two sample sketches from test subjects, with the right side showing an extended model and the left side showing a simplified model.

Continuing with the exploration of participants' mental models, we assessed whether all local elements were accounted for, identifying any

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

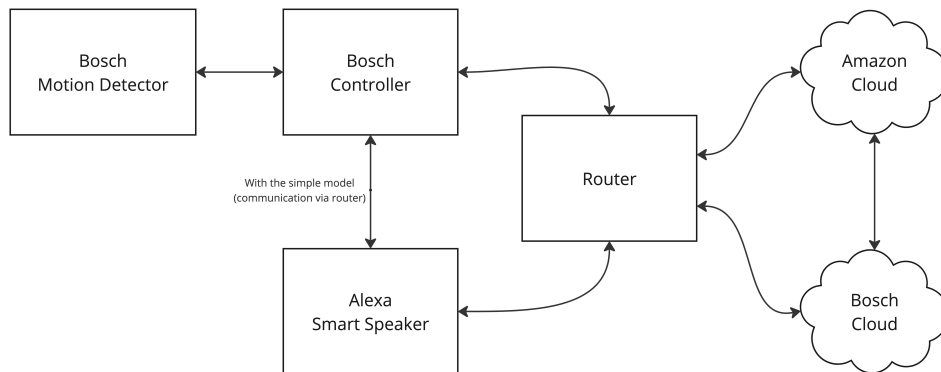


Figure 4.33: The Accurate Data flow model of the SH-Setup

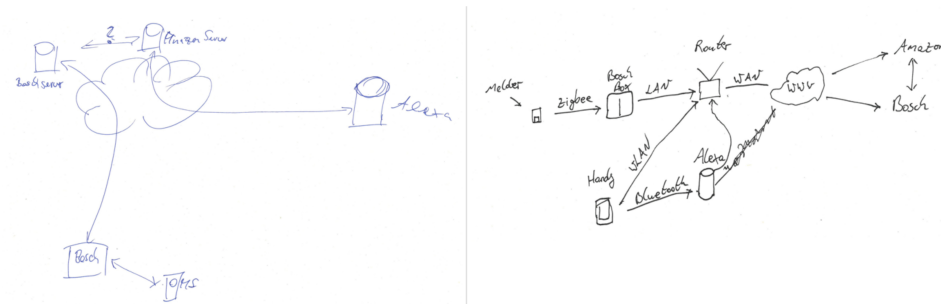


Figure 4.34: Sample sketches from the participants: Simple model on the left, extended model on the right.

errors or omissions in connections to other elements from specific devices. Additionally, we examined how often participants recognized the involvement of providers' clouds and whether they understood the data exchange between these providers. The findings and breakdowns are neatly summarized in Table 4.15 for clarity.

A total of eight individuals accurately depicted the data flow. Among them, three were classified as having technical models, while five had simple models. During their sketches, most subjects ($n = 18$) considered the presence of the providers' cloud. Only one participant illustrated the connection between the clouds, while two others drew question marks at the connection due to uncertainty. However, during the interviews, seven participants discussed the likelihood of manufacturers sharing data with each other. In terms of the sketches, there were inaccuracies in depicting the connections with Alexa (8 participants), the motion sensor (9 participants), the controller (1 participant), and the router (3 participants).

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

Table 4.15: Results of the Participant Drawings

| Overall | Description | Number |
|-----------------------------|--|--------|
| Simple model | Including technical elements like routers | 13 |
| Extended model | Main smart home devices and their connections in focus | 12 |
| Contain all entities | Consider all entities (Alexa, motion detector, controller, and router) | 10 |
| Correct data flow | The data flow is correctly drawn | 8 |
| Incorrect data flow | The data flow is incorrectly drawn | 18 |
| Mistakes | Description | Number |
| Alexa | Connections from/to the Alexa to the entities are drawn incorrectly | 9 |
| Motion Detector | Connections from/to the motion detector to the entities are drawn incorrectly | 8 |
| Bosch Controller | Connections from/to the Bosch controller to the entities are drawn incorrectly | 1 |
| Router not considered | The router is not observed and drawn | 13 |
| Router connection incorrect | The connection to the router is drawn incorrectly | 3 |
| Clouds | Description | Number |
| Observing clouds | Draw the clouds of the providers as well | 18 |
| Data flow between clouds | Establish a connection between the clouds of the providers | 1 |

Participant Mental Model: Interview Based on select questions from the study by Tabassum et al. (2019), the interview aimed to explore participants’ conceptual understanding of essential security and data practices in smart homes. Participants were asked about different aspects of data management, including collection, storage, and sharing, as well as their security behaviors and privacy preferences. The interview questions were carefully assessed using the Mayring method explained earlier in this work.

- *Data Collection:* Participants comprehended the data collection process, showcasing their ability to enumerate primary data acquired by various devices, such as smart speakers that capture voice commands. For example, during discussions on the motion detector, all participants recognized its capacity to record movements and acknowledged that devices like Alexa also capture entertainment preferences. However, there was a lower degree of familiarity with secondary data collection. Specifically, only thirteen individuals were aware that Alexa collects information from other linked applications, encompassing functions like extracting contact lists and tracking music played via Spotify through Alexa. Subject Id757, for example, articulated, “Alexa collects a substantial amount, encompassing your home conversations, depending on your linked accounts. This includes your musical preferences, culinary tastes, recipe choices, viewing preferences, so that’s a lot.”

Furthermore, participants showed a restricted understanding of inference data collection. Specifically, concerning the motion detector, only five participants acknowledged its capability to infer whether someone was at home, with three participants even suggesting it as part of the device’s regular function. In the case of Alexa, seven participants

recognized its ability to assess users' interests based on the gathered data. Subject Id521 offered insights, stating, "The motion detector can derive a significant amount of information, including the presence of the device within the household, identifying when someone is at home, and understanding individual behavioral patterns, such as movements within the home. The amount of information derived depends on the number of devices used." Regarding Alexa, subject Id521 added, "Alexa can essentially evaluate everything it hears, including speaker identification, conversation topics, and keyword, when brands are mentioned, for example."

- *Data Storage:* All participants acknowledged the storage of data collected from Alexa on the provider's servers. Concerning the Bosch motion detector, the majority of participants ($n = 25$) presumed that the motion detector data was housed within the Bosch cloud, with one individual speculating that it could potentially be stored locally. However, none of the respondents knew the exact location of the data storage. One individual (Id251) assumed it might be in the United States, expressing, "I'm not sure. Amazon has its servers in the USA. I don't know where Bosch's are, probably there too, so not close by, the data probably goes further away." Another participant (Id736) suspected that the data is stored in various other countries, saying, "On the servers, which are probably often in other countries." A similar lack of certainty was observed regarding data retention. Most participants ($n = 19$) expressed uncertainty regarding the duration for which the data would be retained, whereas seven individuals believed the data would not be deleted and would be stored permanently. For instance, Subject Id356 expressed, "I think until we delete our account, the data will be stored forever," and Subject Id748 stated, "As long as they need the data. I don't think the data will be deleted."

Approximately half of the participants ($n = 15$) believed it was possible to access their stored data; one participant was unsure, and the remaining ten believed it was not possible. Among the fifteen who thought it was possible, the majority ($n = 10$) believed they could request the data through GDPR, possibly via mail if necessary. For instance, respondent Id757 explained, "You have to write an official letter directly to the company that provides the device with access to this data and request in writing that they transfer or provide you with their stored data." Two participants knew they could access the data through the application, such as Alexa's voice data. Subject Id494

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

mentioned, “With Alexa, you can check the Alexa app to see what data is on the server and delete it if you wish.” Two subjects were confident that checking the data was possible but were unsure about the process. Subject Id836 stated, “It is possible; I saw a video where they check it, but it’s not easily accessible... I don’t remember how.”

Furthermore, seventeen participants knew that it was possible to delete their data and that they had the right to do so. For example, respondent Id695 asserted, “It’s definitely possible. In Germany, companies are legally obligated to delete the data when you are no longer a customer.” Nine participants were unaware of this option. When asked if they had ever considered deleting their data, many ($n = 17$) replied that they had never considered it. Meanwhile, five participants had considered it, and seven participants had deleted their data from other online services but not from their smart homes. Subject Id736 shared, “I started deleting all accounts I don’t use anymore,” and Id748 said, “Yes, I deleted my Facebook account.”

When asked about control over their stored data, most participants ($n = 21$) stated that they did not have control. This lack of control was attributed partly to their lack of knowledge of how to exercise it. Subject Id748 explained, “I know that I don’t have control over it, but also because I don’t know how to do it. I don’t know enough about it for that.” Subject Id744 expressed a similar sentiment, “I have control over Alexa’s records, but in general, I would say I don’t have control over my stored data.” However, five participants believed they had control because they could delete the data or specify its purpose of use. Id340 stated, “Yes, I can say I want it deleted, and I can specify what it’s used for and what purpose.”

- *Data Sharing:* A total of 25 participants were aware that their data was being shared, and they mentioned various organizations and companies involved in this sharing process. Specifically, 11 participants pointed to advertisers, seven mentioned partner companies with which the devices are connected, three identified data processing companies, and one mentioned insurance companies. In comparison, 5 participants could not provide any specific examples. When asked about the reasons for this data sharing, 20 participants mentioned it was primarily for targeted advertising, and 18 believed companies aimed to profit by selling their data. Additionally, some participants noted that data was purchased for product development ($n = 5$) and customer information ($n = 4$). One participant even reasoned that companies preferred purchasing

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

data because collecting it themselves would be time-consuming: “If a company tries to collect the data, they might take several months, maybe even years. It’s easier if they find another company to sell the data to them.” said Id412.

Among the participants, seven mentioned they did not receive any benefit from sharing their data, with one participant (Id279) expressing: “The companies make a profit on the data, and for me per se, there’s no benefit to sharing the data.” Furthermore, 6 participants considered it a disadvantage due to the annoyance caused by personalized advertising. As one participant (Id475) said, “Very rarely do I think the ads I get are interesting. Most of the time, you feel more like you’re being bugged or that your data is being mishandled.” A small group of participants ($n = 3$) believed that sharing their data led to better products, as vendors had more information to enhance their offerings. Four participants appreciated personalized advertising because it often showcased products they were genuinely interested in. For example, subject Id757 mentioned, “For me personally, it’s also nice when the ads are really tailored to you, for your wallet, not so much.”

Despite their knowledge of data sharing, most participants ($n = 21$) had concerns about third parties accessing their data, mainly due to low confidence in handling it. Two participants worried about insecure data practices leading to data leaks, and four expressed concerns about misusing sensitive information, such as banking details. Subject Id471 explained, “The recorded conversations can definitely be reused; for example, if it’s bank access information that I’ve passed through by phone and Alexa overhears that, then of course that would be a problem if that data gets to a third party.” In addition, two participants were apprehensive about being excessively influenced by targeted advertising, leading them to make purchasing decisions they did not genuinely desire. Three participants voiced their discomfort with losing control over their data once it was sold, as one participant (Id340) stated, “The moment any third party has my data, I no longer have control over it.” Moreover, three participants expressed concerns that shared data could be used for discrimination, particularly in countries where certain groups are persecuted based on political or sexual orientation. One participant (Id521) noted, “For example, if Google notices someone is queer and shares that information. In some countries, that can be harmful for that group of people because those are persecuted there.”

- *Security Behaviors:* Individuals often lack comprehensive measures or

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

controls to protect their personal data. Regarding specific practices related to smart home devices, six participants mentioned that when setting up a new device, they typically navigate to the privacy settings to review available options and tailor them to their preferences. One respondent (Id744) expressed, “Currently, I only take steps to safeguard my data during the setup process. I utilize the provided options to minimize personalization and limit data collection. I turn off features such as personalized ads, among others.” Furthermore, two respondents indicated that they research the data collection practices of a smart home device before making a purchase decision. As participant Id855 emphasized, “You have limited control over your data. When considering buying a smart home device, it’s essential to address what data that device collects. If you’re uncomfortable with it, you should reconsider the purchase.” Nine participants stated that they make efforts to minimize the data they share, employing strategies such as turning off app tracking, disclosing only essential information, or opting for online services that do not require account creation. For instance, respondent Id350 explained, “I strive to minimize using services that necessitate sharing personal data. I delete my account if I no longer use a particular service.” Respondent Id748 similarly stated, “The primary action I take when downloading an app is to disable app tracking.” Overall, protecting data poses challenges for most individuals. Among the sixteen participants who took some action, the majority ($n = 12$) found it challenging to implement protective measures, while four found it relatively easy. Additionally, eight participants disclosed that they do not have any steps to protect their data.

- *Privacy Preferences:* The participants strongly desire greater transparency regarding how service providers handle data. Specifically, nine participants emphasized the need to understand what kind of data is being stored and for what purposes. Four individuals wanted to know the duration for which various collected data would be retained. Furthermore, three respondents called for more transparent and consumer-friendly privacy policies, with one (Id757) stating, “I’d appreciate a more accessible presentation because expecting consumers to spend hours deciphering lengthy, fine-print privacy documents when installing software is unrealistic.”

Additionally, one respondent (Id892) advocated for more straightforward labeling of permissions and collected data, ideally displayed directly on product packaging. They suggested that this would simplify

discerning a device’s data requirements, similar to how apps in an app store list necessary permissions and data collection practices.

The participants also strongly desire increased control over the data that service providers store. Five individuals wished to customize which data is stored, allowing them to retain only data directly related to specific purposes. For instance, one respondent (Id855) remarked, “I’d like to have the ability to see what data is being collected quickly and to control which data is transmitted or stored locally easily.”

Three participants emphasized the need for a straightforward mechanism to delete individual data and records held by the provider without necessitating the deletion of their entire account. One participant (Id471) stated, “I’d like the option to easily access information about stored data, including its retention period, and have the ability to customize the data retention period or delete it as needed.” Most importantly, participants expressed a desire for knowledge and control when it comes to sharing their data with third parties. Thirteen individuals wished for greater specificity regarding the recipients and purposes of data sharing. Of these, eleven participants wanted the ability to exercise control over whether their data could be shared with specific third parties and for what reasons. One participant (Id629) articulated this sentiment: “I’d like to have insight into who ultimately has access to my data. It’s one thing to share my data, but another if the company shares it with someone else. I’d appreciate being notified and having the option to consent.”

Additionally, one participant (Id855) proposed the concept of “noisy” data transmission to manufacturers. This idea involves introducing slight alterations to the data using algorithms before transmitting it, making it interpretable for its intended purpose but preventing access to the original data. This approach is particularly valuable for protecting sensitive health data, as it limits the potential for direct personal identification. In summary, the participants voiced a strong desire for greater transparency, control, and customization over their data handling by service providers.

Self-Efficacy Employing a paired sample t-test, we assessed the variations in mean scores derived from the self-efficacy questionnaires. Our analysis unveiled a noteworthy and statistically significant elevation ($t(25) = -8.1$, $p < .001$, $Cohen'sd = -1.58$) in the mean score among participants who engaged with the AR-Setup ($M = 5.52$, $SD = 0.37$) when contrasted with

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

those who interacted with the SH-Setup ($M = 3.66$, $SD = 0.86$).

Motivation and Ability Reported findings reveal significant shifts across all subdomains of the IMI questionnaires, including *Interest/Enjoyment*, *Perceived Competence*, *Perceived Choice*, and *Pressure/Tension*. Results from paired sample t-tests highlight a noteworthy increase in mean scores among participants utilizing the AR-Setup versus the SH-Setup (see Table 4.16). Notably, participants reported heightened interest and enjoyment, greater perceived competence, increased sense of choice, and reduced stress and pressure when engaging with tasks through the AR-Setup.

Table 4.16: IMI Questionnaire Results and Paired T-Test Comparisons

| | SH-Setup | | AR-Setup | | t-test | | | |
|----------------------|----------|----------------|----------|----------------|--------|----|---------|-----------|
| | Mean | Std. Deviation | Mean | Std. Deviation | t | df | p | Cohen's d |
| Interest/Enjoyment | 4.54 | 1.06 | 5.84 | 0.90 | -6.24 | 25 | < .0001 | -1.22 |
| Perceived Competence | 4.63 | 1.06 | 5.12 | 1.00 | -2.51 | 25 | 0.019 | -0.49 |
| Perceived Choice | 4.90 | 1.04 | 5.43 | 0.84 | -3.30 | 25 | 0.003 | -0.65 |
| Pressure/Tension | 2.81 | 1.32 | 2.40 | 1.01 | 2.32 | 25 | 0.029 | 0.45 |

Informed Behavior The Informed Behavior scales assessed respondents through six questions. Upon examining the total scores, notable distinctions surfaced between the SH-Setup and AR-Setup conditions. For questions 2 and 5, which focused on avoiding services that request personal information and favoring local networks over cloud-based services, statistical analysis indicated no significant differences (see Table 4.17 for further elucidation).

Table 4.17: Informed Behavior Results and Paired T-Test Comparisons

| | SH-Setup | | AR-Setup | | t-test | | | |
|------------|----------|----------------|----------|----------------|--------|----|--------|-----------|
| | Mean | Std. Deviation | Mean | Std. Deviation | t | df | p | Cohen's d |
| Question 1 | 2.50 | 0.86 | 3.81 | 0.63 | -6.13 | 25 | < .001 | -1.23 |
| Question 2 | 3.00 | 1.13 | 4.00 | 1.10 | -1.31 | 25 | 0.203 | -0.26 |
| Question 3 | 3.65 | 1.16 | 4.31 | 0.97 | -3.94 | 25 | < .001 | -0.77 |
| Question 4 | 3.12 | 1.11 | 3.96 | 1.04 | -3.73 | 25 | < .001 | -0.73 |
| Question 5 | 2.77 | 1.24 | 2.54 | 1.03 | 1.19 | 25 | 0.247 | 2.23 |
| Question 6 | 3.77 | 1.07 | 4.04 | 1.11 | -2.27 | 25 | 0.032 | -0.45 |
| Overall | 3.00 | 0.69 | 3.51 | 1.73 | -6.70 | 25 | < .001 | -1.31 |

Model Testing Our analysis investigated the influence of self-efficacy on smart home users' informed behavior through Motivation and Ability, comparing conceptual and procedural knowledge scenarios. In the suggested model, Motivation is conceptualized as a synthesis of four key components: *Interest/Enjoyment*, *Perceived Competence*, *Perceived Choice*, and *Pressure/Tension*, with Ability representing *Perceived Competence*. For each construct, Cronbach's α coefficients were computed to assess the internal consistency of the questionnaire items. Table 4.18 summarizes these findings.

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

Prior studies have emphasized the significance of achieving a minimum Cronbach's α threshold of 0.7 to ensure the reliability of item sets (Cronbach, 1951; Tavakol and Dennick, 2011).

Table 4.18: Cronbach's α Coefficient Scores of the Questionnaires

| | Self-Efficacy | Motivation | Ability | Behavior |
|----------|---------------|------------|---------|----------|
| SH-Setup | 0.82 | 0.75 | 0.84 | 0.70 |
| AR-Setup | 0.89 | 0.74 | 0.87 | 0.83 |

Given the violation of normality in our dataset, Spearman's rho correlation was utilized to assess the relationships between Self-Efficacy, Motivation, Ability, and Informed Behavior across both scenarios. Regarding the procedural knowledge scenario, self-efficacy showed significant positive correlations with Motivation ($r_s(24) = 0.459$, $p = .018$) and Ability ($r_s(24) = 0.657$, $p < .001$). In contrast, Motivation ($r_s(24) = 0.501$, $p = 0.009$) and Ability ($r_s(24) = 0.522$, $p = 0.006$) both exhibited significant positive correlations with Informed Behavior. We have not observed any significant correlation within the conceptual knowledge scenario ($p > 0.05$ for all comparisons).

In this analysis, we calculated the R-squared values to determine how much of the variance in the dependent variables (Motivation, Ability, and Informed Behavior) is explained by the independent variable (Self-Efficacy). In the procedural knowledge context, self-efficacy significantly predicted both motivation ($R^2 = 0.246$, $p = 0.010$) and ability ($R^2 = 0.332$, $p = 0.002$). Additionally, Motivation ($R^2 = 0.183$, $p = 0.029$) and Ability ($R^2 = 0.207$, $p = 0.019$) significantly predicted behavior, indicating that higher self-efficacy enhances informed behavior through increased motivation and ability.

The R-squared value of 0.246 for the regression of Self-Efficacy on Motivation indicates that 24.6% of the variance in Motivation is explained by Self-Efficacy. Similarly, the R-squared value of 0.332 for the regression of Self-Efficacy on ability implies that 33.2% of the variance in ability is explained by Self-Efficacy. The R-squared value of 0.138 for the regression of Motivation on Informed Behavior implies that 18.3% of the variance in Informed Behavior is explained by Motivation. Finally, The R-squared value of 0.207 for the regression of Ability on Informed Behavior means that 20.7% of the variance in Informed Behavior is explained by Ability (see Figure 4.35).

Conversely, in the conceptual knowledge scenario, Self-Efficacy did not significantly predict Motivation ($R^2 = 0.021$, $p = 0.481$) or Ability ($R^2 = 0.004$, $p = 0.759$), and neither Motivation ($R^2 = 0.108$, $p = 0.101$) nor Ability ($R^2 = 0.063$, $p = 0.215$) significantly predicted Behavior.

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

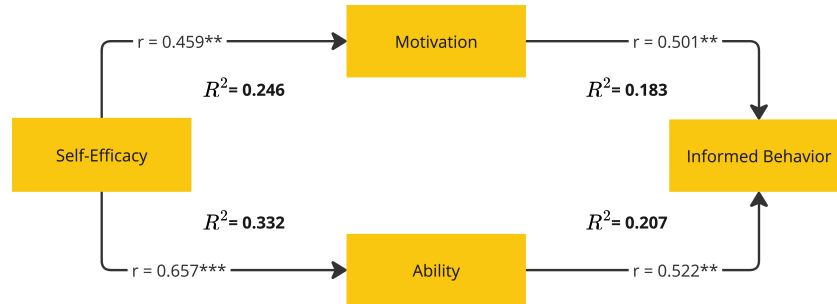


Figure 4.35: Relationships between Self-Efficacy, Motivation, Competence, and Informed Behavior in procedural knowledge, with arrows indicating direction and R-squared values representing variance explained.

User Experience The UEQ values, ranging from -3 to $+3$, provide insights into user experiences. Notably, the AR-Setup surpassed the SH-Setup in the attractiveness category, reflecting overall impressions. Similarly, in terms of efficiency, indicating task completion ease, the AR-Setup significantly outperformed the SH-Setup. Noteworthy differences emerged in the dependability category, assessing user control during the interaction, with the AR-Setup exhibiting significant superiority. Stimulation and originality, evaluating excitement and innovation, favored the AR-Setup over the SH-Setup during task execution. While perspicuity ratings favored the AR-Setup slightly, statistical significance was not reached. Please refer to Table 4.19 for detailed values on both scales. Furthermore, Figure 4.36 visually presents the UEQ benchmarks for both the SH-Setup and AR-Setup, providing a comprehensive overview of the comparative performance.

Table 4.19: UEQ Results and Paired T-Test Comparisons

| | SH-Setup | | AR-Setup | | t-test | | | Cohen's d |
|----------------|----------|----------------|----------|----------------|--------|----|--------|-----------|
| | Mean | Std. Deviation | Mean | Std. Deviation | t | df | p | |
| Attractiveness | 0.69 | 0.69 | 1.38 | 0.42 | -5.43 | 25 | < .001 | -1.06 |
| Perspicuity | 1.08 | 0.75 | 1.13 | 0.61 | -0.4 | 25 | 0.695 | -0.8 |
| Efficiency | 0.78 | 0.83 | 1.23 | 0.63 | -3.03 | 25 | 0.006 | -0.59 |
| Dependability | 0.67 | 0.66 | 1.01 | 0.58 | -2.15 | 25 | 0.0042 | -0.42 |
| Stimulation | 0.67 | 0.69 | 1.42 | 0.50 | -5.80 | 25 | < .001 | -1.13 |
| Novelty | 0.06 | 0.76 | 1.38 | 0.51 | -7.70 | 25 | < .001 | -1.51 |

Final Interview The interview questions delved into participants' perspectives on the AR app and their experiences with augmented reality. The evaluation was structured around four key areas: opinions on the AR interface, experiences with augmented reality versus 2D, improved understanding, and perceptions of the one-pager privacy policy.

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

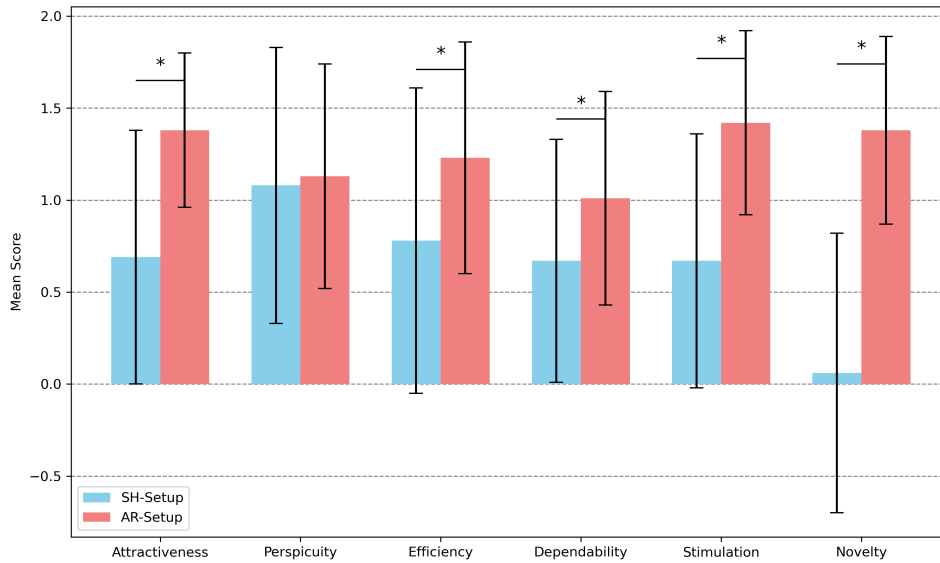


Figure 4.36: UEQ comparison benchmarks for the SH-Setup and AR-Setup.

- *Opinions on the AR Interface:* In answering the interview questions, 24 participants expressed their willingness to utilize an AR application within the context of their smart homes. However, one participant remained uncertain about its utility, while another declined due to insufficient smart home devices. Among the participants ($n = 24$), the most favored aspect of the AR application was its visualization of data flow, as it greatly facilitated their comprehension of how their devices communicate. For instance, subject Id836 enthusiastically remarked, “I would appreciate having an app like this that allows me to visualize the data flow within my home, revealing the complicated interplay between my devices, data sharing mechanisms, storage locations, and cloud servers. It would provide me with valuable insights, especially when it comes to installing new components.” Furthermore, six respondents indicated their intention to employ the app to set up and configure their smart homes. In comparison, five respondents praised the AR app’s utility in simplifying technical concepts, making it particularly valuable for individuals with limited technical knowledge. For example, Id471 remarked, “I find it quite exciting, especially for those completely unfamiliar with the difficulties. It becomes even more thrilling when you can witness the path of data and its various aspects.” Similarly, Id340 highlighted, “The AR app appears exceptionally beneficial for training and educational purposes, making it a valuable resource.”

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

- *Augmented Reality or 2D*: Twenty respondents in our study considered AR a favorable feature of the proposed app concept. Specifically, 15 participants recognized the advantages of AR in enhancing the visualization of data flow, which might be less comprehensible in a two-dimensional (2D) format. Moreover, nine participants demonstrated a heightened interest in utilizing AR applications, praising the spatial interaction they enabled with their smart home devices in their surroundings. Instead of navigating through menus, they could physically approach the device and adjust its settings. One participant (Id251) described it: “It’s nice to see that in the room; it makes me much more interested in reading the information from the devices. It’s exciting to see the devices in real life and be able to click on them. When I want to set up the device, I go there and set it up.”

Nevertheless, opinions on the efficacy and preference between augmented reality and 2D interfaces were polarized among participants. Respondent Id340 suggested, “I believe it requires a bit more effort, and it is easier to manage privacy settings from your smartphone while sitting on your sofa. I find it more convenient.” Similarly, Subject Id982 stated, “If I have numerous devices at home, I would prefer a 2D overview so that I do not have to carry the tablet around all the time.” In general, three participants favored the convenience of making adjustments from their sofa, especially if they had multiple devices distributed throughout their homes.

Nine participants expressed that interacting with a smart home using augmented reality was more captivating than a conventional 2D user interface. Additionally, four subjects believed that it encouraged more significant engagement with smart home settings; as Id251 noted, “The advantage lies in its heightened interest and interactive appeal compared to mere button clicking.” However, four participants contended that a 2D app would likely offer greater clarity, especially when dealing with numerous devices across multiple rooms. Id494 remarked, “Certain aspects can be a bit challenging; you always need to physically approach the devices, aim the camera precisely, and select them, which can become cumbersome when items overlap.” Respondent Id279 concurred, “It may become overly cluttered with multiple devices, so having the option to switch to 2D would be preferable.” Furthermore, six participants indicated a preference for using an AR app, but they also considered a functional 2D version with equivalent features an acceptable alternative.

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

- *Enhanced Understanding:* Concerning whether the respondents gained enhanced comprehension after engaging with the AR application, the data reveals that 24 individuals responded affirmatively, while one answered negatively, and another responded with some uncertainty. Additionally, 16 respondents expressed that they now have a deeper grasp of the data flow within a smart home environment. Five subjects emphasized their heightened awareness regarding the prevalent communication between most smart home devices and the providers' cloud infrastructure. For instance, Subject Id695 shared, "Perhaps it was not something I had considered much or was aware of before, but it was fascinating to witness the data's journey to the cloud and the multitude of clouds involved."

Furthermore, nine participants reported that they gained a more comprehensive understanding of the vendors' data practices directly from their interaction with the application. This outcome can likely be attributed to including a concise one-pager privacy policy for each smart home device that users had to acknowledge before utilizing. This approach resonated with six individuals who had previously expressed dissatisfaction with vendors' practices of concealing the privacy policy behind obscure links. As one participant, labeled as Id855, put it, "Yes, with the providers, it's naturally much more complicated. Either it's only shown very small somewhere, or not at all, or you don't even know how to navigate there. That was much simpler and more obvious with the AR application."

A considerable number of participants ($n = 24$) indicated that they now fully understood the available settings within a smart home environment following their engagement with the AR application. Among these respondents, nine specifically noted that the settings were presented more clearly. At the same time, five more individuals felt they had a heightened awareness of the general range of settings available in a smart home. For instance, Respondent Id989 commented, "I had not paid much attention to this aspect before. Through this application, I have certainly become more cognizant of it." Similarly, Respondent Id471 stated, "Yes, it underscores the importance of paying greater attention to and revisiting these settings."

- *One-Pager Privacy Policy:* Around 20 participants observed a notable distinction between the privacy policies. When directly questioned, all respondents preferred the one-pager privacy policy over the conventional presentation of a continuous text privacy policy. The unanimous

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

consensus was that the one-pager privacy policy was more comprehensible than the regular one. Eleven participants specifically appreciated the absence of extensive textual content, finding it advantageous. The key factors contributing to the one-pager favorability included the ease of locating, reading, and comprehending essential information, which was attributed to the presentation style, which featured bullet points, distinct icons, and varied colors.

Overall, 20 participants found the one-pager format more user-friendly. For instance, respondent Id251 remarked, “I found it very well-structured and clear. Each point was listed individually, and when expanded, the text was not presented as a dense block but rather as a concise and easy-to-read breakdown of the collected information.” Respondent Id695 echoed this sentiment: “I definitely found it clearer because it demanded immediate attention. Additionally, using icons, color-coding, and collapsible sections made it well-organized and easy to navigate. I thought it was a superior design.”

However, one respondent (Id932) raised concerns about interpreting content based on icons and colors, highlighting the subjectivity of individual interests. They remarked, “I find the reliance on icons problematic, as what may be considered risky to one user might be less relevant to another. People have diverse perspectives on data handling.” Nine respondents believed that a design like the one-pager would encourage more people to read privacy policies in general. A subset of 5 participants appreciated the minimal time investment required to grasp the concept. Furthermore, two participants felt that this format gave them greater control over their data because they could better understand the data practices of the manufacturers. As Id757 put it, “Definitely the one-pager, because it is much clearer and encourages a quick review. You feel more in control of your data, and I think that’s crucial.”

Discussion and Limitations

This study evaluated how augmented reality visualization can enhance users’ self-efficacy, motivation, and informed behavior when managing smart home security settings. Building on previous work (Alqahtani and Kavakli-Thorne, 2020a), the AR-Setup introduced an immersive and interactive experience that effectively visualized data flows within smart home ecosystems, providing participants with hands-on engagement. This design addresses the challenges of making often-invisible data flows comprehensible and actionable, ultimately

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

helping users navigate complex security configurations. Our results align with research underscoring AR’s potential to elevate procedural knowledge and foster user confidence in digital security tasks (Cassidy and Eachus, 2002). Through interactive experiences, AR uniquely supports users in demystifying smart home data flows, rendering abstract concepts tangible and enhancing user autonomy in managing privacy and security settings (Oh et al., 2009; O’Connor and Mahony, 2023).

Our approach leverages the Technology Threat Avoidance Theory (TTAT) to frame how users respond to security threats by evaluating perceived risks and their coping strategies (Arachchilage and Love, 2014). Complementing this, the Fogg Behavior Model provided a lens through which to understand how motivation, ability, and triggers drive behaviors (Fogg, 2009). Integrating these theories emphasized procedural knowledge as a pathway to building user self-efficacy, motivation, ability, and ultimately, informed behavior. This integration represents a holistic approach, focusing on users’ immediate emotional responses to security threats and fostering a proactive stance toward smart home security by combining threat appraisal with actionable strategies. By supporting both TTAT and FBM frameworks, the study provides insights into bridging awareness and behavior in complex technology environments.

The AR-Setup significantly improved users’ self-efficacy over the SH-Setup, demonstrating the effectiveness of AR in facilitating experiential learning. This supports our hypothesis H1, which posited that integrating procedural knowledge via AR would enhance self-efficacy. The role of self-efficacy in shaping behavior is well-documented, particularly in technology settings where confidence in managing digital interactions predicts user engagement and cautious behavior (Rhee et al., 2009; Van Dinther et al., 2011). In line with H2a, model testing showed that self-efficacy predicted motivation in the procedural knowledge context. Qualitative responses underscored this finding, with participants describing the AR-Setup as an “exceptional resource for training and education,” emphasizing how the application empowered them to approach security settings with greater confidence (Id340). This interactive approach allowed participants to visualize data flows and receive immediate feedback, reinforcing their understanding and mastery over security configurations.

Beyond self-efficacy, motivation and ability emerged as significant factors, contributing to users’ engagement with the AR-Setup and the effectiveness of their security management. Higher scores in the IMI subscales, such as *Interest/Enjoyment*, *Perceived Competence*, *Perceived Choice*, and reduced *Pressure/Tension*, indicate that the AR application successfully created

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

a stimulating and less stressful environment (Lampropoulos et al., 2023). The elevated motivation scores align with H2b, which hypothesized that procedural knowledge would bolster ability in the AR-Setup. Participants expressed a greater willingness to interact with and manage security settings, citing the process as “exciting” and “engaging,” which fostered intrinsic motivation (Id251, Id471). Additionally, this heightened motivation aligns with existing research that recognizes AR’s ability to make complex security management tasks more intuitive, promoting user willingness to learn and engage actively (Prange et al., 2022).

The AR-Setup also led to more informed security behaviors, supporting H3 by showing that procedural knowledge can translate into practical, protective behaviors. Participants demonstrated greater discretion in selecting services, favoring local networks over cloud-based options, and being more cautious about sharing personal information. This aligns with previous findings that AR-driven experiential learning enhances the procedural understanding, leading users to adopt safer behaviors when handling personal data (O’Connor and Mahony, 2023). The significant differences in informed behavior between the AR and SH setups highlight AR’s potential to empower users to make security-conscious decisions (Alnajim et al., 2023). One participant noted, “I had not paid much attention to this aspect before. Through this application, I have certainly become more cognizant of it” (Id989). These findings reinforce the connection between self-efficacy, motivation, and behavior, demonstrating how users’ confidence in managing security settings translates into actions that better safeguard privacy (Korkiakoski et al., 2023).

Our findings suggest that procedural knowledge, enhanced through the AR-Setup, plays a more significant role than conceptual knowledge in shaping user self-efficacy, motivation, and informed behavior. The AR-Setup’s focus on hands-on engagement, where users could actively interact with data flows, contrasts with traditional, conceptual approaches that often rely on abstract explanations. This hands-on experience aligns with educational frameworks like experiential learning theory, which emphasizes active, meaningful engagement with content to foster understanding and retention (Kolb, 2014). Qualitative feedback reinforced this point, with participants expressing an appreciation for the complexity of data flows. For example, one participant commented, “Perhaps it was not something I had considered much or was aware of before, but it was fascinating to witness the data’s journey to the cloud and the multitude of clouds involved” (Id695), highlighting the limitations of traditional methods (O’Connor and Mahony, 2023).

The study also evaluated user experience, with the UEQ results indicating that AR-Setup was perceived as more attractive, efficient, dependable,

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

stimulating, and novel compared to the SH-Setup. The preference for AR’s one-pager privacy policy, which distills complex information into concise, digestible sections, emphasizes users’ desire for simplicity and clarity when navigating privacy settings (Bahrini et al., 2022). Participants noted that this design minimized cognitive load, allowing them to focus on understanding each point individually rather than being overwhelmed by dense text. One participant shared, “Each point was listed individually, and when expanded, the text was not presented as a dense block but rather as a concise and easy-to-read breakdown of the collected information” (Id251). This feedback underscores the importance of user-friendly interfaces that balance information complexity with ease of understanding, which is critical for AR applications designed to facilitate user interaction and learning (Davidavičienė et al., 2021; Arena et al., 2022).

The findings of this study should be interpreted in light of its limitations. The sample size was limited, and reliance on self-reported measures may introduce bias. Furthermore, there was no direct comparison between the AR-Setup and a 2D application version, which limits our ability to conclude whether AR’s immersive qualities uniquely drive the observed outcomes. Additionally, participants interacted with real smart home applications prior to using the AR app, which may have influenced their engagement and perceptions. Future research should include parallel tests with 2D versions of the application to assess whether comparable gains in self-efficacy, motivation, and informed behavior can be achieved without the complexity of AR. Longitudinal studies would also help examine the durability of these effects over time, providing insight into how repeated exposure to procedural knowledge influences behavior (Zimmermann and Renaud, 2021).

Acknowledgments

This section is based on the master’s thesis:

Tim Görnitz. 2023. *Does Augmented Reality Visualization of Data Flow in Smart Homes Influence Users’ Security Behaviors Regarding Data Control?* Unpublished master’s thesis. Hochschule Bremen.

My contribution to this work: Conceptualization, data curation, formal analysis, investigation, methodology, project administration, resources, partial software development, supervision, validation, and visualization.

4.2.3 Study 14: 2D Interface Drives Security Decisions

Introduction and Background Our previous study revealed that using augmented reality to visualize data flow in smart homes significantly improves users' procedural knowledge, self-efficacy, motivation, and ability, ultimately leading to more informed behavior regarding security settings. Participants using the AR app exhibited a stronger understanding and better management of smart home security than those using conventional methods. However, a limitation of the study was its exclusive focus on AR, without evaluating whether a 2D version of the same app could similarly empower users.

To address this limitation, we designed a new study to test the 2D version of the app with a new set of participants. The study aims to determine whether this approach can similarly enhance users' understanding and behavior regarding smart home security. By replicating the methodology with the 2D version, we seek to provide insights into its effectiveness and compare these findings to our previous AR-based study. This comparison will help us evaluate whether AR and 2D versions can serve as practical tools for improving smart home security practices among users. To ensure consistency, we constructed the theoretical model based on the previous study, which posits that conceptual and procedural knowledge impacts users' self-efficacy concerning security settings in smart homes (see Figure 4.37).

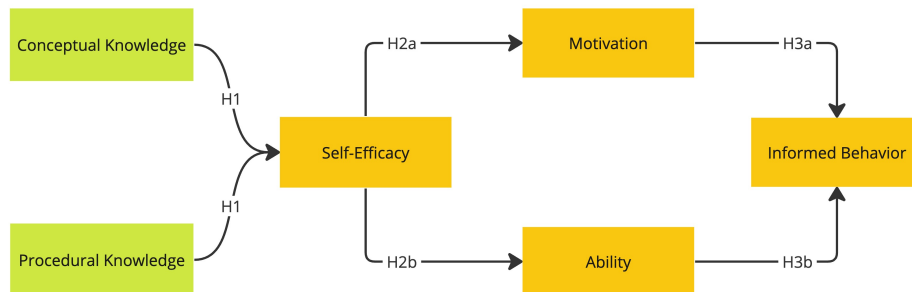


Figure 4.37: The diagram illustrates the research model employed in this study, with arrows denoting their influence on the subjects.

Consequently, this study investigates *RQ) How can providing procedural knowledge and fostering a sense of achievement through 2D visualization enhance self-efficacy, motivation, and ability and promote informed behavior in smart home security settings?* The hypotheses (H) remain unchanged from the prior study. They are represented as follows:

H1. Conceptual and Procedural knowledge affect self-efficacy differently.

H2a. Self-efficacy positively affects motivation.

H2b. Self-efficacy positively affects ability.

H3a. Motivation positively affects informed behavior.

H3b. Ability positively affects informed behavior.

Prototype Description

Concept The 2D app was designed to visually represent the data flow among smart home devices and actuators, similar to the AR app but within a two-dimensional interface. We have integrated a feature in the app that allows users to add specific smart home devices by scanning their QR codes. Users can seamlessly incorporate a device into their network by scanning its QR code through the designated plus button in the app’s interface, a common method used across various applications.

Device Scenarios In this study, we employed the same device and network architecture as in the previous study (see Section 4.2.2, page 273). This consistent setup enables a direct comparison of user interactions and behaviors across different scenarios.

Design The design of the 2D app in this study builds on the core elements established in the AR version, creating a visually comparable experience. As with the AR application, the setup in this version begins with scanning a QR code, which then displays a visual representation of the selected smart home device (see Figure 4.38). This projection mirrors the functionality and configuration options shown in the AR version, using green checkmarks, yellow exclamation marks, and red exclamation marks to convey device security and operational states (refer to Section 4.2.2, page 274).

Device settings are accessible through the 2D interface, where tapping a device icon presents users with a concise one-pager privacy policy. As in the AR version, this policy is organized into three main tabs: “Data,” “Rights,” and “Contact.” Each tab provides summaries with intuitive icons representing different information categories, aiding users in quickly understanding the privacy policies associated with each device (see Section 4.2.2 on page 275).

In the 2D app, devices are represented by icons, and connection pathways between them are shown as lines. Protocol icons, such as Wi-Fi and ZigBee, appear along these lines to indicate the communication method of each connection. Clouds are displayed on the screen, with each device’s connection to its cloud service in a uniform color. Connections between clouds are shown in a distinct color, making them easier to distinguish (see Figure 4.38).

Consistent with the AR design, three main settings menus, “General,” “Privacy,” and “User” are accessible depending on device capabilities. The

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

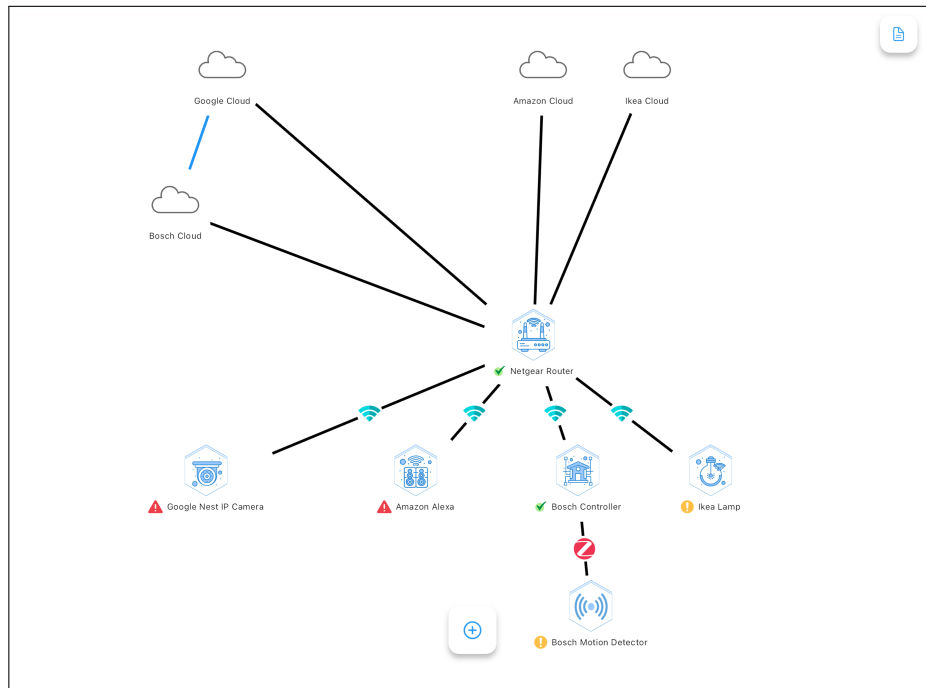


Figure 4.38: Upon scanning QR codes, the 2D app displays interconnected smart home devices linked via lines to the router and clouds.

“General” menu offers options such as firmware updates, signature verification, and device connections. The “Privacy” menu focuses on data protection settings, enabling users to toggle encrypted connections, enable VPN, and manage data anonymization. The “User” menu allows specific configuration options for devices with multi-user functionality, such as managing access permissions and setting password policies (see Section 4.2.2, page 277).

Similarly, task completion and participant tracking in the 2D version are managed through an organized task list. This interface replicates the task flow of the AR application, enabling users to input their identification and complete tasks sequentially. Progress is visually represented, with completed tasks highlighted in green and crossed out, maintaining visual consistency with the AR design (see Figure 4.39).

User Evaluation

Study Design As part of this research, we conducted tests in the same smart home laboratory as in our previous research, adhering to a similar experimental design. This scenario-based approach focused on configuring privacy and security settings within a smart home environment. The BAALL, a fully furnished apartment equipped with advanced smart systems, provided

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

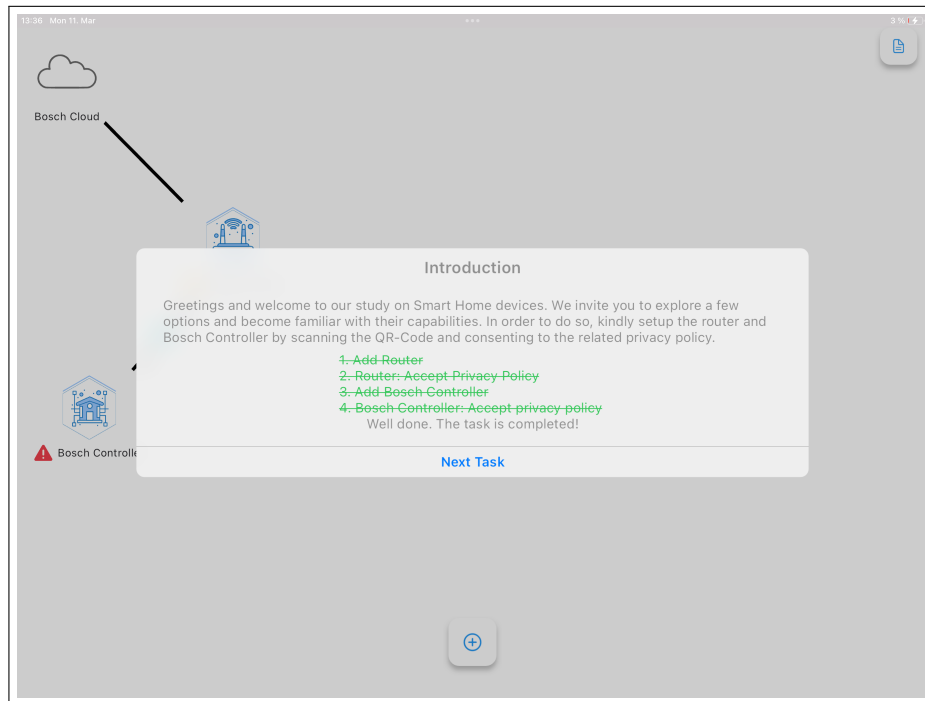


Figure 4.39: User interface for task completion tracking: Similar to the AR app, the task list appears with each task changing to green and crossed out once completed.

a realistic setting for evaluating user behavior and interactions. Participants were instructed to imagine themselves living in the smart home, with the task of configuring various smart devices to optimize their functionality. An additional view of this smart home setup is shown in Figure 4.40.

Materials In this study, we used the same standard questionnaires and custom-designed items as in the previous study (see Section 4.2.2, page 280 for detailed information), with modifications to align them with the 2D interface. An overview of the questions and adjustments is provided as follows.

- *Demographic, Experience, and Knowledge:* We gathered demographic information, including age and gender, from participants. Alongside this, we queried their ownership of specific smart home devices and types owned, their years of experience with smart home systems, their self-assessed knowledge of smart home privacy and security issues, and their level of concern regarding the privacy and security of their own smart homes. Moreover, we asked about their proficiency in utilizing smartphones. The question about AR experiences was removed.

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES



Figure 4.40: Smart home laboratory setup with kitchen, living room, and configurable device stations.

- *Affinity for Technology Interaction:* We utilized the 9-item ATI questionnaire to measure participants' affinity for technology interaction without any modifications.
- *Privacy Concerns:* The Internet Users' Information Privacy Concerns (IUIPC) questionnaire was employed without making any changes, including the dimensions of Control, Awareness, and Unauthorized Secondary Use, along with the context-specific factors of Trusting Beliefs and Risk Beliefs.
- *Practical Setup:* In this part of the study, participants set up a compact smart home system similar to the previous setup. They started by configuring a Bosch Smart Home controller as the central hub, installing the Bosch Smart Home app (version 10.16.1) on an iPad Pro 12.9-inch tablet. Participants then connected a motion detector and linked an Alexa smart speaker using the Alexa app (version 2023.15), both pre-installed on the iPad. In order to assist with setup, login credentials were provided, and support was available if needed. On average, participants completed the setup in 18 minutes.

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

- *Participant Mental Model and Interview:* After setting up the smart homes using manufacturer applications, participants were invited to join a semi-structured interview, using the same questions as in the previous study.
- *Self-Efficacy:* In line with the last study, we utilized the CySESH questionnaire to assess participants' self-efficacy.
- *Motivation and Ability:* In order to evaluate the degree of user enjoyment in performing smart home configuration tasks, we employed the Task Evaluation Questionnaire extracted from the Intrinsic Motivation Inventory. In the context of our research, we adapted these questions to align with the specific nuances of smart home scenarios.
- *Informed Behavior:* We used the same set of six custom-designed questions as in the previous study to assess whether participants intended to engage in informed behavior based on their experiences.
- *User Experience:* User experience was assessed in the study using the UEQ+ questionnaire, which includes 26 items across six dimensions: *Attractiveness, Perspicuity, Efficiency, Dependability, Stimulation,* and *Novelty.*
- *2D-Setup:* In this stage of the study, participants engage with the 2D app, which guides them through a series of five tasks centered around smart home functionalities available in the market. The initial task serves as an introduction to the application. Subsequently, users encounter two straightforward tasks followed by two more challenging tasks, all randomly selected. The 2D app monitors user interactions to assess proficiency and includes a task-tracking functionality. Participants begin by scanning a designated QR code, which initiates an overlay prompting the entry of their subject ID. The task system assigns one task to the user at a time. The study director explains the essential features of the 2D app before participants begin. The app and assigned tasks are designed to equip participants with procedural knowledge of the processes and security configurations within smart home settings. On average, subjects took 15 minutes to complete the tasks with the 2D app.
- *Final Interview:* During the final interview, the interviewer posed four key questions to gather participants' insights and feedback on the 2D interface and its impact on their understanding of smart home systems. First, participants were asked if they could imagine using such

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

an app privately at home to gauge their interest in personal integration. To assess the educational value of the 2D app, the interviewer inquired whether participants better understood the processes in a smart home after using the interface. Subsequently, they were asked if their understanding of the various settings possible within a smart home system had improved following their interaction with the 2D prototype. Finally, participants were questioned about any differences they noticed in the design of privacy policies between the 2D prototype and existing manufacturer applications. When participants did not perceive any differences, the interviewer highlighted the distinctions. If differences were observed, participants were invited to share their opinions on the design of the one-pager privacy policy and to express their preference between this simplified design and traditional privacy policies, including their reasons.

Procedure The study began with an overview of the entire process, communicated orally and through written documentation to each participant. Informed consent was obtained prior to their involvement. Initially, participants provided demographic information and completed questionnaires assessing their comfort with technology and concerns regarding privacy. They then proceeded to physically set up real smart home devices, with careful observation of their interactions and challenges. Following setup, participants engaged in a drawing task to capture their experiences, followed by a semi-structured interview. After completing the device setup and initial interview, participants completed questionnaires covering self-efficacy, motivation, behavior, and user experience. They also launched 2D interface tasks designed to simulate the setup and configuration of smart home devices. Upon finishing these tasks, participants were asked to complete the same questionnaires again to evaluate any changes. Finally, a brief follow-up interview gathered their final reflections. This procedure facilitated an exploration of how the setup and interaction with smart home devices via a 2D interface influence user behavior. Figure 4.41 illustrates the study procedure.

Participants We employed a quota sampling strategy to assemble a cohort of participants meeting pre-established criteria. The primary objective of this recruitment methodology was to create a representative sample of individuals adept at using smart home devices. Participation in the study was strictly voluntary, and participants received a 30-euro compensation voucher for their involvement. The recruitment process involved a multi-faceted approach, utilizing mailing lists, engagement through social networks, and word-of-mouth referrals. The final study cohort comprised 27 participants,

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

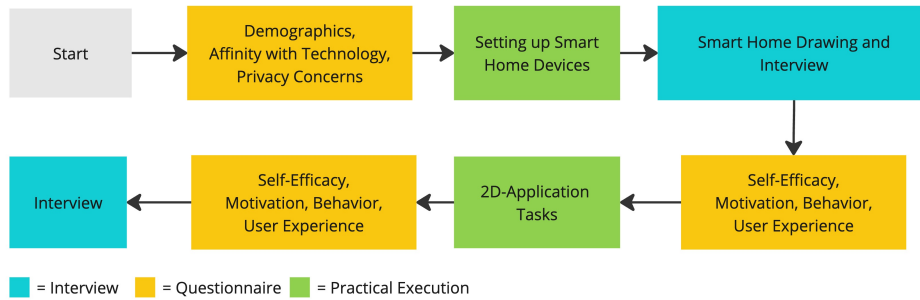


Figure 4.41: User Study Procedure

evenly split between 17 males and ten females. The average age of the participants was 25.63 years ($SD = 3.43$), with an age range from 20 to 35 years. Regarding their privacy or security background, 9 participants had an educational background, 2 had a professional background, and 16 had no background in the field. Figure 4.42 shows the comparison of the demographics of participants in the AR and 2D studies.

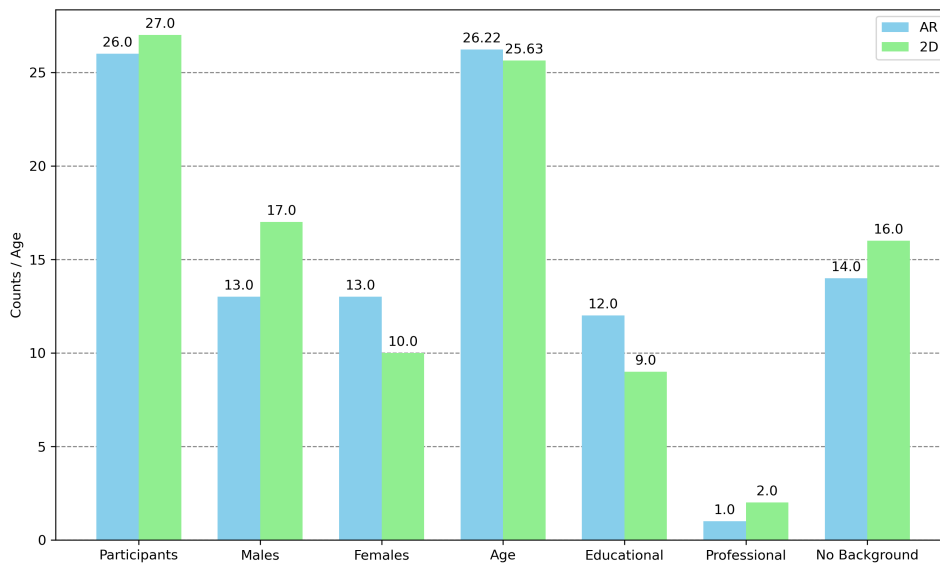


Figure 4.42: Participant demographics comparison: AR vs. 2D studies

Statistical and Qualitative Analyses In this study, we employed the same statistical and qualitative analysis methods as in the AR study to ensure consistency across the SH-Setup (initial configuration with manufacturer applications) and 2D-Setup (tasks using the 2D interface). To analyze quantitative data, we used paired t-tests on scales that were administered

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

twice, once after the SH-Setup and again following the 2D-Setup. An alpha level of 0.05 was applied for significance testing, and Cohen's *d* was calculated to assess effect sizes. The ATI and UIPC mean scores were computed to evaluate participants' privacy concerns across different dimensions.

The qualitative analysis mirrored that of the AR study, employing Mayring's qualitative content analysis for both the SH-Setup Interview and Final Interview phases. This method, which allows for inductive and deductive analysis, is particularly well-suited for mixed methods research. We first identified and organized relevant material to address the study's hypotheses, transforming participant responses into bullet points. Categorical themes were assigned to responses in Excel sheets, where frequencies were tracked. Following an inductive approach, categories were refined and consolidated to capture common themes and avoid duplication.

Empirical Findings

Experience and Knowledge In response to the inquiry, "How long have you been utilizing smart home systems?" four participants reported using them for less than a year, 17 participants indicated a usage period of one to four years, and six participants stated a usage duration exceeding four years. When queried, "How would you evaluate your familiarity with smart home privacy and security issues?" two individuals acknowledged having no knowledge, ten possessed basic knowledge, nine possessed intermediate knowledge, six claimed advanced knowledge, and none claimed expertise in this domain. Addressing the query, "How much concern do you have for the privacy and security of your own smart home?" participants displayed varying degrees of concern. Three respondents expressed no concern, eight held mild concern, 11 demonstrated moderate concern, four exhibited high concern, and two showed very high concern. In reaction to the prompt, "How do you assess your familiarity with smartphones?" most participants rated their smartphone knowledge favorably. Three participants possessed foundational knowledge; eight held intermediate knowledge; 12 claimed advanced knowledge and four professed expert knowledge. Participants were also asked about their ownership of smart home devices. Among the respondents, 25 participants owned at least one smart home device, while two reported not having any of their own.

Comparison To understand the differences in user characteristics between the AR and 2D studies, we compared the mean responses across key questions from both studies. For each question, we calculated the mean scores for participants in each condition, as illustrated in Figure 4.43.

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

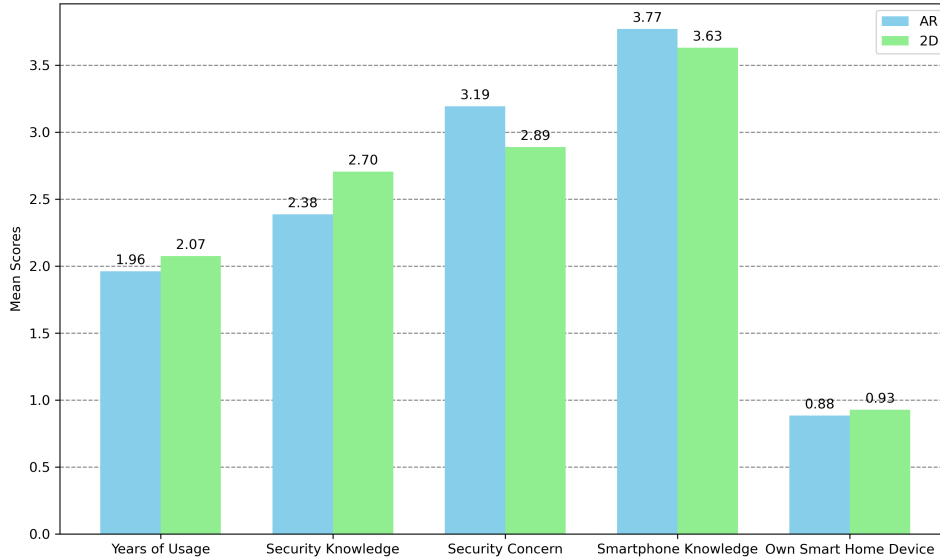


Figure 4.43: Participant experience and knowledge: AR vs. 2D setups

ATI Participants scored an average of 4.19 ($SD = 1.49$) on the ATI scale, reflecting a high level of technical affinity. The assessment also yielded a Cronbach’s α value of 0.90, confirming the reliability of the ATI scale’s results. This score is slightly lower compared to the AR study, where participants achieved an average of 4.48 ($SD = 0.66$).

Privacy Concerns The IUIPC scale, encompassing control, awareness, and unauthorized secondary use, delivers an average score of 6.04 ($SD = 1.38$), with a Cronbach’s α of 0.89. The IUIPC dimensions and context-specific factors (Trusting Beliefs and Risk Beliefs) scores are detailed in Table 4.20. A Pearson correlation coefficient analysis was performed to evaluate the linear relationship between the mean score of the IUIPC and Trusting Beliefs and Risk Beliefs. However, no significant correlations were detected.

Table 4.20: IUIPC Dimensions and Context-Specific Factors Scores

| | Cronbach’s α | Mean | Std. Deviation |
|----------------------------|---------------------|------|----------------|
| Control | 0.69 | 5.91 | 1.32 |
| Awareness | 0.76 | 5.90 | 1.23 |
| Unauthorized Secondary Use | 0.88 | 6.24 | 1.50 |
| Trusting Beliefs | 0.86 | 3.54 | 1.81 |
| Risk Beliefs | 0.65 | 4.90 | 1.41 |

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

Comparison The AR and 2D studies have similar IUIPC scores. Both studies show comparable average scores in the Control and Awareness dimensions, with mean values around 5.6 to 6.0. However, the 2D study participants demonstrated slightly higher overall averages in both the Unauthorized Secondary Use and Risk Beliefs dimensions, while Trusting Beliefs scores were relatively close (see Figure 4.44). Neither study found significant correlations between IUIPC and the context-specific factors.

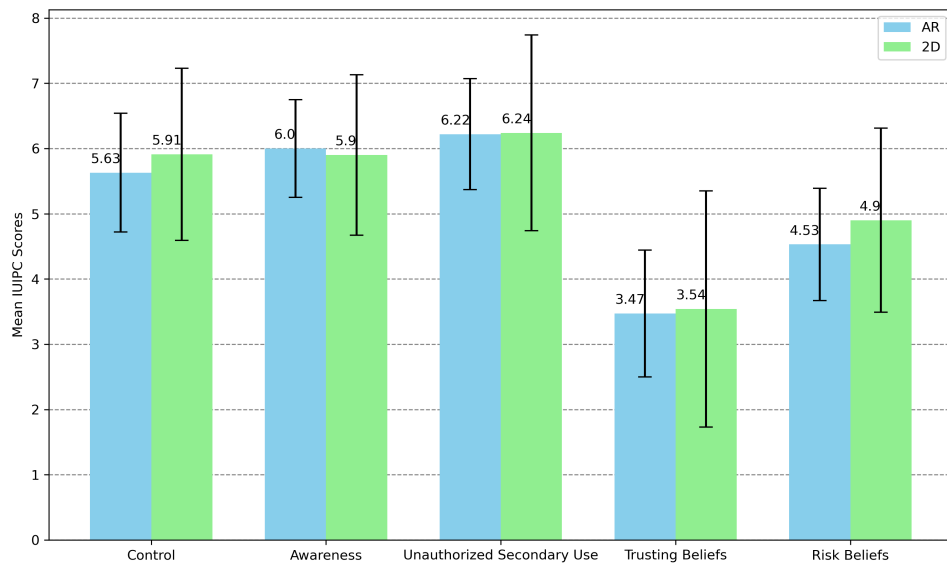


Figure 4.44: Participant IUIPC Comparison: AR vs. 2D studies

Participant Mental Model: Sketching Task After setting up smart homes using the manufacturer applications, participants were asked to illustrate their understanding of the smart home system by sketching their setup on paper. These initial drawings were then analyzed to interpret participants' mental models, with a specific focus on their representation of data flow among the smart home network components. For sketches with unclear elements, such as understanding data exchanges between Bosch and Amazon indicated by a cloud icon, we referenced interview transcripts and participants' comments for clarification. Figure 4.45 provides a visual representation of the accurate data flow within the smart home system as intended for this part of the study.

Consistent with the previous study, participants' sketches were classified into two categories: extended models, which included technical components like routers, and simplified models, focusing solely on primary smart home devices and their connections. Figure 4.46 showcases two example sketches.

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

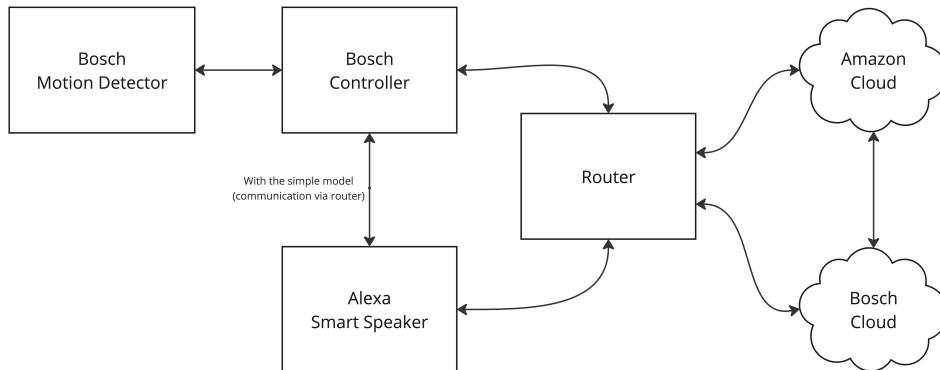


Figure 4.45: The Accurate Data flow model of the SH-Setup

In order to gain deeper insights into participants' mental models, we evaluated whether all local elements were accurately represented and identified any errors or omissions in their connections to specific device components. Additionally, we assessed the extent to which participants recognized third-party cloud services and understood the data exchange processes between these providers. The results are detailed in Table 4.21.

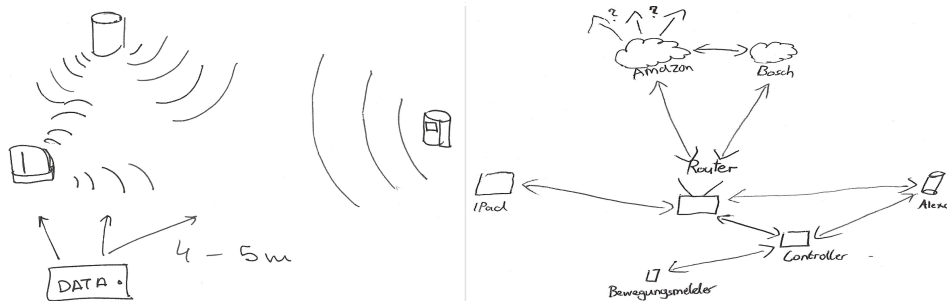


Figure 4.46: Sample sketches from the participants: Simple model on the left, extended model on the right.

Comparison In comparing the results of participant drawings between the AR and 2D studies, key differences emerge in the complexity and accuracy of representations. In the AR study, participants were more evenly split between simple and extended models, with 13 participants using a simple model (including technical elements like routers) and 12 using an extended model focused on primary smart home devices. Conversely, the 2D study showed a stronger preference for extended models, with 25 participants opting for this approach, and only 2 participants used simple models.

Regarding the inclusion of all entities (Alexa, motion detector, controller,

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

Table 4.21: Results of the Participant Drawings

| Overall | Description | Number |
|-----------------------------|--|--------|
| Simple model | Including technical elements like routers | 2 |
| Extended model | Main smart home devices and their connections in focus | 25 |
| Contain all entities | Consider all entities (Alexa, motion detector, controller, and router) | 23 |
| Correct data flow | The data flow is correctly drawn | 3 |
| Incorrect data flow | The data flow is incorrectly drawn | 24 |
| Mistakes | Description | Number |
| Alexa | Connections from/to the Alexa to the entities are drawn incorrectly | 14 |
| Motion Detector | Connections from/to the motion detector to the entities are drawn incorrectly | 14 |
| Bosch Controller | Connections from/to the Bosch controller to the entities are drawn incorrectly | 12 |
| Router not considered | The router is not observed and drawn | 5 |
| Router connection incorrect | The connection to the router is drawn incorrectly | 2 |
| Clouds | Description | Number |
| Observing clouds | Draw the clouds of the providers as well | 15 |
| Data flow between clouds | Establish a connection between the clouds of the providers | 4 |

and router), 23 participants in the 2D study managed to incorporate all entities, whereas only 10 participants did so in the AR study. However, accuracy in depicting data flow was relatively low in both studies, with only 8 participants in the AR study drawing correct data flows, compared to 3 in the 2D study. Common mistakes were also observed, particularly with incorrectly drawn connections for Alexa and the motion detector, as well as incomplete or incorrect router representation. Notably, in the AR study, 9 participants struggled with Alexa connections, whereas in the 2D study, 14 participants made similar mistakes. Additionally, observing provider clouds was common across both studies, with 18 participants in the AR study and 15 in the 2D study, including these in their drawings. Overall, the AR study participants tended toward simpler models with fewer complete entities, while the 2D study encouraged more comprehensive, though not necessarily accurate, representations. See Figure 4.47 for more details.

Participant Mental Model: Interview Similar to the AR study, we employed select questions by Tabassum et al. (2019) to explore participants' conceptual understanding of essential security and data practices in smart homes. Participants were asked about different aspects of data management, including collection, storage, and sharing, as well as their security behaviors and privacy preferences. The interview questions were carefully assessed using the Mayring method explained earlier in this work.

- *Data Collection:* In the analysis of data collection practices, participants provided insights into the types of data gathered by different devices, specifically motion sensors and voice assistants. The feedback covered what data was collected, participants' opinions on whether it should be collected, and perceptions of the necessity for data collection in

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

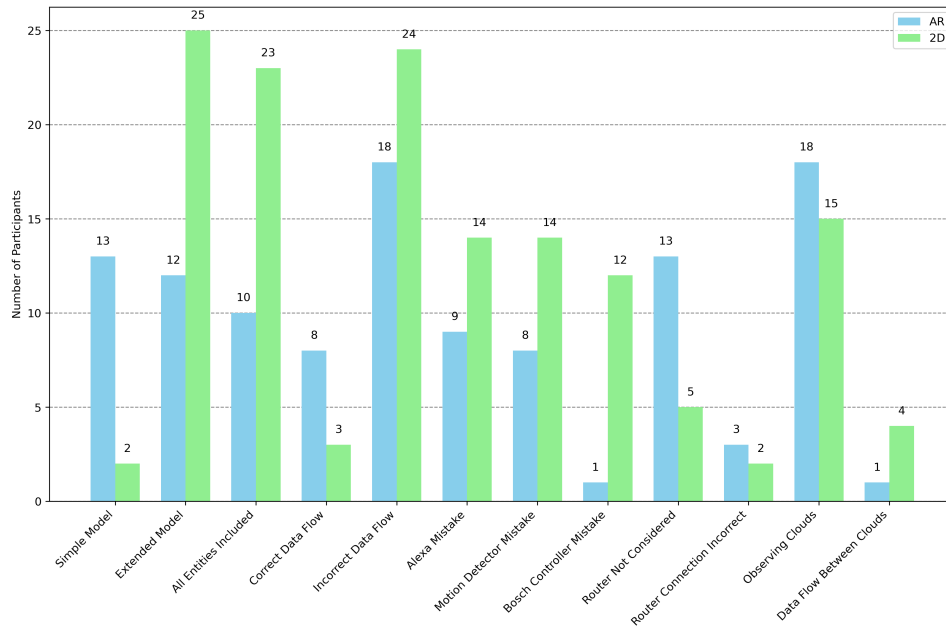


Figure 4.47: Comparison of participant drawings in AR and 2D studies

supporting device functionality. For motion sensors, 27 participants recognized the collection of movement data and activation timestamps. Participant Id1327 noted, “The motion sensor collects data whenever there’s movement, capturing details like the exact time something is triggered.” This functional data collection was generally accepted, with 15 participants supporting it as necessary for motion detection. Id1363 emphasized, “The motion sensor should detect movement as it’s designed to do. So, yes, it should collect data whenever activated.” Nonetheless, privacy was a concern for some, as Id1452 commented, “For basic operation, yes, but not if it involves unnecessary personal data.” Regarding necessity, 8 participants linked data collection to security purposes, like theft prevention; Id2660 stated, “For something like theft prevention, constant data collection may be essential.”

In terms of voice assistants, 26 participants noted that audio data, including commands and ambient conversations, is regularly collected. Id1363 observed, “Alexa records voice data when active, capturing not only what’s said but who says it and possibly even when.” Opinions were mixed on whether this data should be collected, with 15 participants expressing conditional support. Id3408 suggested, “Voice data should be recorded to understand commands, but anything more, like private discussions, feels intrusive.” In contrast, Id3534 argued for the

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

necessity of data collection, “For Alexa to improve its responses, it needs data.” Finally, 4 participants valued the personalization benefits, as Id7988 highlighted, “Alexa’s data collection helps refine responses, especially with personalized features.”

- *Data Storage:* Participants expressed a pragmatic view on data storage practices, noting that device data is likely transmitted to cloud servers or company systems, with 25 participants mentioning data is typically sent to the cloud or the manufacturer’s servers. Id1327 commented, “to the controller, then to the cloud or a server,” while Id1363 noted, “Data goes to the manufacturer, yes.”

Regarding storage location and duration, all participants speculated that data is retained long-term, with Id1363 suggesting “on company servers, possibly for up to ten years” and Id1452 estimating “five to six years on the server with a device-linked ID.” When asked about accessing stored data, 26 participants believed data requests were possible but often complex. Id1327 remarked, “One can request data, but it involves effort,” and Id1363 observed, “Usually on support pages where data can be requested.”

Regarding control, all participants indicated limited influence over stored data, with Id1363 adding, “One can delete it theoretically, but verifying deletion isn’t easy,” while Id1452 shared, “I assume I have some access rights, but I can’t confirm the data is erased.”

Finally, regarding deletion, 26 participants expressed skepticism about whether deletions were fully effective. Id1327 commented, “Deletion is possible, but knowing it’s fully erased is uncertain,” and Id1363 expressed doubts, “We rely on them to delete it properly.” Few participants had personally pursued deletion, though Id1452 noted, “I haven’t tried, but I might if I was concerned about privacy.” Overall, participants voiced a strong desire for more transparent and accessible control over their stored data, reflecting both an awareness of data handling practices and concerns for data privacy.

- *Data Sharing:* Participants generally assumed that data sharing occurs for profit-driven reasons, with many expressing doubts about the direct benefits for users. While there was some acknowledgment of potential product improvements, most participants conveyed a strong concern about privacy and the potential for companies to misuse personal data for financial gain. When asked whether device manufacturers share data with other companies, all participants responded, often assuming

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

that companies share data for profit or partnerships. Id1327 stated, “Of course, companies and organizations receive the data,” while Id1363 noted, “They share data with Amazon and possibly sell it further to advertisers.” Some participants, like Id1452, thought that data might also go to consumer organizations or other corporations for commercial insights and sharing, “data could go to consumer centers and companies that profit from user information, especially regarding purchase behavior.” In discussing the reasons and benefits of data sharing, all participants expressed skepticism about who truly benefits from this practice, with many seeing it primarily as a revenue source for companies. Id1327 observed, “They earn some money from it. For instance, insurance companies might pay for it, or for security product promotions.” Others, like Id1363, noted, “Companies make money from selling data, perhaps to create a profile for targeted advertising.” While some, such as Id1452, saw potential benefits for product improvement, they still expressed concerns about data privacy and commercialization: “It’s fine if data is used to improve products, but selling it carries risks and favors company profits.”

- *Security Behaviors:* Participants expressed varied experiences regarding their ability to control stored data, often highlighting both limitations in existing options and the challenges involved in accessing or managing data collected by smart devices. When asked whether they felt they had control over their data, all responded frequently, noting that while control is theoretically possible, the actual execution is often difficult. Id1327 shared, “I think you can ask companies about files, but it takes effort,” which underscores the perceived complexity and effort required to obtain or control personal data. Similarly, Id1363 reflected on data deletion options, stating, “You can delete it theoretically, but trusting it’s fully gone is difficult,” pointing to a lack of confidence in companies’ data management practices and the transparency of deletion processes.

Participants also highlighted a sense of uncertainty about their rights and the effectiveness of control mechanisms. For instance, Id1452 mentioned, “I assume I have some access rights, but confirming data erasure isn’t easy,” which captures the skepticism many expressed regarding the actual influence they have over personal data. This perceived lack of control and trust in data handling reflects participants’ frustrations with privacy management in the context of connected devices, showing a clear need for more straightforward and reliable control options.

- *Privacy Preferences:* In addition to concerns over control, participants expressed a strong desire for enhanced privacy features that would allow for more personalized and transparent management of their data. Twenty-six participants shared that current privacy controls are often overly complex or difficult to apply effectively. For example, Id1327 remarked, “You can disable certain options, but it may require effort,” indicating that even basic privacy settings might require significant time and effort to manage. Some participants saw a lack of straightforward privacy options as a barrier to data security, with Id1452 suggesting that avoiding specific devices might be the simplest solution: “Not using certain devices might be the best control we have.”

Participants voiced clear preferences for more granular, device-specific controls. Id1327 recommended settings that “allow you to specify what data is sent and when,” envisioning a user-friendly approach where users could directly manage data sharing frequency and detail level. Additionally, Id1452 highlighted the potential benefits of real-time monitoring, proposing that “It would be helpful to see what data is collected and deleted selectively,” which would give users a proactive role in managing their data privacy. Furthermore, Id1363 expressed a preference for device-level customization, stating, “Each device should have tailored options for how much data it shares,” reflecting participants’ desire for privacy controls that align with the unique functions and risks associated with each device.

Comparison In comparing the AR and 2D studies, participants across both setups showed a foundational understanding of primary data collection by smart home devices yet limited awareness of secondary or inference-based data gathering. Participants were aware that data was stored on company servers but expressed uncertainty regarding exact storage locations, retention, and deletion processes, often doubting their ability to access or control their data. Data sharing was commonly perceived as profit-driven, with concerns about limited user benefits and potential misuse of personal information. Despite similar privacy preferences across both studies, participants voiced frustrations over complex data management processes, desiring more transparent, device-specific control options and real-time data monitoring to better manage their privacy.

Self-Efficacy Employing a paired sample t-test, we evaluated the variations in mean scores derived from the self-efficacy questionnaires. Our analysis unveiled a noteworthy and statistically significant elevation ($t(26) = -8.2$, $p < .001$, $Cohen'sd = -1.58$) in the mean score among participants who

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

engaged with the 2D-Setup ($M = 5.82$, $SD = 1.41$) when contrasted with those who interacted with the SH-Setup ($M = 4.33$, $SD = 1.73$).

Comparison The results of the AR and 2D studies showed significant increases in self-efficacy compared to the SH-Setup. In the AR study, mean self-efficacy scores rose from 3.66 to 5.52, and in the 2D study, scores increased from 4.33 to 5.82. Both improvements were statistically significant with strong effect sizes, indicating enhanced self-efficacy in both setups, with slightly higher scores in the 2D-Setup.

Motivation and Ability Reported findings reveal significant shifts across all subdomains of the IMI questionnaires, including *Interest/Enjoyment*, *Perceived Competence*, *Perceived Choice*, and *Pressure/Tension*. Results from paired sample t-tests highlight a noteworthy increase in mean scores among participants utilizing the 2D-Setup versus the SH-Setup, as illustrated in Table 4.22. Notably, participants reported significantly heightened interest and enjoyment, greater perceived competence, increased sense of choice, and reduced stress and pressure when engaging with tasks through the 2D-Setup.

Table 4.22: IMI Questionnaire Results and Paired T-Test Comparisons

| | SH-Setup | | 2D-Setup | | t-test | | | |
|----------------------|----------|----------------|----------|----------------|--------|----|--------|-----------|
| | Mean | Std. Deviation | Mean | Std. Deviation | t | df | p | Cohen's d |
| Interest/Enjoyment | 4.32 | 1.70 | 5.57 | 1.32 | -5.83 | 26 | < .001 | -1.12 |
| Perceived Competence | 4.71 | 1.55 | 5.61 | 1.25 | -4.20 | 26 | < .001 | -0.81 |
| Perceived Choice | 4.93 | 1.64 | 5.35 | 1.64 | -2.42 | 26 | 0.023 | -0.47 |
| Pressure/Tension | 2.93 | 1.61 | 2.18 | 1.47 | 3.23 | 26 | 0.003 | 0.62 |

Comparison The Intrinsic Motivation Inventory questionnaire revealed significant variations in participants' motivation and ability within the four subdomains of *Interest/Enjoyment*, *Perceived Competence*, *Perceived Choice*, and *Pressure/Tension* for both the AR and 2D studies.

Informed Behavior The Informed Behavior scales assessed respondents through six questions. Upon examining the total scores, notable distinctions surfaced between the SH-Setup and 2D-Setup conditions. Specifically, question 2 focuses on avoiding services that request personal information, question 3 addresses changing the default settings of smart home apps to enhance data security, and question 5 pertains to preferring local networks over cloud-based services (see Table 4.23 for further elucidation).

Comparison In the AR and 2D studies, participants demonstrated improved informed behavior scores across six key questions following interactions with either the AR or 2D Setups compared to the SH-Setup. Significant improvements were noted in both setups for Question 1 ("Would you avoid

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

Table 4.23: Informed Behavior Results and Paired T-Test Comparisons

| | SH-Setup | | 2D-Setup | | t-test | | | | |
|------------|----------|----------------|----------|----------------|--------|----|--------|-----------|--|
| | Mean | Std. Deviation | Mean | Std. Deviation | t | df | p | Cohen's d | |
| Question 1 | 2.74 | 0.98 | 3.81 | 1.00 | -6.03 | 26 | < .001 | -1.17 | |
| Question 2 | 2.30 | 1.20 | 2.41 | 1.08 | -0.49 | 26 | 0.631 | -0.09 | |
| Question 3 | 4.04 | 1.06 | 4.30 | 0.87 | -1.66 | 26 | 0.110 | -0.32 | |
| Question 4 | 3.07 | 1.38 | 3.81 | 1.18 | -3.76 | 26 | < .001 | -0.72 | |
| Question 5 | 2.96 | 1.32 | 3.19 | 1.27 | -1.00 | 26 | 0.327 | -0.19 | |
| Question 6 | 3.48 | 1.09 | 4.15 | 0.72 | -3.95 | 26 | < .001 | -0.76 | |
| Overall | 3.10 | 0.86 | 3.61 | 0.66 | -5.02 | 26 | < .001 | -0.97 | |

services requiring personal information?”), where scores rose from 2.50 to 3.81 in AR and from 2.74 to 3.81 in 2D, indicating heightened privacy awareness. Similarly, Question 4, which asks about checking privacy policies, showed positive change, increasing from 3.07 to 3.81 in AR and from 3.12 to 3.96 in 2D, with statistically significant effects.

Both setups had non-significant changes in Questions 2 and 5, focused on avoiding services requiring personal information and preferring local over cloud-based services. However, the overall trend highlights that both AR and 2D interfaces facilitated more informed behavior. The overall mean scores increased notably (AR: 3.10 to 3.61; 2D: 3.00 to 3.51), underscoring the positive influence of both interfaces on users' informed security behaviors.

Model Testing Our analysis investigated the influence of self-efficacy on smart home users' informed behavior through Motivation and Ability, comparing conceptual and procedural knowledge scenarios. In the suggested model, Motivation is conceptualized as a synthesis of four key components: *Interest/Enjoyment*, *Perceived Competence*, *Perceived Choice*, and *Pressure/Tension*, with Ability representing *Perceived Competence*. For each construct, Cronbach's α coefficients were computed to assess the internal consistency of the questionnaire items. Table 4.24 summarizes these findings, illuminating the coherence within our measurement instrument. Prior studies have emphasized the significance of achieving a minimum Cronbach's α threshold of 0.7 to ensure the reliability of item sets.

Table 4.24: Cronbach's α Coefficient scores of the questionnaires

| | Self-Efficacy | Motivation | Ability | Behavior |
|----------|---------------|------------|---------|----------|
| SH-Setup | 0.84 | 0.76 | 0.87 | 0.84 |
| 2D-Setup | 0.85 | 0.63 | 0.87 | 0.72 |

We explored the interrelationships among Self-Efficacy, Motivation, Ability, and Informed Behavior across both the SH-Setup and 2D-Setup versions.

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

In the SH-Setup version, Self-Efficacy and Ability are significantly correlated with a p-value of 0.029 and a Pearson's r-value of 0.42, indicating a moderate positive relationship between these variables. In the 2D-Setup version, several correlations were observed. Firstly, Self-Efficacy exhibited a robust association with Motivation ($r(25) = 0.548, p = 0.003$), underscoring that individuals with higher self-efficacy tend to demonstrate stronger motivational tendencies. Secondly, the relationship between Self-Efficacy and Ability was also significant ($r(25) = 0.395, p = 0.042$), suggesting that individuals who perceive themselves as capable are more likely to leverage their skills effectively. Moreover, Motivation itself showed a positive correlation with Informed Behavior ($r(25) = 0.463, p = 0.015$), implying that individuals with higher motivation levels are more inclined towards informed decision-making. Lastly, the correlation between Ability and Informed Behavior ($r(25) = 0.493, p = 0.009$) further substantiates that individuals with greater abilities are more likely to engage in informed behaviors.

The R-squared values, representing the proportion of variance in one variable that is predictable from another, were calculated for these significant correlations. For the SH-Setup version, the R-squared value for the correlation between Self-Efficacy and Informed Behavior was 0.146, indicating that approximately 14.6% of the variance in Informed Behavior can be explained by Self-Efficacy. In the 2D-Setup version of our analysis, the R-squared values for significant correlations provide insight into the predictive relationships between variables. Self-Efficacy explains 30.1% of the variance in Motivation ($R^2 = 0.301$), indicating its substantial role in influencing motivational levels. Similarly, Self-Efficacy accounts for 15.6% of the variability in Ability ($R^2 = 0.156$), underscoring its moderate impact on perceived capability. Moreover, Motivation explains 21.3% of the variance in Informed Behavior ($R^2 = 0.213$), suggesting that individuals with higher motivational levels are more likely to engage in informed decision-making processes. Lastly, Ability explains 24.3% of the variance in Informed Behavior ($R^2 = 0.243$), highlighting the importance of skills and capabilities in facilitating informed behaviors (see Figure 4.48).

Comparison Model testing in the AR and 2D studies examined how self-efficacy influenced participants' informed behaviors, particularly through procedural and conceptual knowledge contexts. For the AR-Setup, self-efficacy significantly impacted motivation and ability, explaining 24.6% of the variance in motivation and 33.2% in ability. Motivation and ability then accounted for 18.3% and 20.7% of the variance in informed behavior, respectively, underscoring the AR-Setup's effectiveness in promoting engaged,

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

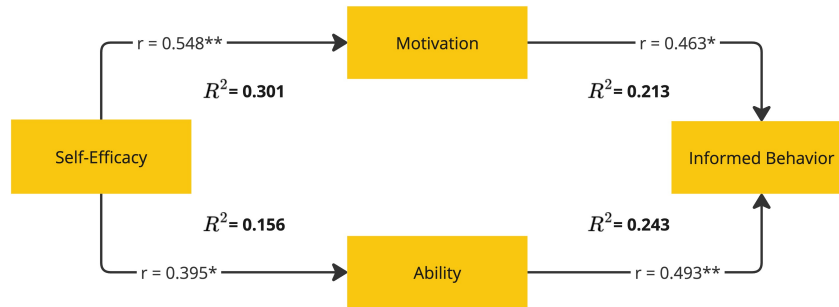


Figure 4.48: Relationships between Self-Efficacy, Motivation, Competence, and Informed Behavior in procedural knowledge, with arrows indicating direction and R-squared values representing variance explained.

informed user behavior. In the 2D-Setup, self-efficacy similarly influenced motivation and ability, explaining 30.1% and 15.6% of their variances, respectively. Here, motivation and ability contributed to 21.3% and 24.3% of the variance in informed behavior, affirming the predictive role of these factors on user behavior. At the same time, both setups indicate self-efficacy's critical role in shaping motivation, ability, and informed behaviors; the AR-Setup slightly outperformed in overall predictive strength.

User Experience The UEQ scores, which range from -3 to +3, serve as pivotal indicators of user experience across dimensions such as Attractiveness, Perspicuity, Efficiency, Dependability, Stimulation, and Novelty. In this study, we analyzed these dimensions for both SH-Setup and 2D-Setup configurations. Mean scores and standard deviations for each setup are presented in Table 4.25, along with results from paired t-tests that assess the statistical significance of differences between the setups. Our findings reveal robust distinctions in user perceptions across all dimensions ($p < .001$), with Cohen's d effect sizes indicating moderate to large practical differences. These results underscore the significant impact of 2D-setup configuration on user experience, influencing factors such as interface appeal, clarity of use, operational efficiency, reliability, stimulation, and perceived novelty. Figure 4.49 visually presents the UEQ benchmarks for both the SH-Setup and 2D-Setup, providing a comprehensive overview of the comparative performance.

Comparison The User Experience Questionnaire reveal that AR-Setup and 2D-Setup configurations significantly enhanced user experience compared to the SH-Setup across the core dimensions of Attractiveness, Efficiency, Dependability, Stimulation, and Novelty. For both setups, the highest scores were observed in Attractiveness and Efficiency, with users finding these

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

Table 4.25: UEQ Results and Paired T-Test Comparisons

| | SH-Setup | | 2D-Setup | | t-test | | | |
|----------------|----------|----------------|----------|----------------|--------|----|--------|-----------|
| | Mean | Std. Deviation | Mean | Std. Deviation | t | df | p | Cohen's d |
| Attractiveness | 0.50 | 1.02 | 1.85 | 0.73 | -6.48 | 26 | < .001 | -1.25 |
| Perspiciuity | 0.89 | 1.25 | 2.16 | 0.70 | -4.59 | 26 | < .001 | -0.88 |
| Efficiency | 0.81 | 1.12 | 2.31 | 0.59 | -6.40 | 26 | < .001 | -1.23 |
| Dependability | 0.44 | 1.01 | 1.84 | 0.79 | -5.77 | 26 | < .001 | -1.11 |
| Stimulation | 0.37 | 1.07 | 1.82 | 0.88 | -6.81 | 26 | < .001 | -1.31 |
| Novelty | 0.11 | 1.19 | 1.54 | 0.71 | -5.14 | 26 | < .001 | -0.99 |

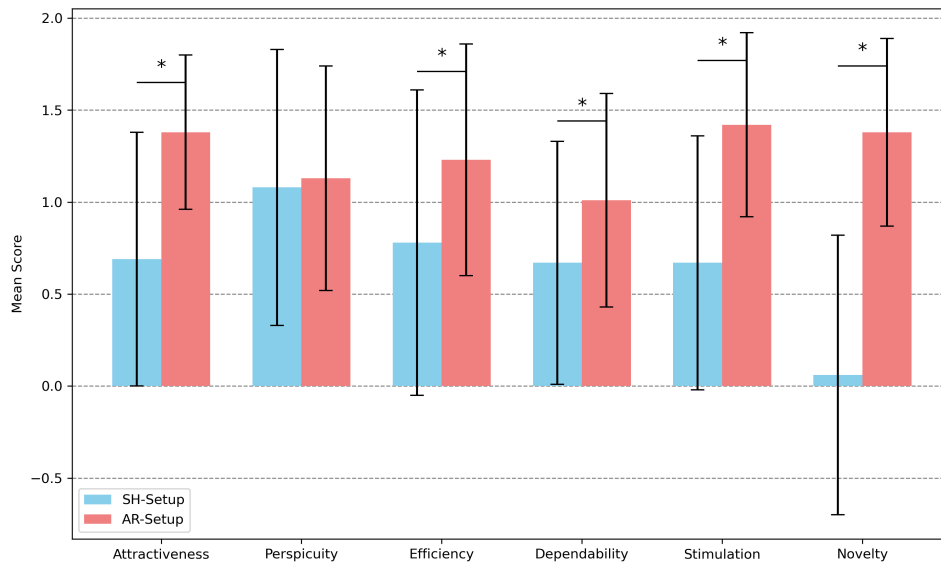


Figure 4.49: UEQ Comparison benchmarks for SH-Setup and 2D-Setup

configurations more engaging and efficient than the standard setup.

In the AR-Setup, Attractiveness, Efficiency, and Stimulation showed notable improvements, with mean scores indicating increased interest, perceived enjoyment, and operational ease. Dependability also scored higher in the AR-Setup, suggesting that users felt a greater sense of control and reliability during the interaction. However, Perspiciuity improvements were modest, indicating only a slight enhancement in user clarity of the interface.

In the 2D-Setup, the user experience scores also demonstrated strong gains. Attractiveness and Efficiency improvements were even more pronounced than in the AR-Setup, as the 2D-Setup received higher mean scores across these dimensions. Additionally, Dependability, Stimulation, and Novelty scored significantly higher in the 2D-Setup, suggesting that users positively received the 2D interface's clarity, engagement, and innovativeness. Unlike in the AR-Setup, Perspiciuity reached statistical significance, indicating clearer guidance in using the 2D interface.

Final Interview During the final interview, participants were presented with four key questions designed to gather their insights and feedback on the 2D interface and its impact on their understanding of smart home systems. These questions aimed to evaluate the participants' willingness to use such an app privately at home, assess their enhanced comprehension of smart home processes and settings after interacting with the 2D prototype, and identify any perceived differences in privacy policies between the prototype and existing manufacturer applications.

- *Private Usage of the App at Home:* Most participants expressed a strong willingness to adopt the app in their private home settings, with 21 participants confirming they would use it and 6 showing potential interest. Many cited the app's ability to enhance transparency and control over their devices as a primary attraction, with several viewing it as a valuable tool for managing connected technology. For instance, participant Id1327 enthusiastically remarked, "Yes, definitely," emphasizing the app's usefulness in centralizing device management in one place. Similarly, participant Id3408 appreciated the app's "significantly more transparent overview," suggesting that its structure clarified previously hidden or complex device interactions. Others, like participant Id7856, highlighted the enjoyment factor, describing the app as "cool" for providing a "nice overview" of which devices are connected and how they interact. Participant Id6957 specifically noted that the app's potential for giving an integrated view across multiple devices addressed a real need, something that traditional setups often fail to do. Notably, no participant explicitly declined private use, underscoring the app's perceived value and accessibility among users.
- *Understanding of Smart Home Processes:* The responses indicate that the 2D prototype was largely effective in helping participants better understand the data flow and interactions between devices within a smart home environment. Many participants appreciated how the app visually simplified otherwise complex processes, turning abstract interactions into something tangible. Participant Id1363 expressed that the app provided clearer insights into how devices exchange data, saying, "Yes, definitely," which suggests that the visual clarity was instrumental in demystifying these interactions. Similarly, participant Id8734 noted that they gained "an understanding of how data is shared," which illustrates the prototype's strength in revealing hidden or misunderstood aspects of device communication. Participant Id3327 added that they felt "a little" more informed, highlighting that even a moderate increase

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

in clarity made the smart home setup more accessible. However, the prototype's impact varied depending on participants' prior knowledge or expectations. For instance, participant Id3452 mentioned that they gained "a little" insight, enough to appreciate the interconnection of devices without feeling fully informed. Conversely, participant Id3774 found the improvement limited, describing their understanding as "more or less" enhanced. This suggests that, while the app effectively improved many participants' understanding, those with previous smart home experience may have required a more in-depth demonstration to meet their expectations completely.

- *Understanding of Smart Home Settings:* The 2D prototype appears to have significantly improved participants' understanding of customization options within a smart home system, providing them with a clearer sense of how they could adjust settings to control their environment. Among the participants, 17 confirmed that their understanding was enhanced, while 2 reported partial improvement, 3 saw no improvement, and 5 offered no response. For example, participant Id6957 expressed a positive shift, saying, "In general, I would say yes," indicating that the app broadened their grasp of adjustable features. Participant Id3327 echoed this, noting that the prototype helped them achieve "definitely a bit more" knowledge, suggesting that the interactive demonstration provided a hands-on learning experience, which made the options more memorable and practical.

Some participants offered specific examples of settings they appreciated, such as participant Id3408, who mentioned the app's "ability to adjust security features quickly," emphasizing the appeal of having security settings readily accessible for immediate adjustment. This feature resonated well with many, as it illustrated the app's potential to simplify configuration tasks. Participant Id7856 reinforced this sentiment with an enthusiastic "Yes, definitely," underscoring the app's effectiveness in clarifying how customization works.

While the majority found the prototype beneficial, there were a few participants who felt the insights gained were limited. For instance, Id7799 mentioned that they "did not discover so much more" compared to their existing knowledge, suggesting that prior familiarity with smart home customization influenced how much value the app added for them. This feedback highlights the app's effectiveness in educating users with less experience, while also suggesting opportunities for additional depth or advanced features to cater to more knowledgeable users.

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

- *One-Pager Privacy Policy*: Participants provided thoughtful feedback on the differences between the 2D prototype’s privacy statement and those commonly found in standard manufacturer applications, with 18 participants responding. A strong preference emerged for the prototype’s clear and concise format, as it was widely viewed as more accessible and user-friendly than typical lengthy, complex privacy statements. Participant Id1452 appreciated the prototype’s brevity, describing it as “a bit shorter,” which they found made it much easier to engage with than the dense statements they were accustomed to. Similarly, participant 7856 pointed out that the Bosch privacy policy, for instance, was “somehow 25 pages,” emphasizing that the prototype’s simplified structure reduced the effort required to understand the content, making it feel more approachable. This perspective was echoed by participant Id3824, who noted that typical privacy statements tend to be overly detailed and technical, which can make them difficult for the average user to follow.

While many favored the prototype’s streamlined approach, a few participants admitted they had not engaged closely with the content. For example, participant Id5320 mentioned they “didn’t really notice any big differences,” possibly reflecting a sense of familiarity or indifference toward privacy statements in general. Participant Id8712 similarly remarked that they had not paid close attention to specific terms and conditions, indicating a common reluctance to read through complex legal language. These responses underscore that participants are more likely to read and understand privacy information when it is presented in a straightforward, accessible manner, as seen in the prototype.

Comparison In comparing the AR and 2D studies, both prototypes improved participants’ understanding of smart home settings and increased engagement with privacy statements, but the AR format had a notably stronger impact. In the 2D study, 17 participants reported enhanced comprehension of settings, with a particular appreciation for security adjustment options, though 3 saw no improvement, and two felt only partially informed. By contrast, the AR study resulted in 24 participants affirming a clear understanding, with nine specifically noting improved clarity of settings and 5 gaining a broader awareness of options, suggesting that AR’s immersive quality provided a deeper learning experience. For privacy, both groups preferred simplified formats over conventional policies. However, in the 2D study, 18 participants favored the concise privacy statement for its clarity.

In contrast, in the AR study, all 20 respondents preferred the one-pager

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

format with bullet points, icons, and color-coded sections, which made it more readable and memorable. Furthermore, 9 participants in the AR study indicated they would be more likely to read privacy policies in this format, and two felt it offered greater control over their data. The AR study's structured, visual presentation style proved particularly effective, creating a more engaging and user-friendly experience in understanding and privacy perceptions.

Discussion and Limitations

This study examined how a 2D interface impacts users' self-efficacy, motivation, and informed behavior in managing smart home security settings, replicating the core aims of an earlier study that utilized augmented reality for the same purpose. Both studies intended to elevate procedural knowledge and user engagement through distinct interaction modalities. By providing a structured 2D interface, this study aimed to present complex security tasks in an accessible format, facilitating an understanding of data flow among smart home devices.

Participants in this study had varied levels of familiarity with smart home privacy and security, which played a foundational role in shaping their mental models and informed behaviors. Experience with smart home systems and self-assessed knowledge of privacy issues provided helpful context for understanding how users approached privacy management within the 2D setup. The ATI scores indicated a high overall comfort with technology among participants. This technological affinity likely supported their engagement with new technologies. However, high ATI scores alone do not imply an inherent understanding of security complexities in smart home systems.

Privacy concerns measured by IUIPC, particularly in dimensions of control, awareness, and unauthorized secondary use, showed moderate to high privacy concerns among users, with elevated scores in unauthorized data use and risk beliefs. These findings indicate that while users were generally aware of potential risks in data sharing, they may have lacked a nuanced understanding of how to exercise control over security settings within a smart home ecosystem. Interviews revealed that many participants possessed only surface-level knowledge of smart home data flow and expressed concerns about device interactions with third-party providers. Nevertheless, they felt uncertain about how to manage these concerns actively. This background highlights that users' initial privacy concerns, shaped by general experience rather than specific knowledge, left them with fragmented mental models of smart home privacy controls (Tabassum et al., 2019).

The drawing task and initial interview further illuminated gaps in partic-

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

ipants' conceptual understanding of smart home data management. Many sketches featured incomplete models that either lacked third-party elements or inaccurately represented device interactions, suggesting that users perceived individual devices as discrete entities rather than parts of a networked system. Participants often depicted only primary device interactions (e.g., Alexa and Bosch controllers) but omitted or misrepresented data flow, cloud connections, and inter-device communication, indicating an insufficiency of understanding of the ecosystem. In interviews, users expressed inadequate assumptions about data collection but lacked awareness of secondary or inference data collection, especially about third-party data exchanges. This suggests that, despite comfort with technology, their mental models did not initially encompass the interconnected and often complex data flows typical in smart homes (Marky et al., 2022).

This study employed the theoretical model from the previous one that integrated the Fogg Behavior Model and self-efficacy to predict and shape informed user behavior in smart home privacy management. While Technology Threat Avoidance Theory served as a backbone for the study, framing users' behaviors in terms of threat appraisal and avoidance, the primary focus lay on enhancing motivation and ability through procedural knowledge, as guided by Fogg and self-efficacy principles. In this model, self-efficacy served as a key mediator, confirming hypothesis 1 that procedural knowledge substantially improves users' ability to manage their smart home security. The structured, task-based nature of the 2D setup allowed users to perform specific actions (e.g., adjusting privacy settings), thereby fostering an actionable sense of competence. This increase in self-efficacy was evident in post-study questionnaires, where users reported feeling more capable and prepared to navigate smart home privacy settings. Participants' feedback underscored this finding; many expressed a sense of empowerment in managing their data settings independently, a shift from the initial uncertainty they felt in the SH-Setup. By reinforcing users' perception of ability, the 2D setup supported self-efficacy theory, which is crucial in security domains, influencing users' confidence to tackle complex security tasks effectively (Stanton et al., 2005; Arachchilage and Love, 2014).

The Fogg Behavior Model's Motivation and Ability components were further emphasized by users' positive reactions to the 2D interface's structure. *Interest/Enjoyment* and *Perceived Competence* scores from the IMI scale suggest that the 2D design created a task environment that engaged users and built their confidence, aligning with H2a and H2b. Many participants appreciated the straightforward layout and procedural clarity, stating that these features allowed them to manage privacy and security settings effort-

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

lessly, without confusion or stress. This underscores the FBM’s principle that simplicity enhances ability by minimizing cognitive load and simplifying tasks (Fogg, 2009), thereby increasing users’ motivation to actively engage with privacy and security settings in the 2D design. Those who previously felt unmotivated to delve into privacy settings reported that the well-structured interface made it straightforward to understand where to go and what to adjust.

The enhancement of informed behavior in the 2D-Setup provides robust support for H3a and H3b and demonstrates that self-efficacy interacted with Fogg’s Motivation and Ability components to predict informed behavior. As participants felt more capable and motivated, their actions shifted towards more privacy-conscious behaviors. The 2D interface facilitated this behavioral change by enabling users to follow a clear path to complete privacy tasks without relying heavily on external triggers. This distinction from the AR-Setup, which relied on immersive visuals as triggers, highlights how structured security tasks that prioritize procedural clarity can foster intrinsic motivation for security behaviors (Padayachee, 2012).

Furthermore, the final interview provided insights into how the 2D interface influenced participants’ perceptions and understanding of smart home privacy management. First, a majority of participants expressed a strong interest in using the app in their own homes, primarily due to its straightforward design and ability to provide a centralized overview of device interactions. This positive reception suggests that the app’s layout made privacy management feel more practical and manageable, which is essential for encouraging regular engagement with privacy controls.

In terms of understanding smart home processes, many participants reported that the 2D interface helped them better visualize how data flows between devices and connects to third-party servers. Before using the app, many participants saw smart home devices as independent units rather than parts of an interconnected system. The 2D layout’s structured representation clarified these connections, making it easier for users to grasp the broader data flow and thus gain a clearer picture of potential privacy implications.

When it came to adjusting settings, participants highlighted that the 2D app’s organization of security options allowed them to navigate and adjust privacy settings with confidence. This increase in understanding suggests that the interface’s task-oriented structure reduced the complexity often associated with privacy management and security configurations, empowering participants to make informed choices about their settings.

Finally, participants were very receptive to the one-pager privacy policy provided in the app, describing it as much easier to read than typical lengthy

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

policies. Many appreciated the use of bullet points, icons, and a concise format, which helped them quickly understand important privacy details without feeling overwhelmed. This feedback reinforces the importance of clear and accessible privacy information, as participants felt the simplified format gave them better control over their data (Brodie et al., 2005; Kelley et al., 2009; Reinhardt et al., 2021).

This study acknowledges several limitations that must be considered. Specifically, the limitations of the 2D study stem from the interface's lack of immersive qualities and potential oversimplification of data flow, which may have impacted the depth of users' understanding of smart home interactions. While the straightforward design offered procedural clarity, it lacked the spatial engagement present in the AR-Setup, possibly resulting in a more linear, less nuanced mental model of data connections. The 2D interface may have been less engaging for visually oriented or hands-on learners, as it provided a simplified visual representation that did not fully capture the complexities of inter-device relationships. Additionally, since the study relied on participants' existing comfort with technology, the findings may not generalize to users with lower tech familiarity. Unlike AR, which offers a contextualized, real-world experience, the 2D setup's flat-screen format did not incorporate physical environments, potentially limiting the practical relevance for users attempting to visualize device locations in their own homes. Furthermore, the 2D design lacked the novelty factor often associated with AR, which may have affected engagement levels, especially for users accustomed to interactive interfaces. Future adaptations could explore hybrid features like dynamic animations to combine clarity with enhanced engagement and better support varied learning styles.

Comparison The comparison of AR and 2D studies underscores distinct user engagement outcomes within the framework of procedural knowledge, motivation, and ability driving informed security behaviors. Both methods utilized task-driven interaction and visual representations to boost self-efficacy and encourage privacy-aware behaviors in smart home security settings. However, their impacts on participants' experiences and behaviors differed due to each interface's unique ability to shape mental models and responses.

Influence on Self-Efficacy and Privacy Engagement Both studies noted significant increases in self-efficacy from the initial SH-Setup. With its immersive visualization of data flow and device interconnections, the AR study showed slightly greater gains, reinforcing users' confidence more effectively than the 2D layout. In the AR-Setup, participants connected spatial interactions with privacy management more intuitively, reflecting a

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

real-world interaction experience. In contrast, the 2D-Setup, though less immersive, enabled users to complete tasks approximately 7 minutes faster, thanks to its streamlined and simplified interface.

Feedback from participants supports these findings. In the AR-Setup, users frequently cited the spatial nature of interactions as helping them connect privacy management with the physical layout of their smart home. The immersive experience of navigating between devices in an AR environment seemed to instill a more active sense of agency, possibly because it mimicked real-world interactions. The 2D study, while slightly lower in self-efficacy improvement, provided a structured and simplified view that allowed users to complete tasks easily. This interface was particularly helpful for users who benefit from straightforward steps rather than complex spatial engagement. Both studies thus aligned well with the model's prediction of self-efficacy improvement, though the AR-Setup added a unique experiential dimension that seemed to boost confidence slightly more.

Task Interaction and Mental Model Formation Each interface shaped users' mental models differently, reflected in how participants conceptualized the device interactions and data flows. In the AR study, the dashed lines connecting devices in a spatially immersive environment allowed users to physically explore the data connections, deepening their understanding of inter-device relationships. This spatial interaction helped participants build a mental data flow model incorporating physical context, encouraging them to consider how their environment affected privacy risks. Many participants noted feeling more aware of how devices could connect and transmit data, providing a dynamic mental model that situated privacy within the spatial layout of their homes.

In the 2D study, participants interacted with solid lines connecting devices on a screen, following a structured layout that provided procedural clarity. This design supported a more direct and linear mental model, emphasizing the sequential steps of privacy management without requiring physical navigation. Participants could see device interactions as straightforward connections and follow tasks step-by-step, creating a mental model focused on process rather than spatial relationships. This approach proved highly effective for participants who preferred simplicity, as they could understand data flow and device connections without managing spatial orientation, making it an accessible model for users who prioritize clarity and control over immersion.

Motivational Differences and Engagement Outcomes Both setups fostered increased user motivation, but the type of engagement differed. In the AR study, the immersive environment promoted interest and enjoy-

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

ment as users explored connections spatially, which motivated them to engage with privacy settings. The novelty of the AR interface, combined with the spatial exploration, allowed users to feel engaged with privacy management as an enhanced reality process. This deeper engagement seemed particularly effective for users who appreciated interactivity and could benefit from the unique hands-on experience AR offers.

The 2D-Setup, on the other hand, encouraged motivation through simplicity and ease of use, which allowed participants to focus directly on completing tasks without needing to navigate spatial complexities. Users appreciated the organized layout, which fostered a sense of control and independence in managing privacy. This straightforward engagement facilitated intrinsic motivation by making the process feel accessible and manageable, particularly for users who may find spatial interaction challenging. While the AR environment leveraged immersive engagement to drive motivation, the 2D approach's simplicity achieved similar motivational effects by reducing cognitive load and making privacy tasks easier to complete confidently.

Informed Behavior and Privacy-Conscious Actions Both studies supported informed behavior due to increased self-efficacy, motivation, and ability to manage privacy. However, the AR and 2D setups encouraged privacy-conscious actions differently. With its immersive visualization, the AR interface encouraged users to consider study tasks more thoughtfully, as the spatial layout reinforced a holistic view of device relationships and data flow. This design resonated particularly with users interested in a hands-on exploration of privacy settings, fostering a proactive approach to security.

In contrast, the 2D setup encouraged informed behavior through interface transparency. Participants could follow clear, task-based instructions to adjust privacy settings without confusion or distraction. Many users appreciated that they could understand settings through a direct, visually organized interface, which allowed them to make privacy-conscious adjustments efficiently. This approach supported a sense of empowerment in managing privacy settings independently and was especially effective for users who preferred a simple, process-oriented design. By providing a clear path to completion, the 2D-Setup demonstrated that well-structured interfaces could foster informed behavior without immersive elements, supporting privacy engagement through direct and accessible design.

Limitations of Both Studies A shared limitation in AR and 2D studies is the challenge of visualizing large-scale smart home systems with multiple interconnected devices. While each interface effectively represented connections and data flow for smaller, controlled setups, scaling to environ-

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

ments with numerous smart home devices presents practical difficulties. In the AR study, visual clutter becomes a concern as the immersive environment struggles to represent numerous connections clearly without overwhelming the user. As more devices are added, it becomes harder for users to navigate the spatial layout and maintain a coherent view of data flow, which could reduce the effectiveness of the AR interface in larger setups.

Similarly, in the 2D study, while the structured layout was beneficial for clarity, increasing the number of devices would result in a more complex and potentially crowded interface. Managing multiple connections on a flat screen could hinder users' ability to quickly identify and interact with specific device settings, potentially diminishing the interface clarity that was advantageous in smaller setups. This limitation suggests that, although the AR and 2D interfaces are valuable for engaging users with security management tasks, additional strategies, such as hierarchical organization, filtering options, or adaptive visual representations, may be necessary to maintain usability and clarity in large-scale smart home environments.

Acknowledgments

This section is based on the master's thesis:

Mike Schöning. 2024. *Informed Decisions in Smart Home Security: Boosting Self-Efficacy through Intuitive Settings*. Unpublished master's thesis. University of Bremen.

My contribution to this work: Conceptualization, data curation, formal analysis, investigation, methodology, project administration, resources, partial software development, supervision, validation, and visualization.

4.2.4 Key Insights of Informed Security Behavior

Study 12: AR Visualization Raises Security Perception

This study investigated the impact of AR visualization of device connections on user security perception in smart home setups. The AR interface with visual data flow lines significantly enhanced user experience compared to a non-visual version. Participants appreciated the visual elements, which improved their understanding and interaction with the system. However, the trust indices did not show significant enhancements despite these improvements, indicating a gap between understanding and trust. Related research demonstrated that AR visualizations can serve as effective triggers by simplifying complex data flows and enhancing user ability. Furthermore, self-efficacy theory suggests that visual aids can boost users' confidence in managing privacy settings by making abstract concepts more tangible and easier to understand. The positive feedback on the AR interface's intuitiveness and engagement confirms the capability of the AR interface and indicates increased perceived competence and motivation. The study also noted gender differences in the Key Performance Indicator scores, with men showing higher enhancements than women. This highlights the importance of considering diverse user backgrounds in designing inclusive interfaces. The positive correlation between security concerns and the perceived importance of data protection suggests that users who prioritize security view AR features favorably.

Study 13: AR Visualization Drives Security Decisions

This study explored how AR visualization of data flow in smart homes influences users' security behavior. The AR app significantly improved participants' self-efficacy, motivation, and ability compared to standard smart home setups (SH-Setup). The immersive experience of AR made data flows more comprehensible and engaging, leading to better security practices. The integration of the Technology Threat Avoidance Theory and the Fogg Behavior Model in this study highlights the importance of procedural knowledge in enhancing self-efficacy. AR's interactive nature served as a powerful trigger, increasing users' motivation and ability to manage security settings effectively. Self-efficacy theory suggests that hands-on, immersive learning experiences like AR can significantly boost users' confidence in their ability to handle complex tasks. Furthermore, participants demonstrated improved behaviors in avoiding services requesting personal information and favoring local networks over cloud-based services. The AR-Setup was rated higher in terms of attractiveness, efficiency, dependability, stimulation,

and novelty, indicating a strong preference for AR interfaces over common methods. Enhanced user experiences and clear, interactive visualizations can boost users' perceived competence and motivation, leading to more informed and proactive behaviors.

Study 14: 2D Interface Drives Security Decisions This study replicated the AR study using a 2D interface to compare the effectiveness of AR and 2D interfaces. The findings show that a structured, task-based interface significantly improves users' confidence and competence in managing smart home privacy and security settings, even without the immersive qualities of augmented reality. The results highlight that the 2D-Setup, with its clear, sequential layout, allows users to understand and adjust data flows and device connections, which in turn increases their self-efficacy and motivation for privacy-related tasks. Users reported feeling empowered by the straightforward organization of the interface, with higher scores in perceived competence and reduced pressure during tasks. Unlike the AR interface, which relied on spatial cues, the 2D interface achieved similar gains in user engagement by minimizing cognitive load and simplifying complex privacy configurations. This study underscores that a well-structured design focused on procedural clarity can drive informed security behaviors and user empowerment, making it particularly effective for users seeking a direct, accessible approach to privacy management within the smart home ecosystem.

Integration of Theories and Findings

These studies collectively underscore the importance of interaction techniques in HCI, particularly AR and visual 2D interfaces, in enhancing users' sense of capability (self-efficacy) through procedural knowledge. Our developed enhanced AR and 2D interfaces demonstrate their effectiveness in promoting motivation, ability, and informed behavior within privacy and security tasks by offering transparent, engaging, and user-friendly experiences.

From the user's perspective, these interactions improve self-efficacy by simplifying complex concepts, making them more accessible and easier to understand. For developers, creating intuitive, engaging interfaces that offer transparent communication and convey procedural knowledge is essential, as it not only builds users' confidence and competence in managing privacy and security settings but also helps maintain overall system security. Legislators benefit from supporting accessible, user-friendly privacy and security interfaces, as these align with regulatory goals to encourage better privacy practices and foster informed behaviors among users.

These studies demonstrated that this paradigm shift can be effectively realized by integrating the Fogg Behavior Model and self-efficacy theory,

4.2. INFORMED BEHAVIOR USING INTERACTIVE INTERFACES

helping users feel informed and empowered in managing their privacy rights. This approach is essential for cultivating a privacy-conscious and secure digital environment, directly addressing our fifth research question. Overall, interactions with enhanced AR and 2D interfaces are powerful means for improving self-efficacy and promoting informed behavior in privacy and security contexts.

RQ5

How can augmented reality enhance users' self-efficacy and procedural knowledge to promote motivation, ability, and informed behavior in privacy and security tasks?

By addressing Research Question 5, we evaluate the overall effectiveness of the model by examining how motivation, ability, goal-setting, and knowledge collectively foster informed behavior (see Figure 4.50). This question validates the model's structure, showing how these components interact to support empowered decision-making in privacy and security contexts. The insights from this question highlight the comprehensive impact of integrating these factors in designing user-centered digital environments.

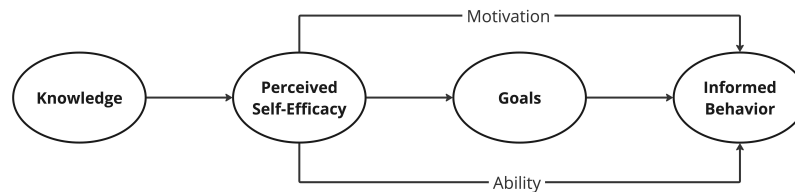


Figure 4.50: This model illustrates how knowledge acquisition influences users' self-efficacy, motivation, and ability and promotes informed behaviors.

5

Discussion

This section systematically examines the findings from 14 studies investigating user empowerment in the privacy and security domain in mobile and ubiquitous applications. We begin by revisiting our research questions to guide our subsequent analysis. Each study is briefly summarized to underscore its unique contributions, setting the stage for a meta-review. Through the meta-review, we identify recurring themes and differences across the studies. We integrate these insights with established theoretical frameworks to deepen our understanding of user behavior in response to privacy and security challenges. Our discussion concludes by exploring implications for practice, policy, and future research avenues. We also address methodological limitations and propose directions for further investigation.

5.1 Recap of Research Questions

This dissertation investigates how integrating psychological principles, particularly self-efficacy and the Fogg Behavior Model (FBM), within Human-Computer Interaction (HCI) strategies can enhance users' comprehension, engagement, and informed decision-making in privacy and security tasks in mobile and ubiquitous applications. This primary question is systematically addressed through five focused research questions.

RQ1, addressed in studies 1, 2, and 3, examines how integrating game elements within mobile apps can enhance users' intrinsic motivation and informed behaviors by leveraging self-efficacy principles. These studies show that gamification significantly boosts user engagement and comprehension, indicating that gamified learning can foster proactive security behaviors. For instance, Study 1 highlighted that incorporating gamification elements in mobile security apps can bridge knowledge gaps and boost user engagement. Similarly, Study 2 found that humorous decision-making games positively influence user motivation and awareness regarding mobile privacy and security issues. Study 3 demonstrated that good and evil game premises enhanced engagement, though not significantly, suggesting the importance of well-designed educational games in fostering learning and motivation.

RQ2, addressed in studies 4, 5, and 6, explores how visualization techniques, such as infographics and interactive tools like the HappyPermi and MASS apps, improve users' abilities to manage privacy settings and security measures, thereby enhancing self-efficacy and informed behavior. Study 4 found that infographics significantly improve performance in understanding smart home security by providing visual aids that enhance the retention of complex information. Study 5 revealed that the HappyPermi app effectively visualizes data transmission and implications of permission requests, improving user comprehension and proactive management of privacy settings. Study 6 indicated that static and privacy analysis tools can significantly enhance user awareness and decision-making regarding app permissions and privacy policies.

RQ3, addressed in studies 7, 8, and 9, investigates the impact of the temporal precision of triggers (timing and contextual relevance of notifications) on user decision-making and actions in privacy and security settings. Study 7 highlighted that providing users with summaries of their data inputs during app configuration enhances their ability to assess privacy and security risks. Study 8 demonstrated that one-pager privacy policies presented in different formats affect usability and users' workload, with tab-based presentations improving usability and reducing cognitive load. Study 9 showed that

5.2. INTEGRATION WITH THEORETICAL FRAMEWORKS

just-in-time presentation of privacy choices can enhance users' self-efficacy and awareness, indicating the importance of timely information delivery in promoting user engagement and informed decision-making.

RQ4, addressed in studies 10 and 11, delves into the imperative for a paradigm shift towards empowering users to navigate their privacy rights. Study 10 revealed significant gaps in user comprehension of privacy and security terms and highlighted the need for targeted educational efforts to improve user understanding and trust in smart home technology. Study 11 exposed discrepancies between privacy policies and actual data practices, emphasizing the need for clearer and more transparent information to build user trust and ensure informed consent. These studies underscore the necessity of clear, transparent privacy information and the reduction of manipulative practices like dark patterns to build trust and enhance user empowerment.

RQ5, addressed in studies 12, 13, and 14, compares the effectiveness of AR and classic 2D interfaces in enhancing users' self-efficacy through procedural knowledge, thereby promoting motivation, ability, and informed behavior in privacy and security tasks. Study 12 found that AR visualization of device connections in smart homes significantly improves user experience and security perception. Study 13 demonstrated that AR interaction enhances self-efficacy, motivation, and informed behavior by providing immersive and interactive learning experiences. Study 14 showed that 2D interfaces also improve self-efficacy and informed behavior, offering a more engaging user experience.

These studies collectively explore how psychological principles and HCI strategies improve user understanding, engagement, and decision-making in privacy and security within mobile and ubiquitous apps. The findings underscore the importance of user-centered design, transparency, and timely, contextually relevant information in fostering a secure digital environment.

5.2 Integration with Theoretical Frameworks

The introduction of this dissertation emphasized that HCI integrates theories from various disciplines to analyze and predict user performance with computer interfaces comprehensively. These theories encompass cognitive, social, and organizational domains (Rogers, 2022). Behavioral theories are categorized by their level of generality or specificity, guiding research methodologies, and application strategies (Hekler et al., 2013). *Conceptual frameworks*, exemplified by self-efficacy theory, delve deeply into specific aspects of human behavior, such as how beliefs in one's capabilities shape actions (Consolvo et al., 2017). In contrast, *Meta-Models*, such as the Fogg Behavior Model, provide overarching structures that offer a generalized understanding of

5.2. INTEGRATION WITH THEORETICAL FRAMEWORKS

behavior across diverse contexts (Consolvo et al., 2017). While foundational, these models typically necessitate the integration of conceptual frameworks and empirical methodologies to achieve detailed and practical applications.

The integration of these diverse theoretical perspectives within HCI underscores their pivotal role in developing technologically effective and user-centered designs, especially in sensitive domains like privacy and security (Rogers, 2022). For instance, applying the Fogg Behavior Model in the context of mobile device security can illuminate how factors such as motivation, ability, and triggers influence users' decisions to engage with privacy settings. Meanwhile, Social Cognitive Theory provides insights into how personal beliefs and environmental factors shape individuals' adoption of secure behaviors in digital environments.

This work proposes a strategic approach to behavioral research within ubiquitous computing applications, starting with the integration of meta-models (Fogg Behavior Model and Social Cognitive Theory) and progressing to the application of more specific conceptual frameworks like self-efficacy theory (Consolvo et al., 2017). By exploring these theories in the context of privacy and security, researchers can gain deeper insights into user motivations, perceptions of risk, and behavioral patterns concerning the use of security features in digital technologies. This structured approach ensures a comprehensive exploration of motivational factors and self-perceived abilities in interaction with technology, which is essential for designing effective and user-friendly security solutions.

We approach this topic from several perspectives. Firstly, we examine it through the lens of theoretical integration in HCI, where theories from cognitive, social, and organizational domains converge to enhance our understanding of user behavior with computer interfaces. Specifically, we explore how meta-models like the Fogg Behavior Model provide a broad framework for understanding behaviors related to privacy and security across various technological contexts. Secondly, we delve into practical applications within ubiquitous computing environments. This involves implementing these theoretical frameworks to analyze and predict user interactions with privacy and security features in digital platforms. For example, understanding how self-efficacy theory influences individuals' confidence in managing their privacy settings on smart home applications can lead to well-informed decisions. Furthermore, our approach integrates empirical methodologies such as experience sampling and usability testing to validate these theoretical constructs in real-world scenarios. This multidimensional perspective ensures that theoretical insights translate into practical strategies for enhancing user-centered design in privacy-sensitive technologies.

RQ1: Integration of Game Elements and Self-Efficacy Beliefs

How do game elements and narratives in ubiquitous and mobile applications enhance users' self-efficacy, boost intrinsic motivation, and promote the adoption of informed behaviors?

The strategic integration of game elements within ubiquitous and mobile applications significantly interacts with users' self-efficacy beliefs to enhance intrinsic motivation and promote consistent adoption of informed behaviors. Studies 1, 2, and 3 collectively underscore this interaction. In Study 1, the gamified application *Make my phone secure!* effectively elevated users' engagement and comprehension of mobile security settings, particularly among those with prior knowledge of Android permissions management. This supports the notion that gamification can satisfy psychological needs for autonomy, competence, and relatedness, thereby enhancing intrinsic motivation (Ryan and Deci, 2000; Von Ahn and Dabbish, 2008). Study 2 further corroborates this by showing that a humorous decision-making game significantly increased user motivation and awareness of mobile privacy and security issues. Participants exposed to the game demonstrated a higher inclination to re-engage with similar content, suggesting that interactive and entertaining elements can bolster engagement and comprehension (Dormann et al., 2006; Lombardi, 2012). This aligns with the Fogg Behavior Model's emphasis on motivation as a key factor in behavior change. Finally, Study 3 highlights that the thematic context of a game (good vs. evil) does not significantly influence motivation or learning outcomes. Instead, effective game design and integration of educational content play a more pivotal role in fostering engagement and learning (Sweller, 1988). This suggests that the efficacy of game elements in enhancing self-efficacy and promoting informed behaviors lies in their design and educational integration rather than their thematic elements.

All three studies underscore the importance of engagement and motivation in learning about privacy and security. Study 1 and Study 2 found that gamification and humor significantly enhance user engagement and intrinsic motivation. Study 1 highlighted the role of self-determination theory, suggesting that gamification fulfills psychological needs, thereby boosting motivation. Study 2 demonstrated that humor adds an element of enjoyment, making the learning process more engaging. Study 3, however, found that the thematic context of the game (good vs. evil) did not significantly impact engagement or motivation. This finding suggests that while thematic elements can add flavor to educational content, they are not as crucial as the overall design

5.2. INTEGRATION WITH THEORETICAL FRAMEWORKS

and integration of educational content and game mechanics.

Improving user comprehension and awareness of privacy and security issues was a common outcome in all three studies. Study 1 showed that gamification significantly improved users' understanding of mobile security settings. Study 2 found that a humorous decision-making game enhanced users' awareness of privacy and security issues. Study 3 demonstrated that well-designed educational games, regardless of their thematic context, effectively improved user performance and comprehension.

The studies collectively highlight the application of different theoretical frameworks in understanding user behavior and enhancing learning outcomes. Study 1 applied self-determination theory to explain how gamification boosts intrinsic motivation by fulfilling psychological needs. Study 2 implicitly applied theories related to humor and learning, suggesting that humor can make learning more enjoyable and memorable. Study 3 utilized cognitive load theory to argue that effective game design and integration of educational content are more important than thematic elements in enhancing user engagement and learning.

Studies 1, 2, and 3 collectively demonstrate the effectiveness of game elements in enhancing user engagement, motivation, and comprehension in the context of privacy and security education. While Study 1 and Study 2 emphasize the roles of gamification and humor, respectively, Study 3 highlights the importance of effective game design and educational integration over thematic context. These findings suggest that a strategic combination of game elements, humor, and thoughtful design can significantly enhance users' learning experiences and outcomes in mobile and ubiquitous applications.

RQ2: Visualization Techniques and Self-Efficacy Beliefs

How do visualization techniques in ubiquitous and mobile applications enhance users' ability to manage security settings, interact with their self-efficacy, and promote informed behaviors?

Studies 4, 5, and 6 collectively underscore the critical role of visualization techniques in enhancing user comprehension and engagement with privacy and security information. Study 4 explored the application of infographics in a smart home security game, demonstrating that infographics significantly improved performance and perceived competence by making complex information more accessible and engaging. Participants who received infographics showed significantly higher performance in answering questions correctly compared to those who received textual feedback. This finding aligns with

5.2. INTEGRATION WITH THEORETICAL FRAMEWORKS

previous research suggesting that infographics enhance awareness and retention of complex information by providing visual aids alongside textual content (Krum, 2013; Lyra et al., 2016). The dynamic nature of infographics, blending text, images, and charts, facilitates a deeper understanding of the subject matter, particularly in scenarios where the topic is inherently intricate (Haan et al., 2018). Moreover, the increase in players' *Perceived Competence* following exposure to infographics underscores the motivational benefits associated with this form of feedback.

Similarly, Study 5 investigated the *HappyPermi* app, which used visual representations to clarify data destinations and permission implications. This app significantly improved user comprehension and proactive management of privacy settings. The *HappyPermi* app provided users with a user-friendly interface that demystified complex Android permissions, aligning with self-efficacy theory by boosting users' confidence in managing their privacy settings (Breitinger et al., 2020). The study found that 69% of users opted to turn off the contact permission, underscoring a practical understanding of the potential risks associated with unnecessary data access. This significant proportion of users altering permissions highlights their awareness and proactive management of their privacy, reflecting their discomfort with potential risks and the real-world implications of permission settings. Additionally, the usability scores revealed that the *HappyPermi* app maintained good levels of usability, essential for ensuring that users are aware of the permissions they authorize and fully grasp the associated consequences.

Following Study 5, Study 6 examined static and privacy analysis tools, particularly the MASS app, which featured interactive elements and clear information presentation that significantly enhanced user awareness and decision-making (Grundy et al., 2019). The study revealed that static and privacy analysis tools like the MASS app improve user awareness and decision-making regarding Android application permissions and privacy policies. The MASS app's user-friendly design, interactive elements, and comprehensive information presentation were consistently praised, underscoring its potential to enhance user understanding and management of app permissions and privacy. The positive feedback for the MASS app, compared to mixed reviews for other tools like *Apk Analyzer*, *App Inspector*, and *APK-Info*, suggests that tools designed with the user in mind can significantly improve comprehension and engagement. Participants' evaluations provided valuable insights into effective app design. The MASS app stood out for its intuitive interface, clear presentation of information, and interactive features, which aligned with Shneiderman's eight golden interface design rules, particularly regarding consistency, feedback, and user control. These critiques emphasize

5.2. INTEGRATION WITH THEORETICAL FRAMEWORKS

balancing comprehensive information with clarity and accessibility to avoid overwhelming users.

A common theme across these studies is the significance of user-centered design in developing effective privacy and security tools. Study 4 emphasized the need for visual aids like infographics to make complex information more understandable. Study 5 showcased the importance of a user-friendly interface in the *HappyPermi* app to demystify privacy settings. Study 6 highlighted the value of interactive design and clear information presentation in the MASS app to boost user awareness and decision-making. These findings suggest that privacy and security tools must be designed with the user in mind, focusing on accessibility, clarity, and interactivity to be effective.

All three studies also underscore the importance of enhancing users' self-efficacy to promote proactive privacy and security behaviors. Study 4 indicated that infographics, by making information more accessible and engaging, increased participants' perceived competence and motivation. Study 5, aligned with self-efficacy theory, shows that visualizing complex privacy settings boosted users' confidence in managing their privacy. Study 6 highlighted that interactive design and clear information presentation in the MASS app enhanced user comprehension and engagement, which are critical components of self-efficacy.

In conclusion, Studies 4, 5, and 6 collectively demonstrate the effectiveness of visualization techniques and user-centered design in enhancing user comprehension, self-efficacy, and proactive management of privacy and security settings. Study 4 highlighted the role of infographics in improving performance and perceived competence. Study 5 showed that visual representations in the *HappyPermi* app significantly improved users' understanding and proactive behavior. Study 6 emphasized the importance of interactive design and clear information presentation in the MASS app to boost user awareness and decision-making. These findings underscore the need for privacy and security tools that are visually engaging, user-friendly, and designed to enhance users' self-efficacy and informed behavior.

RQ3: Temporal Precision of Triggers

How does the temporal precision of triggers impact users' decision-making and actions when configuring privacy and security settings within ubiquitous and mobile applications?

Studies 7, 8, and 9 collectively demonstrate the importance of information presentation, timing, and usability in enhancing users' privacy and security

5.2. INTEGRATION WITH THEORETICAL FRAMEWORKS

decision-making processes. Study 7 examined the impact of the automatic appearance of the APP-INFO page compared to providing users with summaries of their data inputs during app configuration on their ability to assess privacy and security risks. The findings revealed that the group exposed to user data summaries (UDAP) exhibited a more conservative and cautious approach to app permissions, likely due to heightened awareness of privacy and security issues. This group accurately assessed high-risk scenarios, reflecting a robust understanding of potential privacy infringements. Conversely, the group exposed to the APP-INFO page showed a moderate understanding of risks, which aligns with real-world app usage scenarios where users recognize trade-offs between functionality and privacy. Qualitative feedback indicated a lack of awareness about the APP-INFO page among participants and a desire for more comprehensive privacy and security information. Users preferred the UDAP interface for its ability to furnish detailed privacy and security details, suggesting that detailed and context-specific information can significantly enhance users' risk assessment and decision-making processes (Wottrich et al., 2018; Frik et al., 2022).

In Study 8, our focus shifted towards real-world applications, particularly emphasizing the critical role of privacy policies. These policies serve as essential sections within applications, facilitating communication with individuals about their rights and privacy concerns. We aimed to improve the one-pager privacy policy design by employing various representation formats and investigating their effects on usability and users' workload. Participants in the tab-based condition demonstrated quicker response times and higher usability ratings compared to other conditions. This format helped users better understand information by providing a clear overview and structuring the content in a meaningful manner. Significant differences in usability ratings indicated that the tab-based and device-based conditions were superior to the List version, suggesting that categorization and structuring of information can reduce cognitive load and improve comprehension. The NASA-TLX results showed that segmenting privacy policies into tabs significantly reduced perceived workload, especially in terms of physical and mental demands and effort (Zhang and Adipat, 2005; Reeder et al., 2008; Lipford et al., 2010). This indicates that well-organized information presentations can enhance usability and make privacy policies more user-friendly.

In Study 9, we advanced our investigation to explore whether adjusting the timing of privacy choice presentations, alongside applying principles from Bandura's self-efficacy theory, could influence individuals' behaviors. The study used a web application based on the self-efficacy theory and integrated three timing dimensions for presenting privacy choices (Feng et al., 2021). The

5.2. INTEGRATION WITH THEORETICAL FRAMEWORKS

findings showed that just-in-time presentation of privacy choices significantly enhanced self-efficacy, awareness, and cautiousness in information sharing compared to at-setup and on-demand presentations. Participants in the just-in-time group demonstrated higher self-efficacy scores, indicating that timely presentation of privacy choices can increase users' confidence in managing their privacy settings. Awareness scores were also highest in the just-in-time group, suggesting that presenting privacy choices at the moment of need is more effective in enhancing users' perceived awareness. However, there were no significant differences in perceived privacy protection among the groups, implying that while timing affects immediate awareness, it might not influence deeper perceptions of privacy protection abilities. Qualitative feedback highlighted the importance of timing, with participants in the just-in-time group expressing higher satisfaction with the presentation of privacy choices.

Studies 7, 8, and 9 all emphasize the critical role of information presentation in enhancing users' privacy and security decision-making processes. Study 7 showed that providing detailed summaries of user data inputs during app configuration (UDAP) significantly improved users' ability to assess privacy and security risks. This finding highlights the importance of context-specific and comprehensive information in helping users make informed decisions. Study 8 supported this by demonstrating that well-organized privacy policies (tab-based and device-based formats) reduce cognitive load and improve usability, making complex information more accessible and understandable. Study 9 further reinforced the importance of timely information presentation, showing that just-in-time privacy choice presentations significantly enhance self-efficacy and awareness.

Moreover, the timing and context of information presentation emerged as essential factors in influencing users' decision-making and actions. Study 9's finding that just-in-time presentation of privacy choices significantly enhances self-efficacy and awareness underscores the importance of providing information when it is most relevant to users. This aligns with the Fogg Behavior Model's emphasis on the role of timely prompts (triggers) in driving desired behaviors. Study 7 also highlighted the importance of context-specific information, with the UDAP group showing better risk assessment and decision-making due to the detailed and relevant information provided during app configuration.

User-centered design and usability are recurring themes across the studies. Study 8 demonstrated that structuring privacy policies into tabs significantly improves usability and reduces cognitive load, making it easier for users to navigate and comprehend complex information. Study 7's qualitative

5.2. INTEGRATION WITH THEORETICAL FRAMEWORKS

feedback indicated a preference for the UDAP interface, which provided more detailed and user-friendly privacy and security information. Study 9's participants expressed higher satisfaction with the just-in-time presentation of privacy choices, indicating that timing and user experience are crucial in designing effective privacy and security tools.

In conclusion, all three studies underscore the importance of enhancing users' self-efficacy to promote informed privacy and security behaviors. Study 7 showed that providing detailed summaries during app configuration (UDAP) increased users' understanding and cautiousness in assessing risks. Study 8 highlighted that well-organized privacy policies can reduce cognitive load, thereby potentially enhancing users' confidence in managing their privacy. Study 9 explicitly focused on self-efficacy, demonstrating that just-in-time presentation of privacy choices significantly enhances users' confidence and awareness in managing their privacy settings. These findings underscore the need for privacy and security tools that are designed with the user in mind, focusing on providing relevant, timely, and well-organized information to enhance users' self-efficacy and informed decision-making.

RQ4: Imperative for a Paradigm Shift

Do users understand the basic components of security, and do apps implement transparent mechanisms to support this understanding?

Studies 10 and 11 together provide a comprehensive view of the challenges users face in understanding and managing their privacy and security in the context of smart home technology and health & fitness apps. Study 10 investigated users' comprehension of privacy and security terms related to smart home technology and how exposure to these terms influences their behavioral intentions. The findings revealed a wide range of familiarity and understanding among participants, from minimal to advanced levels, with most users having only a basic or moderate grasp of key concepts. Terms such as "Authentication," "Password," and "Privacy Policy" were generally well understood, while more complex terms like "Access Control," "Pseudonymization," and "Communication Protocol" were not as well comprehended. This disparity underscores the need for targeted educational efforts to improve user understanding of more technical privacy and security concepts (Zwilling et al., 2022). The study also explored how exposure to these terms affects behavioral intentions. It found a moderate negative correlation between privacy concerns and trusting beliefs, suggesting that higher privacy concerns are associated with lower trust in data handling entities. Additionally, there

5.2. INTEGRATION WITH THEORETICAL FRAMEWORKS

was a strong positive correlation between trusting beliefs and risk beliefs, indicating that users who trust data-handling entities are also more aware of the associated risks. The regression analysis showed that privacy concerns significantly predict security behavioral intentions, highlighting the critical role of privacy concerns in shaping users' behaviors toward smart home security practices (Guhr et al., 2020).

In Study 11, we shifted our strategy to focus on applications that handle sensitive data. This decision was motivated by the need to examine how developers and companies design apps requiring heightened user privacy and security considerations. We employed an interdisciplinary approach to examine the gaps between privacy policies and actual data transmission practices within health & fitness apps. The analysis revealed significant discrepancies, particularly in the disclosure of third countries and data recipients. For instance, 65% of privacy policies categorized countries rather than explicitly naming them, leaving users uncertain about where their data might end up. This ambiguity challenges users trying to pinpoint the destination of their data and undermines transparency (Wagner, 2018; Juliussen et al., 2023). Similarly, privacy policies often used broad categories like "Advertising Partners" and "Service Partners" instead of naming specific entities, further obscuring data practices. Although 85% of the technical analysis aligned with the privacy policies regarding data recipients, the lack of specificity erodes user trust. The study also uncovered that many apps transmitted data before users consented to privacy policies, raising concerns about unauthorized data sharing. The presence of dark patterns in consent dialogs, such as misdirection and forced action, was prevalent, coercing users into agreeing to data collection without fully understanding the implications (Di Geronimo et al., 2020).

Both studies emphasize the importance of user comprehension and awareness in managing privacy and security. Study 10 highlighted that while users are familiar with basic terms like "Password" and "Privacy Policy," there is a significant gap in understanding more complex concepts. This gap in comprehension can lead to misconceptions and a lack of proper security practices. Study 11 corroborates this by showing that even when privacy policies are available, their vague and broad language often fails to provide users with a clear understanding of data practices, leading to confusion and mistrust. The studies also explore the relationship between privacy concerns, trust, and behavioral intentions. Study 10 found that higher privacy concerns correlate with lower trust in data-handling entities and that privacy concerns significantly predict security behavioral intentions. This suggests that users who are more concerned about their privacy are

5.2. INTEGRATION WITH THEORETICAL FRAMEWORKS

likely to adopt more cautious security behaviors. Study 11 extends this by showing that the lack of specificity and transparency in privacy policies diminishes trust, highlighting the need for clear and detailed privacy information to build user trust and promote informed behaviors. Furthermore, transparency is a critical theme in both studies. Study 10 indicates that a better understanding of privacy and security terms can influence users' trust and behavioral intentions. However, Study 11 reveals that even when users attempt to engage with privacy policies, the lack of transparency in these documents hinders their ability to make informed decisions. The study's findings on the presence of dark patterns in consent dialogs further illustrate how users can be misled or coerced into agreeing to data practices they do not fully understand, highlighting a significant ethical concern in app design and privacy communication. Additionally, both studies underscore the need for improved privacy education and clearer privacy policies. Study 10 suggests targeted educational efforts to enhance users' understanding of complex privacy and security terms, which can lead to more informed and cautious behavior. Study 11 calls for stricter regulatory oversight and the development of standardized guidelines to ensure that privacy policies are clear, specific, and transparent. This includes explicit naming of data recipients and third countries, as well as the elimination of dark patterns that manipulate user consent. These findings highlight the urgent need for a paradigm shift towards empowering users through better privacy education, clearer privacy policies, and more transparent data practices.

RQ5: Procedural Knowledge and Interaction Techniques

How can augmented reality enhance users' self-efficacy and procedural knowledge to promote motivation, ability, and informed behavior in privacy and security tasks?

Studies 12, 13, and 14 collectively demonstrate the effectiveness of visualization techniques in enhancing user engagement, self-efficacy, and informed behavior in managing smart home security. Study 12 explored the application of augmented reality technology in smart home setups, focusing on how visualizing device connections influences users' security perceptions. The study used an AR app to overlay virtual smart home devices onto the real environment, connecting them to a virtual router. Participants interacted with two versions of the app: one without visual data flow lines (*Linker*) and one with visual data flow lines (*Connector*). The results indicated that the *Connector* interface, which visualized data flow, significantly enhanced

5.2. INTEGRATION WITH THEORETICAL FRAMEWORKS

user engagement and understanding of security settings. Participants found the visual elements like color-coded lines and icons particularly helpful for depicting connections and security statuses, making the interface intuitive and engaging (Nikhashemi et al., 2021; Zeng et al., 2017).

Study 12 provided us with an overview of user experiences but prompted us to explore additional avenues of inquiry. In alignment with the theories we have elucidated, Study 13 explored how the AR visualization of data flow in smart homes influences users' security behavior. An AR application was designed to provide an interactive and immersive experience, allowing users to configure hypothetical security and privacy settings visually. The study integrated concepts from the Technology Threat Avoidance Theory and the Fogg Behavior Model to highlight the importance of procedural knowledge in improving users' self-efficacy, motivation, and informed behavior regarding smart home security. The findings showed that the AR-Setup significantly improved participants' self-efficacy, motivation, and ability compared to a traditional smart home setup (SH-Setup). Participants demonstrated better behaviors in avoiding services that request personal information and favoring local networks over cloud-based services (Consolvo et al., 2017).

Despite focusing on AR interactions, we continued to explore 2D interfaces. Therefore, Study 14 replicated Study 13 but employed a 2D interface instead of AR. The study sought to determine whether a conventional 2D interface could achieve similar benefits. Participants interacted with 2D-Setup interfaces designed to visualize data flows and configure security settings. The results indicated significant improvements in self-efficacy, motivation, and informed behavior compared to the traditional smart home setup, though not as pronounced as with the AR-Setup. Participants reported heightened interest and enjoyment, greater perceived competence, and increased informed behavior when using the 2D interface. This study highlighted that while AR offers a more immersive experience, a well-designed 2D interface can also significantly enhance user comprehension and engagement (Nikou, 2019).

All three studies emphasize the importance of visualization in enhancing user engagement and comprehension in managing smart home security. Study 12 demonstrated that AR visualization of device connections (Connector) significantly improved user understanding of security settings. The visual data flow lines and color-coded icons helped users intuitively grasp the security statuses of their devices. Similarly, Study 13's AR-Setup showed that AR visualization of data flow significantly enhanced self-efficacy, motivation, and informed behavior. The immersive experience provided by AR made complex security configurations more tangible and understandable. Study 14, while using a 2D interface, also found that visualizing data flows improved

5.2. INTEGRATION WITH THEORETICAL FRAMEWORKS

user engagement and comprehension, though the effect was slightly less pronounced than with AR.

Furthermore, enhancing self-efficacy is a critical outcome in all three studies. Study 12 found that the *Connector* interface improved participants' perceived competence and confidence in managing smart home security settings. Study 13 further highlighted this by showing that the AR-Setup significantly boosted self-efficacy, motivation, and informed behavior compared to a traditional setup. Participants were more proactive in managing their privacy settings and exhibited better security behaviors. Study 14 corroborated these findings, demonstrating that a well-designed 2D interface could also enhance self-efficacy and informed behavior, although to a slightly lesser extent than AR. This suggests that both AR and 2D visualizations can effectively empower users, but AR may offer additional benefits in terms of immersion and engagement.

Procedural knowledge is a central theme in these studies, reflecting how users learn to manage security settings through interaction. Study 12's focus on visualizing device connections helped users build a mental model of their smart home network, improving their procedural knowledge. Study 13 extended this by integrating TTAT and FBM, showing that AR visualization of data flow helps users develop a deeper understanding of security practices, enhancing their self-efficacy and informed behavior. Study 14, while using a 2D interface, also emphasized the importance of procedural knowledge. Participants who interacted with the 2D visualization reported better understanding and management of their smart home security settings. These findings suggest that both AR and 2D interfaces can effectively convey procedural knowledge, though AR's immersive nature might provide a more engaging learning experience.

Moreover, user-centered design and usability are recurring themes across these studies. Study 12 highlighted the importance of intuitive visual elements, such as color-coded lines and icons, in making the *Connector* interface user-friendly. Study 13's AR-Setup was praised for its immersive and interactive design, significantly enhancing user engagement and understanding. Despite being less immersive, study 14's 2D interface still provided a clear and structured visualization that improved usability and comprehension. These studies collectively suggest that effective privacy and security tools must be designed with the user in mind, focusing on intuitive, clear, and engaging visualizations to enhance usability and user experience. These studies underscore the importance of user-centered design, procedural knowledge, and visualization in developing effective privacy and security tools. Both AR and 2D interfaces can empower users to better understand and manage their

smart home security settings by focusing on clear, intuitive, and engaging visualizations.

5.3 Implications and Contributions

This dissertation thoroughly examines how Human-Computer Interaction strategies can be utilized to enhance users' comprehension and engagement in privacy and security tasks within mobile and ubiquitous applications, integrating psychological principles such as self-efficacy and the Fogg Behavior Model. We employed diverse methodologies to study user behavior in this field and identified factors that influence their actions. Across multiple studies, we explored HCI techniques like gamification, visualization, and augmented reality interaction alongside users' privacy concerns, risk perceptions, and levels of trust. We also examined the role of knowledge empowerment in strengthening users' self-efficacy.

As introduced in the background section, our model outlines the relationships between these elements, and its validity was confirmed by the 14 studies. The integration of game elements (RQ1) demonstrated that enhancing users' motivation and comprehension through gamification boosts self-efficacy, thereby promoting the consistent adoption of informed behaviors, as evidenced in studies 1, 2, and 3. Visualization techniques (RQ2) further improved users' perceived abilities and informed behavior by making complex privacy settings more accessible and understandable, validated by studies 4, 5, and 6. The timing and contextual relevance of notifications (RQ3) significantly improved informed behaviors by helping users set and achieve short-term and immediate goals, as demonstrated in studies 7, 8, and 9. An urgent need for a paradigm shift (RQ4) was underscored by studies 10 and 11, highlighting the importance of transparent and ethical interfaces to enable users to manage privacy and security settings effectively. Research question 5 addressed the role of AR and 2D interfaces in fostering users' self-efficacy through procedural knowledge, which in turn led to improved motivation, ability, and informed behavior. This question also served to validate the entire model, showing that these interactive interfaces enhance self-efficacy and promote a secure approach to privacy management, confirmed through studies 12, 13, and 14 (see Figure 5.1). Finally, we found that while privacy concerns influence behavior, the combination of knowledge, self-efficacy, and user motivation are critical factors driving informed decision-making, as demonstrated in studies 10, 12, 13, and 14. The model illustrates how these components interact within the framework of HCI approaches and privacy concerns to promote informed behavior in managing security tasks.

This work has profound implications and contributions to human-computer

5.3. IMPLICATIONS AND CONTRIBUTIONS

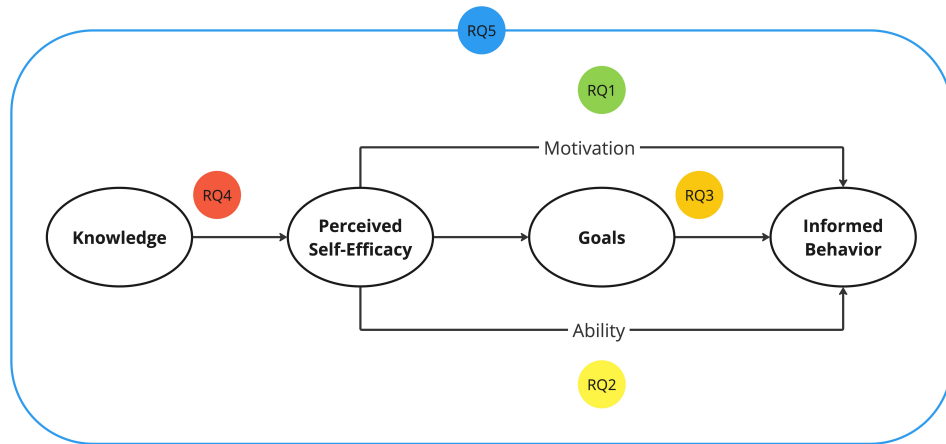


Figure 5.1: This model illustrates how knowledge acquisition influences users' self-efficacy, motivation, and ability and promotes informed behaviors in mobile and ubiquitous applications.

interaction and privacy management in mobile and ubiquitous applications. By employing various methodologies, we have demonstrated how HCI techniques such as gamification, visualization, and AR interfaces significantly enhance users' self-efficacy, knowledge, and engagement in managing privacy and security settings. The studies validate the proposed model, revealing the intricate interplay between knowledge acquisition, perceived self-efficacy, and informed behavior. Our findings underscore the critical importance of timely and contextually relevant information in fostering better decision-making, highlighting how triggers aligned with users' immediate needs can effectively drive desired behaviors.

Furthermore, this dissertation emphasizes the need for a paradigm shift towards empowering users with clear, transparent privacy and security interfaces. The positive impact of user-centered design on enhancing self-efficacy and informed behavior highlights the importance of integrating intuitive, engaging, and accessible interfaces for privacy and security settings. By bridging the gap between privacy concerns and informed actions, this work advances more effective privacy and security solutions that address users' needs and equip them with the confidence and skills to manage their data proactively.

Additionally, this work highlights the nuanced role of trust and risk perceptions in user behavior, suggesting that enhancing knowledge and self-efficacy can mitigate the adverse effects of privacy concerns on trust. The comprehensive approach taken in this research, incorporating elements of the Fogg Behavior Model and self-efficacy theory, provides a robust framework

for understanding and influencing user behavior in digital contexts. Overall, this work offers valuable insights for designing more effective, user-friendly privacy and security mechanisms, ultimately enhancing user autonomy, trust, and informed decision-making in mobile and ubiquitous applications.

5.4 Limitations and Future Directions

This dissertation faced several limitations, providing a foundation for future work. One significant limitation was the relatively small and homogeneous participant group, which affects the generalizability of the findings; future research should aim for more extensive and diverse samples. Additionally, the scenarios used in our studies did not encompass various smart home configurations, limiting the applicability to a broader range of setups. The reliance on self-reported data introduces potential biases, such as social desirability and recall inaccuracies, highlighting the need for objective measures and longitudinal studies for more accurate insights. Simulated environments in some studies may not fully replicate real-world complexities, suggesting future research should incorporate real-world scenarios and actual device usage. Technological constraints also influenced outcomes, pointing to the necessity of continued technological advancements to support more nuanced findings. While this work focused primarily on specific applications, like smart homes and health and fitness apps, future studies should explore broader applications to gain a comprehensive understanding.

Expanding sample diversity across demographics, technological proficiency, and cultural backgrounds will enhance the robustness of the findings. Longitudinal studies could reveal shifts in user behavior over time, providing insights into the long-term impact of HCI techniques. Incorporating objective metrics and real-world testing environments can yield more realistic insights into user behaviors and practical challenges. Exploring new technologies, including advanced AR interfaces and machine learning-driven personalization, will be essential to improving the usability and effectiveness of privacy tools. Finally, further integrating behavioral and psychological theories could deepen understanding of user behavior within digital environments. More practical, user-centered privacy and security solutions for mobile and ubiquitous applications can be developed by addressing these limitations and exploring future research directions.

6

Conclusion

This dissertation addresses the essential challenges in privacy and security that arise as technology becomes seamlessly embedded in everyday life through ubiquitous and mobile computing. The concept of ubiquitous computing, initially articulated by Weiser (1991), envisions a world where technology blends invisibly into our environment. While enhancing usability, this integration brings privacy risks due to the continual, often hidden, data exchange. Ubiquitous computing relies on principles like context-awareness, invisibility, and distributed computation to create smooth interactions between users and devices, but also raises substantial concerns about maintaining privacy and control over personal information (Poslad, 2011). The inherent, near-constant data exchange, combined with the growth of interconnected devices, can lead to privacy risks, as personal data is often shared without the user's explicit knowledge or consent (Langheinrich, 2018). Similarly, mobile computing emphasizes portability and real-time connectivity, resulting in continuous data exchange that can expose users to security threats, especially as devices act as rich sensors capable of capturing sensitive, context-specific information (Satyanarayanan, 2011). These ubiquitous and mobile computing challenges reveal an essential need to balance enhanced connectivity's benefits with adequate privacy and security measures that protect user autonomy and personal data (Sheng et al., 2008).

In response to these challenges, this work explores a range of Human-Computer Interaction approaches and theoretical frameworks to address privacy and security needs effectively. Drawing on Social Cognitive Theory and the Fogg Behavior Model, we examine how individual beliefs, motivations, and abilities influence user interactions with privacy and security tasks. As proposed by Bandura, SCT introduces elements like self-efficacy and goals, which explain an individual's confidence in their ability to perform an action (Bandura and Walters, 1977; Bandura, 1986). For example, an individual's belief in their capability to manage privacy settings can positively influence their behavior, leading to more secure interactions. The FBM further complements this by focusing on motivation, ability, and triggers as three essential components to drive behavior change effectively (Fogg, 2009). By integrating these models, we develop insights for designing applications that boost users' motivation to engage with privacy settings (via gamified elements), enhance their ability to navigate these settings (using visualization techniques), and encourage timely actions through well-placed prompts.

A fundamental part of this approach is understanding the types of knowledge required for informed privacy management. Conceptual knowledge enables users to understand the rationale behind privacy and security measures, while procedural knowledge equips them with practical skills to manage these settings (McCormick, 1997). Together, these knowledge types empower users, helping them to grasp privacy risks and effectively manage them. We introduce tools such as visualization and Augmented Reality to make privacy and security settings more comprehensible, translating complex information into intuitive, interactive experiences. For instance, AR can overlay virtual data flows onto real environments, allowing users to visualize the connections between devices in a smart home and recognize potential privacy risks. These HCI methods make privacy information more accessible and actionable, guiding users toward informed, privacy-protective behaviors.

Guided by these foundational concepts, this work addresses five research questions: investigating how gamified elements (RQ1), visualization techniques (RQ2), well-timed triggers (RQ3), and AR interfaces (RQ5) can enhance user motivation, ability, and informed behavior in privacy and security tasks. Additionally, RQ4 explores the broader paradigm shift required to empower users to exercise their privacy rights effectively. Each question is designed to deepen our understanding of user behavior in privacy and security contexts, underscoring the importance of transparent, user-centered designs that foster autonomy and trust in digital environments. This structured investigation seeks to inform the development of privacy and security tools that meet technical standards while aligning with users' needs and

expectations for control in increasingly interconnected, data-driven settings.

This work offers several contributions that extend current practices in privacy and security design, emphasizing user empowerment through accessible, engaging, and intuitively designed tools. First, by integrating Social Cognitive Theory and the Fogg Behavior Model within the HCI framework, we provide a theoretical basis for understanding user interactions with privacy and security features in ubiquitous and mobile applications. This model highlights how self-efficacy, motivation, ability, and contextually relevant triggers shape user behaviors, guiding developers in designing applications that empower users to make informed privacy and security decisions.

Another significant contribution is the emphasis on knowledge types (conceptual and procedural) and their role in enhancing user self-efficacy. We propose using techniques such as gamification and AR interfaces to build both knowledge types, making privacy and security concepts more transparent and more actionable for users. Our findings suggest that gamified elements can improve users' motivation to engage with privacy settings. At the same time, AR and visualization techniques aid in developing procedural knowledge, allowing users to navigate and apply these settings effectively.

Furthermore, this work explores how triggers, particularly those timed with users' contextual needs, can encourage timely actions in managing security settings. This research contributes insights into the importance of well-timed and context-sensitive notifications, which can reduce cognitive load and increase engagement with privacy tools. We also introduce augmented reality as a powerful tool to bridge users' conceptual understanding of data flows and procedural interactions with settings, enhancing confidence and self-efficacy in managing privacy and security tasks.

Lastly, the dissertation addresses a critical gap in the current design of privacy and security tools by identifying the need for transparency and user-centered design. Findings from our studies indicate that users feel more confident and trusting when privacy settings are presented transparently, supported by visual cues and interactive guidance. This work thus lays a foundation for privacy and security applications that are not only technically secure but also foster user autonomy, trust, and informed decision-making through intuitive, engaging, and contextually relevant design. The cumulative effect of these contributions points towards a future where privacy and security tools are embedded seamlessly in users' environments, helping them navigate increasingly complex digital landscapes with confidence and control.



Study Materials

This appendix provides all the questionnaires, tasks, and materials utilized across the various studies conducted as part of this dissertation. These instruments include detailed survey questions, task descriptions, and other relevant study materials. Each item has been included to offer transparency regarding the methodology and to enable replication or further exploration of the study designs.

A.1 Study 6

Demographic Data and User Experience

1. What is your gender?
2. How old are you?
3. Do you have any background knowledge of privacy and security? (training courses, profession)
4. How would you rate your knowledge of smartphones?
5. How would you rate your understanding of smartphone security and privacy?
6. How important is security and privacy to you when using smartphone devices?
7. How worried are you about the security of your own smartphone?
8. How would you install Android apps on your phone?
9. To what extent do you pay attention to the app description before installing it?
10. Do you know what dangerous permissions are? If so, could you please write them down?
11. Have you ever read an app's privacy policy before or after you install it?
12. Have you ever heard of the app TikTok?
13. Did you ever question the permissions, or did you always just click "Yes"? Did you consciously click on "Yes" or just to make the modal disappear?

Interview Structure

The interview is divided into four sections:

- **Section 1:** Testing the user's knowledge, focusing on awareness of information collection and usage within a pre-selected app.
- **Section 2:** Inspecting three scanning apps and the newly developed MASS scan app.

- **Section 3:** Scanning the pre-selected app from Section 1 with the user's favorite scanning app from Section 2.
- **Section 4:** User feedback on the interview process and scan apps.

Interviews

Interview Section 1: User Awareness

- **a.** Please explain the permissions of the app and their purposes.
- **b.** Based on your analysis, what kind of information could be collected?
- **c.** Do you know the destination of the collected data? If so, can you please provide details?
- **d.** Who can access the collected data, and for what purposes?
- **e.** Do you recognize any rights of the app's users?

Interview Section 2: Testing App Analyzers

- **a. General**
 1. Have you ever heard of App Analyzer?
 2. Which one?
 3. Did you use it?
- **b. Ranking**
 1. Do you understand all terms: privacy policy, permission, certificate, services, tracker, activities, user apps/all apps, third party, server, UID, package name, target SDK, APK?
 2. Sort them by personal importance.
- **c. Rating**
 1. What do you see?
 2. What is your first impression?
 3. Do you have ambiguities or open questions?
 4. Can you immediately understand everything touchable on the user interface?
 5. What do you like about it? Why?
 6. What do you dislike about it? Why?

7. Would you change or add something? Why?

• **d. Comparison**

1. Which one solicited a strong initial reaction from you? Why? (e.g., surprise, irritation, interest) [Emotional Response]
2. Which one did you understand most easily? Why? [Comprehensibility]
3. Which one contains the most useful information to you? Why? [Useful Information]
4. What was your overall favorite? Why? [Overall Favorite]

Interview Section 3: Analyzing TikTok

- **a.** Please explain the permissions of the app and their purposes.
- **b.** Based on your analysis, what kind of information could be collected?
- **c.** Do you know the destination of the collected data? If so, can you please provide details?
- **d.** Who can access the collected data, and for what purposes?
- **e.** Do you recognize any rights of the app's users?

Interview Section 4: Participants Feedback

- **a.** Do you have any feedback?

A.2 Study 7

Android Awareness Questions

- How do you usually install an app on your smartphone?
- What information do you look for before installing an app?
- Based on the previous question, how do you find this information?
- Do you pay attention to the permissions of a new app?
- Are you comfortable determining whether or not requested permissions are required?
- Do permissions affect your decision to download or use an app?
- How concerned are you about your privacy when installing a new app?
- Can you comfortably determine if an app violates your privacy?

Post-Exposure Questions: Overall Risk Assessment

- How do you assess the risk of the installed Flashlight app violating your privacy?
- How do you assess the risk of the installed Game app violating your privacy?
- How do you assess the risk of the installed Health & Fitness app violating your privacy?
- How do you assess the risk of the installed Social Media app violating your privacy?

Post-Exposure Questions: Categories Risk Assessment

- Which of the queries in the Flashlight app pose a risk to your privacy, and to what extent?
- Which of the queries in the Game app pose a risk to your privacy, and to what extent?
- Which of the queries in the Health & Fitness app pose a risk to your privacy, and to what extent?
- Which of the queries in the Social Media app pose a risk to your privacy, and to what extent?

Post-Exposure Questions: Feedback (App-Info group)

- The App-Info page displays information about installed apps in the Android settings. Do you use this page on your smartphone?
- How satisfied are you that the App-Info page contains enough security and privacy information about the specific app?
- On Android, you can manage permissions through settings. However, some settings in the apps can affect your privacy. Do you think Android needs a mechanism to indicate security and privacy concerns about an app?
- If you have an idea about such a mechanism based on the last question, please share how the Android settings or the Google Play Store should inform users about app privacy and security.

Post-Exposure Questions: Feedback (UDAP group)

- The UDAP page displays information about installed apps in the Android settings. Do you want to see and use it on your smartphone?
- How satisfied are you that the UDAP page contains enough security and privacy information about the specific app?
- On Android, you can manage permissions through settings. However, some settings in the apps can affect your privacy. Do you think Android needs the UDAP mechanism to indicate security and privacy concerns about an app?
- The UDAP mechanism can be implemented either in the Google Play Store or in the Android operating system. In which environment would you prefer this mechanism?
- Based on the last question, please indicate to what extent the UDAP should inform users about app privacy and security in Android settings or the Google Play Store.

A.3 Study 8

First Questionnaire: General Policies

1. What happens when the privacy policy changes?
2. What types of data are collected from you when using smart home devices?
3. Who can you contact with questions, suggestions, or complaints about the processing of your personal data?
4. Will your data be sent abroad (other countries)?
5. You have given consent to the collection of your data. Do you have the right to revoke it?

Second Questionnaire: User Rights

1. What are your rights in terms of deleting your own data?
2. When will your data be deleted?
3. What rights do you have regarding accessing your own data?
4. Who is the person responsible for processing your data?
5. Which reasons are not specifically given for the data processing?

Third Questionnaire: Device-Specific Policies

1. Will data be forwarded to third parties when using the Alarm Protection Starter Kit?
2. If voice assistants are intended to use the indoor camera, your voice commands will be sent to the camera. What kind of data could be shared with voice assistant companies?
3. While using the health device, you can prohibit access by external third parties. In such cases, what parts of your data could be affected?
4. You have the right to file a complaint with a data protection authority. In such cases, who should you contact?
5. The Health device is able to send sensitive data to your doctor. To do this, you must first give permission to the device. To what extent do you have access to your data?

A.4 Study 9

Self-Efficacy Questions

1. I feel confident in my ability to protect myself by using the privacy choices of my IP-Camera (Kang and Oh, 2023).
 2. I feel in control over the information I provide while setting up my IP-Camera (Kang and Oh, 2023).
 3. Privacy settings allow me to have full control over the information I provide on my IP-Camera (Kang and Oh, 2023).
 4. I feel in control of who can view my information on my IP-Camera (Kang and Oh, 2023).
-
1. I feel comfortable taking measures to secure my online payment (Thompson et al., 2017).
 2. Taking the necessary privacy measures is entirely under my control (Thompson et al., 2017).
 3. I have the resources and knowledge to take the necessary privacy measures (Thompson et al., 2017).
 4. I can protect my online payment by myself (Thompson et al., 2017).

1. I know how to evaluate online privacy policies (Lee and Kobsa, 2019).
2. I know how to change the privacy choices of this smart home webpage to increase privacy (Lee and Kobsa, 2019).
3. I am able to protect myself against the release of personal information (Lee and Kobsa, 2019).
4. I know how to block unwanted/marketing emails (Lee and Kobsa, 2019).
5. Overall, I am confident that I can protect my privacy online (Lee and Kobsa, 2019).

Perceived Privacy Protection Questions

1. This web application is collecting too much personal information from me (Kim et al., 2008).
2. This web application will use my personal information for other purposes without my authorization (Kim et al., 2008).
3. This web application will share my personal information with other entities without my authorization (Kim et al., 2008).
4. I am concerned about the privacy of my personal information during a transaction (Kim et al., 2008).
5. This web application will sell my personal information to others without my permission (Kim et al., 2008).

A.5 Study 13

A.5.1 AR Tasks

Introduction

Greetings and welcome to our study on Smart Home devices. We invite you to explore a few options and become familiar with their capabilities. To get started, kindly set up the router and Bosch Controller by scanning the QR code and consenting to the related privacy policy.

- Add Router.
- Router: Accept privacy policy.
- Add Bosch Controller.
- Bosch Controller: Accept privacy policy.

Privacy Settings (Easy)

Have you ever read a privacy policy before agreeing to it? If not, we have prepared a one-page summary of the privacy policy. Set up the IKEA lamp and review the privacy policy regarding data sharing with third-party companies. Check if data exchange occurs between the two clouds and turn off third-party data sharing in the settings.

- Add IKEA Lamp.
- IKEA Lamp: Accept privacy policy.
- Can you see the data exchange between the two clouds?
- Bosch Controller: Disable third-party data sharing.

Router Settings (Complex)

A router is essential for a smart home network. In this task, update the router firmware, change the security protocol to WPA3, check for open ports, and close them.

- Update the router firmware.
- Change security protocol to WPA3.

Smart Home Connections (Easy)

Set up the Google Nest Camera and inspect its connection to the cloud. Check if the data flow over the network is encrypted and stored anonymously in the cloud. If not, adjust the settings to enable a VPN for added security.

- Add Google Nest Camera.
- Google Nest Camera: Accept privacy policy.
- Inspect its connection to the cloud.
- Is the data stored encrypted or anonymously?
- Enable encrypted connection.
- Enable anonymous data storage.
- Enable VPN connection for the device.

Update (Easy)

Protect against vulnerabilities by updating firmware on all smart home devices. For the Bosch Motion Detector, postpone the update to a later time.

- Update all devices.
- Postpone the update for the Bosch Motion Detector.

User Management (Easy)

Grant access to your new roommate “Kim” by adding a user account. Additionally, create a guest account for “Robin.”

- Add a user account for “Kim.”
- Add a guest account for “Robin.”

Credential Management (Complex)

Add Alexa and agree to the privacy policy. Connect Alexa with the Bosch Controller and check for data exchange between the two clouds. If you plan to give Alexa to a friend, disconnect it by deleting your credentials from the Bosch Controller.

- Add Alexa.
- Alexa: Accept privacy policy.
- Can you see the data exchange between the two clouds?
- Bosch Controller: Delete credentials.

Device Validation (Complex)

Verify all smart home devices for authenticity and establish a secure connection between Bosch devices by renewing the verification key.

- Check for verified signatures.
- Renew verification key for Bosch devices.

Managing Privacy (Complex)

Check what personal data is stored in the Bosch Cloud. Delete personal and telemetry data, and revoke consent to the privacy policy to stop data sharing with the service provider.

- Check data in the Bosch Cloud.
- Delete personal data.
- Revoke consent.

Vulnerabilities (Complex)

As an administrator, set a password policy of 8-20 characters, including an uppercase letter, a number, and a special character. Limit the number of authentication attempts to three for all users.

- Set password policy.
- Limit authentication attempts.

A.5.2 Participant Mental Model

Drawing Exercise

Draw how smart home devices collect information and show how data flows between devices and other entities involved.

Data Collection

- What information is collected by the device?
- Is the data collection necessary? If so, for what purpose?

Data Storage

- Where is the data transmitted and stored? For how long?
- Can you check what data is stored? Do you have control over it?
- Is it possible to remove stored data? Have you considered doing so?

Data Sharing

- Does the manufacturer share data with other companies? If so, with whom and for what reasons?

Data Inference

- How might third parties use your data? What concerns do you have about this?

Mitigation Techniques

- What controls do you have over your data? Are they easy to use?
- What additional controls would you like to have regarding data privacy?

B

Publications

- Bahrini, M., Weglewski, J., Sohr, K., & Malaka, R. (2024). Empowering User Security Awareness and Risk Assessment Within Gamified Smartphone Environment. In Entertainment Computing – ICEC 2024. 23rd IFIP TC 14 International Conference, ICEC 2024, Manaus/Amazonas, Brazil, September 30th - October 3rd, 2024. (pp. 16-34) Springer International Publishing.
- Kohn, M., Freye, M., Bahrini, M. & Herbst, A. (2023, September). Gesundheits-Apps auf dem Prüfstand –Überprüfung der Angaben in Datenschutzerklärungen zur Datenweitergabe. INFORMATIK 2023 - Designing Futures: Zukünfte gestalten. Bonn: Gesellschaft für Informatik e.V. (pp. 677-688). Cybersecurity & Privatsphäre - Recht und Technik. Datenschutz im Diskurs (RuT2023). Berlin. 26.-29.
- Bahrini, M., Münder, T., Sohr, K., & Malaka, R. (2023). Verständliche Informationssicherheit in Smarthome-Netzen: Herausforderungen, Lösungen und Ausblick. Datenschutz und Datensicherheit-DuD, 47(6), (pp. 350-353).
- Bahrini, M., Zargham, N., Wolff, A., Kipker, D. K., Sohr, K., & Malaka, R. (2022, October). It's Long and Complicated! Enhancing One-Pager Privacy Policies in Smart Home Applications. In Nordic Human-Computer Interaction Conference (pp. 1-13).

- Reichmann, H., Elson, M., Borgert, N., Kipker, D. K., Malaka, R., Sohr, K., & Bahrini, M. (2021). Erfahrbarer Datenschutz und IT-Sicherheit in Smart Home-Anwendungen. *Datenschutz und Datensicherheit-DuD*, 45(4), (pp. 259-264).
- Bahrini, M., Zargham, N., Pfau, J., Lemke, S., Sohr, K., & Malaka, R. (2020, November). Good vs. evil: Investigating the effect of game premise in a smart home security educational game. In *Extended Abstracts of the 2020 Annual Symposium on Computer-Human Interaction in Play* (pp. 182-187).
- Bahrini, M., Zargham, N., Pfau, J., Lemke, S., Sohr, K., & Malaka, R. (2020). Enhancing game-based learning through infographics in the context of smart home security. In *Entertainment Computing-ICEC 2020: 19th IFIP TC 14 International Conference, ICEC 2020, Xi'an, China, November 10-13, 2020, Proceedings 19* (pp. 18-36). Springer International Publishing.
- Zargham, N., Bahrini, M., Volkmar, G., Wenig, D., Sohr, K., & Malaka, R. (2019, October). What could go wrong? raising mobile privacy and security awareness through a decision-making game. In *Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts* (pp. 805-812).
- Bahrini, M., Volkmar, G., Schmutte, J., Wenig, N., Sohr, K., & Malaka, R. (2019). Make my phone secure! Using gamification for mobile security settings. In *Proceedings of Mensch und Computer 2019* (pp. 299-308).
- Bahrini, M., Wenig, N., Meissner, M., Sohr, K., & Malaka, R. (2019, May). HappyPerMi: Presenting critical data flows in mobile application to raise user security awareness. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-6).

References

- Aarseth, E. (2014). *I Fought the Law: Transgressive Play and the Implied Player*, pages 180–188. Palgrave Macmillan UK, London.
- Abras, C., Maloney-Krichmar, D., Preece, J., et al. (2004). User-centered design. *Bainbridge, W. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage Publications*, 37(4):445–456.
- Abt, C. C. (1987). *Serious games*. University press of America.
- Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., and Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users’ choices online. *ACM Comput. Surv.*, 50(3).
- Adaji, I. and Adisa, M. (2022). A review of the use of persuasive technologies to influence sustainable behaviour. In *Adjunct Proceedings of the 30th ACM Conference on User Modeling, Adaptation and Personalization, UMAP '22 Adjunct*, page 317–325, New York, NY, USA. Association for Computing Machinery.
- Adams, W. C. (2015). *Conducting Semi-Structured Interviews*, chapter 19, pages 492–505. John Wiley & Sons, Ltd.
- Ahmad Faudzi, M., Che Cob, Z., Omar, R., Sharudin, S. A., and Ghazali, M. (2023). Investigating the user interface design frameworks of current mobile learning applications: A systematic review. *Education Sciences*, 13(1).
- Ajzen, I. (1980). Understanding attitudes and predictiing social behavior. *Englewood cliffs*.
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2):179–211. Theories of Cognitive Self-Regulation.

REFERENCES

- Al-Azawi, R., Al-Faliti, F., and Al-Blushi, M. (2016). Educational gamification vs. game based learning: Comparative study. *International journal of innovation, management and technology*, 7(4):132–136.
- Al Muhandar, B., Wiese, J., Rana, O., and Perera, C. (2023). Interactive privacy management: Toward enhancing privacy awareness and control in the internet of things. *ACM Trans. Internet Things*, 4(3).
- AlMarshedi, A., Wanick, V., Wills, G. B., and Ranchhod, A. (2017). *Gamification and Behaviour*, pages 19–29. Springer International Publishing, Cham.
- Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L. F., and Agarwal, Y. (2015). Your location has been shared 5,398 times! a field study on mobile app privacy nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, page 787–796, New York, NY, USA. Association for Computing Machinery.
- Almusaylim, Z. A. and Zaman, N. (2019). A review on smart home present state and challenges: linked to context-awareness internet of things (iot). *Wireless networks*, 25(6):3193–3204.
- Alnajim, A. M., Habib, S., Islam, M., AlRawashdeh, H. S., and Wasim, M. (2023). Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches. *Symmetry*, 15(12).
- Alqahtani, H. and Kavakli-Thorne, M. (2020a). Design and evaluation of an augmented reality game for cybersecurity awareness (cybar). *Information*, 11(2).
- Alqahtani, H. and Kavakli-Thorne, M. (2020b). Exploring factors affecting user’s cybersecurity behaviour by using mobile augmented reality app (cybar). In *Proceedings of the 2020 12th International Conference on Computer and Automation Engineering*, ICCAE 2020, page 129–135, New York, NY, USA. Association for Computing Machinery.
- Alrwele, N. S. (2017). Effects of infographics on student achievement and students’ perceptions of the impacts of infographics. *Journal of Education and Human Development*, 6(3):104–117.

REFERENCES

- Alsawaier, R. S. (2018). The effect of gamification on motivation and engagement. *The International Journal of Information and Learning Technology*, 35(1):56–79.
- Alsoubai, A., Ghaiumy Anaraky, R., Li, Y., Page, X., Knijnenburg, B., and Wisniewski, P. J. (2022). Permission vs. app limiters: Profiling smartphone users to understand differing strategies for mobile privacy management. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA. Association for Computing Machinery.
- Ammari, T., Kaye, J., Tsai, J. Y., and Bentley, F. (2019). Music, search, and iot: How people (really) use voice assistants. *ACM Trans. Comput.-Hum. Interact.*, 26(3).
- Amos, R., Acar, G., Lucherini, E., Kshirsagar, M., Narayanan, A., and Mayer, J. (2021). Privacy policies over time: Curation and analysis of a million-document dataset. In *Proceedings of the Web Conference 2021*, WWW '21, page 2165–2176, New York, NY, USA. Association for Computing Machinery.
- Anderson, K. E. (2020). Getting acquainted with social networks and apps: it is time to talk about tiktok. *Library hi tech news*, 37(4):7–12.
- Andow, B., Mahmud, S. Y., Wang, W., Whitaker, J., Enck, W., Reaves, B., Singh, K., and Xie, T. (2019). PolicyLint: Investigating internal privacy policy contradictions on google play. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 585–602, Santa Clara, CA. USENIX Association.
- Annetta, L. A. (2010). The “i’s” have it: A framework for serious educational game design. *Review of General Psychology*, 14(2):105–113.
- Appfigures and Statista (2022). Google play most popular app categories 2022. <https://www.statista.com/statistics/279286/google-play-android-app-categories/>. Accessed: 2024-3-27.
- Arachchilage, N. A. G. and Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38:304–312.
- Arena, F., Collotta, M., Pau, G., and Termine, F. (2022). An overview of augmented reality. *Computers*, 11(2).

REFERENCES

- Arzt, S., Rasthofer, S., Fritz, C., Bodden, E., Bartel, A., Klein, J., Le Traon, Y., Octeau, D., and McDaniel, P. (2014). Flowdroid: precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps. In *Proceedings of the 35th ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI '14*, page 259–269, New York, NY, USA. Association for Computing Machinery.
- Attig, C., Wessel, D., and Franke, T. (2017). Assessing personality differences in human-technology interaction: An overview of key self-report scales to predict successful interaction. In Stephanidis, C., editor, *HCI International 2017 – Posters' Extended Abstracts*, pages 19–29, Cham. Springer International Publishing.
- Bachy, Y., Nicomette, V., Kaâniche, M., and Alata, E. (2019). Smart-tv security: risk analysis and experiments on smart-tv communication channels. *Journal of Computer Virology and Hacking Techniques*, 15(1):61–76.
- Bada, M., Sasse, A. M., and Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?
- Bagheri, H., Sadeghi, A., Garcia, J., and Malek, S. (2015). Covert: Compositional analysis of android inter-app permission leakage. *IEEE Transactions on Software Engineering*, 41(9):866–886.
- Bahrini, M., Volkmar, G., Schmutte, J., Wenig, N., Sohr, K., and Malaka, R. (2019a). Make my phone secure! using gamification for mobile security settings. In *Proceedings of Mensch Und Computer 2019, MuC '19*, page 299–308, New York, NY, USA. Association for Computing Machinery.
- Bahrini, M., Wenig, N., Meissner, M., Sohr, K., and Malaka, R. (2019b). Happypermi: Presenting critical data flows in mobile application to raise user security awareness. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, CHI EA '19*, page 1–6, New York, NY, USA. Association for Computing Machinery.
- Bahrini, M., Zargham, N., Wolff, A., Kipker, D.-K., Sohr, K., and Malaka, R. (2022). It's long and complicated! enhancing one-pager privacy policies in smart home applications. In *Nordic Human-Computer Interaction Conference, NordiCHI '22*, New York, NY, USA. Association for Computing Machinery.
- Bailey, M., Dittrich, D., Kenneally, E., and Maughan, D. (2012). The menlo report. *IEEE Security and Privacy*, 10(2):71–75.

REFERENCES

- Balagtas-Fernandez, F., Forrai, J., and Hussmann, H. (2009). Evaluation of user interface design and input methods for applications on mobile touch screen devices. In Gross, T., Gulliksen, J., Kotzé, P., Oestreicher, L., Palanque, P., Prates, R. O., and Winckler, M., editors, *Human-Computer Interaction – INTERACT 2009*, pages 243–246, Berlin, Heidelberg. Springer Berlin Heidelberg.
- Balebako, R., Jung, J., Lu, W., Cranor, L. F., and Nguyen, C. (2013). "little brothers watching you": raising awareness of data leaks on smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security, SOUPS '13*, New York, NY, USA. Association for Computing Machinery.
- Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review*, 84(2):191–215.
- Bandura, A. (1982). Self-efficacy mechanism in human agency. *American psychologist*, 37(2):122–147.
- Bandura, A. (1986). Social foundations of thought and action: A social cognitive theory. *Englewood Cliffs, NJ*, 1986(23-28).
- Bandura, A. (2004). Health promotion by social cognitive means. *Health Education & Behavior*, 31(2):143–164. PMID: 15090118.
- Bandura, A. (2012). *Cultivate Self-efficacy for Personal and Organizational Effectiveness*, chapter 10, pages 179–200. John Wiley & Sons, Ltd.
- Bandura, A., Freeman, W. H., and Lightsey, R. (1999). Self-efficacy: The exercise of control. *Journal of Cognitive Psychotherapy*, 13(2):158–166.
- Bandura, A. and Walters, R. H. (1977). *Social learning theory*, volume 1. Englewood cliffs Prentice Hall.
- Baragash, R. S., Al-Samarraie, H., Moody, L., and Zaqout, F. (2022). Augmented reality and functional skills acquisition among individuals with special needs: A meta-analysis of group design studies. *Journal of Special Education Technology*, 37(1):74–81.
- Baral, G. and Arachchilage, N. A. G. (2019). Building confidence not to be phished through a gamified approach: Conceptualising user's self-efficacy in phishing threat avoidance behaviour. In *2019 Cybersecurity and Cyberforensics Conference (CCC)*, pages 102–110.
- Barker, S. (2017). "flashlight" trojan targets australian banking apps, takes pictures of victims.

REFERENCES

- Barr, M. (2017). Video games can develop graduate skills in higher education students: A randomised trial. *Computers & Education*, 113:86–97.
- Barral, O., Kosunen, I., and Jacucci, G. (2017). No need to laugh out loud: Predicting humor appraisal of comic strips based on physiological signals in a realistic environment. *ACM Trans. Comput.-Hum. Interact.*, 24(6):40:1–40:29.
- Barth, S., de Jong, M. D., Junger, M., Hartel, P. H., and Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, 41:55–69.
- Bashir, R. N., Qadri, S., Saleem, R. M., Naeem, M., and Ghafoor, Y. (2014). Human computer interaction (hci) in ubiquitous computing. *International Journal of Innovation and Applied Studies*, 9(2):534.
- Bateman, S., Mandryk, R. L., Gutwin, C., Genest, A., McDine, D., and Brooks, C. (2010). Useful junk?: The effects of visual embellishment on comprehension and memorability of charts. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '10*, pages 2573–2582, New York, NY, USA. ACM.
- Bauer, M., Glenn, T., Geddes, J., Gitlin, M., Grof, P., Kessing, L. V., Monteith, S., Faurholt-Jepsen, M., Severus, E., and Whybrow, P. C. (2020). Smartphones in mental health: a critical review of background issues, current status and future concerns. *International Journal of Bipolar Disorders*, 8(1):2.
- Berisford, C. J., Blackburn, L., Ollett, J. M., Tonner, T. B., Yuen, C. S. H., Walton, R., and Olayinka, O. (2022). Can gamification help to teach cybersecurity? In *2022 20th International Conference on Information Technology Based Higher Education and Training (ITHET)*, pages 1–9.
- Bermejo Fernandez, C., Lee, L. H., Nurmi, P., and Hui, P. (2021). Para: Privacy management and control in emerging iot ecosystems using augmented reality. In *Proceedings of the 2021 International Conference on Multimodal Interaction, ICMI '21*, page 478–486, New York, NY, USA. Association for Computing Machinery.
- Bhattacharya, M., Roy, S., Chattopadhyay, S., Das, A. K., and Shetty, S. (2023). A comprehensive survey on online social networks security and privacy issues: Threats, machine learning-based solutions, and open challenges. *SECURITY AND PRIVACY*, 6(1):e275.

REFERENCES

- Billinghurst, M., Clark, A., and Lee, G. (2015). A survey of augmented reality. *Foundations and Trends® in Human-Computer Interaction*, 8(2-3):73–272.
- Bloustein, E. J. (1964). Privacy as an aspect of human dignity: An answer to dean prosser. *NYUL rev.*, 39:962.
- Bongard-Blanchy, K., Rossi, A., Rivas, S., Doublet, S., Koenig, V., and Lenzi, G. (2021). "i am definitely manipulated, even when i am aware of it. it's ridiculous!" - dark patterns from the end-user perspective. In *Proceedings of the 2021 ACM Designing Interactive Systems Conference*, DIS '21, page 763–776, New York, NY, USA. Association for Computing Machinery.
- Boopathi, K., Sreejith, S., and Bithin, A. (2015). Learning cyber security through gamification. *Indian Journal of Science and Technology*, 8(7):642–649.
- Bopp, J. A., Mekler, E. D., and Opwis, K. (2016). Negative emotion, positive experience? emotionally moving moments in digital games. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, page 2996–3006, New York, NY, USA. Association for Computing Machinery.
- Borgert, N., Reithmaier, O. D., Jansen, L., Hillemann, L., Hussey, I., and Elson, M. (2023). Home is where the smart is: Development and validation of the cybersecurity self-efficacy in smart homes (cysesh) scale. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA. Association for Computing Machinery.
- Borgesius, F. Z. (2017). The breyer case of the court of justice of the european union: Ip addresses and the personal data definition. *Eur. Data Prot. L. Rev.*, 3:130.
- Bosu, A., Liu, F., Yao, D. D., and Wang, G. (2017). Collusive data leak and more: Large-scale threat analysis of inter-app communications. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '17, page 71–85, New York, NY, USA. Association for Computing Machinery.
- Bourgonjon, J., De Grove, F., De Smet, C., Van Looy, J., Soetaert, R., and Valcke, M. (2013). Acceptance of game-based learning by secondary school teachers. *Computers & Education*, 67:21–35.

REFERENCES

- Bradley, M. M. and Lang, P. J. (1994). Measuring emotion: The self-assessment manikin and the semantic differential. *Journal of Behavior Therapy and Experimental Psychiatry*, 25(1):49–59.
- Breitinger, F., Tully-Doyle, R., and Hassenfeldt, C. (2020). A survey on smartphone user’s security choices, awareness and education. *Computers & Security*, 88:101647.
- Brodie, C., Karat, C.-M., Karat, J., and Feng, J. (2005). Usable security and privacy: A case study of developing privacy management tools. In *Proceedings of the 2005 Symposium on Usable Privacy and Security, SOUPS '05*, page 35–43, New York, NY, USA. Association for Computing Machinery.
- Brooke, J. (1996). Sus-a quick and dirty usability scale. *Usability evaluation in industry*, 189(194):4–7.
- Bugeja, J., Jacobsson, A., and Davidsson, P. (2016). On privacy and security challenges in smart connected homes. In *2016 European Intelligence and Security Informatics Conference (EISIC)*, pages 172–175.
- Böhm, F., Dietz, M., Preindl, T., and Pernul, G. (2021). Augmented reality and the digital twin: State-of-the-art and perspectives for cybersecurity. *Journal of Cybersecurity and Privacy*, 1(3):519–538.
- Bösch, C., Erb, B., Kargl, F., Kopp, H., and Pfattheicher, S. (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies*, 2016:237–254.
- Caboni, F. and Hagberg, J. (2019). Augmented reality in retailing: a review of features, applications and value. *International Journal of Retail & Distribution Management*, 47(11):1125–1140.
- Calzavara, S., Grishchenko, I., and Maffei, M. (2016). Horndroid: Practical and sound static analysis of android applications by smt solving. In *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 47–62.
- Canova, G., Volkamer, M., Bergmann, C., and Borza, R. (2014). Nophish: An anti-phishing education app. In Mauw, S. and Jensen, C. D., editors, *Security and Trust Management*, pages 188–192, Cham. Springer International Publishing.
- Cao, W., Xia, C., Peddinti, S. T., Lie, D., Taft, N., and Austin, L. M. (2021). A large scale study of user behavior, expectations and engagement with

REFERENCES

- android permissions. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 803–820. USENIX Association.
- Carlini, N., Mishra, P., Vaidya, T., Zhang, Y., Sherr, M., Shields, C., Wagner, D., and Zhou, W. (2016). Hidden voice commands. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 513–530, Austin, TX. USENIX Association.
- Carre, J. R., Curtis, S. R., and Jones, D. N. (2018). Ascribing responsibility for online security and data breaches. *Managerial Auditing Journal*, 33(4):436–446.
- Cassidy, S. and Eachus, P. (2002). Developing the computer user self-efficacy (cuse) scale: Investigating the relationship between computer self-efficacy, gender and experience with computers. *Journal of Educational Computing Research*, 26(2):133–153.
- Catal, C., Ozcan, A., Donmez, E., and Kasif, A. (2023). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education and Information Technologies*, 28(2):1809–1831.
- Chakraborty, A., Islam, M., Shahriyar, F., Islam, S., Zaman, H. U., and Hasan, M. (2023). Smart home system: A comprehensive review. *Journal of Electrical and Computer Engineering*, 2023(1):7616683.
- Chalhoub, G., Flechais, I., Nthala, N., Abu-Salma, R., and Tom, E. (2020). Factoring user experience into the security and privacy design of smart home devices: A case study. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI EA '20, page 1–9, New York, NY, USA. Association for Computing Machinery.
- Chang, C.-Y. and Hwang, G.-J. (2019). Trends in digital game-based learning in the mobile era: a systematic review of journal publications from 2007 to 2016. *International Journal of Mobile Learning and Organisation*, 13(1):68–90.
- Chang, J. C., Kim, Y., Miller, V., Liu, M. X., Myers, B. A., and Kittur, A. (2021). *Tabs.Do: Task-Centric Browser Tab Management*, page 663–676. Association for Computing Machinery, New York, NY, USA.
- Charsky, D. (2010). From edutainment to serious games: A change in the use of game characteristics. *Games and Culture*, 5(2):177–198.

REFERENCES

- Charters, E. (2003). The use of think-aloud methods in qualitative research an introduction to think-aloud methods. *Brock Education Journal*, 12(2).
- Chen, T., Hammer, J., and Dabbish, L. (2019). Self-efficacy-based game design to encourage security behavior online. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI EA '19, New York, NY, USA. Association for Computing Machinery.
- Chen, Y. (2018). Understanding how educational gamification impacts users' behavior: a theoretical analysis. In *Proceedings of the 6th International Conference on Information and Education Technology*, ICIET '18, page 154–159, New York, NY, USA. Association for Computing Machinery.
- Chen, Y., Zahedi, F., and Abbasi, A. (2011). Interface design elements for anti-phishing systems. In *Service-Oriented Perspectives in Design Science Research*, DESRIST'11, page 253–265, Berlin, Heidelberg. Springer-Verlag.
- Cheng, P. and Roedig, U. (2022). Personal voice assistant security and privacy—a survey. *Proceedings of the IEEE*, 110(4):476–507.
- Chitkara, S., Gothoskar, N., Harish, S., Hong, J. I., and Agarwal, Y. (2017). Does this app really need my location? context-aware privacy management for smartphones. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 1(3).
- Choe, E. K., Jung, J., Lee, B., and Fisher, K. (2013). Nudging people away from privacy-invasive mobile apps through visual framing. In Kotzé, P., Marsden, G., Lindgaard, G., Wesson, J., and Winckler, M., editors, *Human-Computer Interaction – INTERACT 2013*, pages 74–91, Berlin, Heidelberg. Springer Berlin Heidelberg.
- Chung, K.-C., Chen, C.-H., Tsai, H.-H., and Chuang, Y.-H. (2021). Social media privacy management strategies: A sem analysis of user privacy behaviors. *Computer Communications*, 174:122–130.
- Claesson, A. and Bjørstad, T. E. (2020). Out of control—a review of data sharing by popular mobile apps. *Oslo: Norwegian Consumer Council*.
- Claesson, A. and Bjørstad, T. E. (2020). “Out of Control” – a review of data sharing by popular mobile apps. Technical report, Norwegian Consumer Council, Oslo.
- Clark, J. W., Snyder, P., McCoy, D., and Kanich, C. (2015). “i saw images i didn’t even know i had”: Understanding user perceptions of cloud storage

REFERENCES

- privacy. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, page 1641–1644, New York, NY, USA. Association for Computing Machinery.
- Colbourn, C. J. and Dinitz, J. H. (2006). *Handbook of Combinatorial Designs*. CRC press.
- Colella, A. and Colombini, C. (2012). Security paradigm in ubiquitous computing. In *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pages 634–638.
- Cone, B. D., Irvine, C. E., Thompson, M. F., and Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security*, 26(1):63 – 72.
- Conner, M. and Norman, P. (2015). *Predicting and changing health behaviour: research and practice with social cognition models*. McGraw-hill education (UK).
- Consolvo, S., Bentley, F. R., Hekler, E. B., and Phatak, S. S. (2017). *Using Theory in Mobile User Research*, pages 133–156. Springer International Publishing, Cham.
- Conti, G. and Sobiesk, E. (2010). Malicious interface design: exploiting the user. In *Proceedings of the 19th International Conference on World Wide Web*, WWW '10, page 271–280, New York, NY, USA. Association for Computing Machinery.
- Corrales Compagnucci, M., Fenwick, M., Haapio, H., and Vermeulen, E. P. M. (2022). Integrating law, technology, and design: teaching data protection and privacy law in a digital age. *International Data Privacy Law*, 12(3):239–252.
- Costin, A. (2016). Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations. In *Proceedings of the 6th International Workshop on Trustworthy Embedded Devices*, TrustED '16, page 45–54, New York, NY, USA. Association for Computing Machinery.
- Creswell, J. W. (2021). *A concise introduction to mixed methods research*. SAGE publications.
- Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *psychometrika*, 16(3):297–334.

REFERENCES

- Cuthbertson, A. (2019). La liga “secretly listened through people’s microphones” to catch out pirates illegally streaming games.
- Darejeh, A. and Singh, D. (2013). A review on user interface design principles to increase software usability for users with less computer literacy. *Journal of computer science*, 9(11):1443.
- Das, A. and Khan, H. U. (2016). Security behaviors of smartphone users. *Information & Computer Security*, 24(1):116–134.
- Davidavičienė, V., Raudeliūnienė, J., and Viršilaitė, R. (2021). Evaluation of user experience in augmented reality mobile applications. *Journal of business economics and management*, 22(2):467–481.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3):319–340.
- Denning, T., Lerner, A., Shostack, A., and Kohno, T. (2013). Control-alt-hack: the design and evaluation of a card game for computer security awareness and education. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, CCS '13*, page 915–928, New York, NY, USA. Association for Computing Machinery.
- Deterding, S., Dixon, D., Khaled, R., and Nacke, L. (2011). From game design elements to gamefulness: Defining “gamification”. In *Proceedings of the 15th international academic MindTrek conference: Envisioning future media environments, MindTrek '11*, page 9–15, New York, NY, USA. Association for Computing Machinery.
- Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., and Bacchelli, A. (2020). *UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception*, page 1–14. Association for Computing Machinery, New York, NY, USA.
- Diercks, N. (2015). Der „one pager“ des bundesministeriums der justiz und für verbraucherschutz (bmjv) – die schnelle und einfache alternative zur datenschutzklärung? <https://t1p.de/w3i0v>. Accessed: 2024.05.12.
- Dimara, E. and Perin, C. (2020). What is interaction for data visualization? *IEEE Transactions on Visualization and Computer Graphics*, 26(1):119–129.
- Distler, V., Lallemand, C., and Koenig, V. (2020). Making encryption feel secure: Investigating how descriptions of encryption impact perceived

REFERENCES

- security. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 220–229, Genoa, Italy. IEEE.
- Distler, V., Zollinger, M.-L., Lallemand, C., Roenne, P. B., Ryan, P. Y. A., and Koenig, V. (2019). Security - visible, yet unseen? In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–13, New York, NY, USA. Association for Computing Machinery.
- Dixon, M., Gamagedara Arachchilage, N. A., and Nicholson, J. (2019). Engaging users with educational games: The case of phishing. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI EA '19, New York, NY, USA. Association for Computing Machinery.
- Dodd, E. (2023). A natural progression? Why there are so many data centres in Ireland — buzz.ie. <https://www.buzz.ie/news/irish-news/data-centres-ireland-economy-energy-25529167>. [Accessed 30-05-2024].
- Dormann, C., Barr, P., and Biddle, R. (2006). Humour theory and videogames: Laughter in the slaughter. In *Proceedings of the 2006 ACM SIGGRAPH Symposium on Videogames, Sandbox '06*, pages 95–98, New York, NY, USA. ACM.
- Dormann, C. and Biddle, R. (2006). Humour in game-based learning. *Learning, Media and Technology*, 31(4):411–424.
- Dormann, C. and Biddle, R. (2009). A review of humor for computer games: Play, laugh and more. *Simulation & Gaming*, 40(6):802–824.
- Dutson, J., Allen, D., Eggett, D., and Seamons, K. (2019). Don't punish all of us: Measuring user attitudes about two-factor authentication. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 119–128.
- Eberhard, K. (2023). The effects of visualization on judgment and decision-making: a systematic literature review. *Management Review Quarterly*, 73(1):167–214.
- Ebert, N., Alexander Ackermann, K., and Scheppler, B. (2021). Bolder is better: Raising user awareness through salient and concise privacy notices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA. Association for Computing Machinery.

REFERENCES

- Edwards, J. R. (1992). A cybernetic theory of stress, coping, and well-being in organizations. *Academy of management review*, 17(2):238–274.
- Egelman, S., Cranor, L. F., and Hong, J. (2008). You’ve been warned: An empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI ’08, page 1065–1074, New York, NY, USA. Association for Computing Machinery.
- Egelman, S., Felt, A. P., and Wagner, D. (2013). *Choice Architecture and Smartphone Privacy: There’s a Price for That*, pages 211–236. Springer Berlin Heidelberg, Berlin, Heidelberg.
- Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P., and Sheth, A. N. (2014). Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones. *ACM Trans. Comput. Syst.*, 32(2).
- European Commission (2024). What is personal data? — commission.europa.eu. https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en. [Accessed 31-05-2024].
- Fabian, B., Ermakova, T., and Lentz, T. (2017). Large-scale readability analysis of privacy policies. In *Proceedings of the International Conference on Web Intelligence*, WI ’17, page 18–25, New York, NY, USA. Association for Computing Machinery.
- Fagan, M. and Khan, M. M. H. (2016). Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 59–75, Denver, CO. USENIX Association.
- Fahl, S., Harbach, M., Muders, T., Baumgärtner, L., Freisleben, B., and Smith, M. (2012). Why eve and mallory love android: an analysis of android ssl (in)security. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS ’12, page 50–61, New York, NY, USA. Association for Computing Machinery.
- Faul, F., Erdfelder, E., Lang, A.-G., and Buchner, A. (2007). G* power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior research methods*, 39(2):175–191.

REFERENCES

- Faurie, P., Moldovan, A.-N., and Tal, I. (2020). Privacy policy – “i agree”?! – do alternatives to text-based policies increase the awareness of the users?
- Feldner, D. (2020). Redesigning organizations.
- Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., and Wagner, D. (2012). Android permissions: User attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security, SOUPS '12*, pages 3:1–3:14, New York, NY, USA. ACM.
- Felt, A. P., Reeder, R. W., Ainslie, A., Harris, H., Walker, M., Thompson, C., Acer, M. E., Morant, E., and Consolvo, S. (2016). Rethinking connection security indicators. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 1–14, Denver, CO. USENIX Association.
- Feng, Y., Yao, Y., and Sadeh, N. (2021). A design space for privacy choices: Towards meaningful privacy control in the internet of things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, CHI '21*, New York, NY, USA. Association for Computing Machinery.
- Fernández Galeote, D., Legaki, N.-Z., and Hamari, J. (2023). From traditional to game-based learning of climate change: A media comparison experiment. *Proc. ACM Hum.-Comput. Interact.*, 7(CHI PLAY).
- Ferre, X. (2003). Integration of usability techniques into the software development process. In *ICSE Workshop on SE-HCI*, pages 28–35.
- Finck, M. and Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the gdpr. *International Data Privacy Law*, 10(1):11–36.
- Fisher, R. A. (1970). Statistical methods for research workers. In *Breakthroughs in statistics: Methodology and distribution*, pages 66–70. Springer.
- Fogg, B. (2009). A behavior model for persuasive design. In *Proceedings of the 4th International Conference on Persuasive Technology, Persuasive '09*, New York, NY, USA. Association for Computing Machinery.
- Fogg, B. J. (2002). Persuasive technology: Using computers to change what we think and do. *Ubiquity*, 2002(December).
- Folmer, E. and Bosch, J. (2004). Architecting for usability: a survey. *Journal of Systems and Software*, 70(1):61–78.

REFERENCES

- Forget, A., Pearman, S., Thomas, J., Acquisti, A., Christin, N., Cranor, L. F., Egelman, S., Harbach, M., and Telang, R. (2016). Do or do not, there is no try: User engagement may not improve security outcomes. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 97–111, Denver, CO. USENIX Association.
- Fox, K. (2022). Ireland’s data centers are an economic lifeline. But environmentalists say they’re wrecking the planet — CNN Business — edition.cnn.com. <https://edition.cnn.com/2022/01/23/tech/ireland-data-centers-climate-intl-cmd/index.html>. [Accessed 30-05-2024].
- Francia, G., Thornton, D., Trifas, M., and Bowden, T. (2014). Chapter 5 - gamification of information security awareness training. In Akhgar, B. and Arabnia, H. R., editors, *Emerging Trends in ICT Security*, pages 85–97. Morgan Kaufmann, Boston.
- Franke, T., Attig, C., and Wessel, D. (2019). A personal resource for technology interaction: Development and validation of the affinity for technology interaction (ati) scale. *International Journal of Human-Computer Interaction*, 35(6):456–467.
- Frik, A., Kim, J., Sanchez, J. R., and Ma, J. (2022). Users’ expectations about and use of smartphone privacy and security settings. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI ’22, New York, NY, USA. Association for Computing Machinery.
- Fryling, M. J., Johnston, C., and Hayes, L. J. (2011). Understanding observational learning: An interbehavioral approach. *The Analysis of verbal behavior*, 27:191–203.
- Fu, K., Kohno, T., Lopresti, D., Mynatt, E., Nahrstedt, K., Patel, S., Richardson, D., and Zorn, B. (2017). Safety, security, and privacy threats posed by accelerating trends in the internet of things. *Computing Community Consortium (CCC) Technical Report*, 29(3).
- Fullerton, T. (2014). *Game design workshop: a playcentric approach to creating innovative games*. CRC press.
- Gajrani, J., Laxmi, V., Tripathi, M., Gaur, M. S., Zemmari, A., Mosbah, M., and Conti, M. (2020). Effectiveness of state-of-the-art dynamic analysis techniques in identifying diverse android malware and future enhancements. In Hurson, A. R., editor, *Advances in Computers*, volume 119, pages 73–120. Elsevier.

REFERENCES

- Garneli, V., Giannakos, M., and Chorianopoulos, K. (2017). Serious games as a malleable learning medium: The effects of narrative, gameplay, and making on students' performance and attitudes. *British Journal of Educational Technology*, 48(3):842–859.
- Gee, J. P. (2003). What video games have to teach us about learning and literacy. *Comput. Entertain.*, 1(1):20.
- Gerber, N., Gerber, P., Drews, H., Kirchner, E., Schlegel, N., Schmidt, T., and Scholz, L. (2018). Foxit: enhancing mobile users' privacy behavior by increasing knowledge and awareness. In *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust, STAST '17*, page 53–63, New York, NY, USA. Association for Computing Machinery.
- Gerlitz, E., Häring, M., and Smith, M. (2021). Please do not use !?_ or your license plate number: Analyzing password policies in german companies. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 17–36. USENIX Association.
- Giannakas, F., Kambourakis, G., Papasalouros, A., and Gritzalis, S. (2018). A critical review of 13 years of mobile game-based learning. *Educational Technology Research and Development*, 66:341–384.
- Girden, E. R. (1992). Anova: Repeated measures.
- Gjertsen, E. G. B., Gjære, E. A., Bartnes, M., and Flores, W. R. (2017). Gamification of information security awareness and training. In *ICISSP*, pages 59–70.
- Gong, J., Tarasewich, P., et al. (2004). Guidelines for handheld mobile device interface design.
- Google (2024). Advertising ID - Play Console Help — support.google.com. <https://support.google.com/googleplay/android-developer/answer/6048248?hl=en>. [Accessed 31-05-2024].
- Goulart, V. G., Liboni, L. B., and Cezarino, L. O. (2022). Balancing skills in the digital transformation era: The future of jobs and the role of higher education. *Industry and Higher Education*, 36(2):118–127.
- Graber, D. A. (1976). *Verbal behavior and politics*. University of Illinois Press.

REFERENCES

- Graneheim, U. and Lundman, B. (2004). Qualitative content analysis in nursing research: concepts, procedures and measures to achieve trustworthiness. *Nurse Education Today*, 24(2):105–112.
- Granić, A. and Marangunić, N. (2019). Technology acceptance model in educational context: A systematic literature review. *British Journal of Educational Technology*, 50(5):2572–2593.
- Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., and Toombs, A. L. (2018). The dark (patterns) side of ux design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, page 1–14, New York, NY, USA. Association for Computing Machinery.
- Greenberg, S., Boring, S., Vermeulen, J., and Dostal, J. (2014). Dark patterns in proxemic interactions: a critical perspective. In *Proceedings of the 2014 Conference on Designing Interactive Systems*, DIS '14, page 523–532, New York, NY, USA. Association for Computing Machinery.
- Greg, C. (2002). I have no words & i must design: Toward a critical vocabulary for games. In *Computer Games and Digital Cultures Conference Proceedings*. Tampere University Press.
- Griffith, C. (2017). *Mobile App Development with Ionic, Revised Edition: Cross-Platform Apps with Ionic, Angular, and Cordova.* ” O’Reilly Media, Inc.”, USA.
- Gros, B. (2007). Digital games in education. *Journal of Research on Technology in Education*, 40(1):23–38.
- Grudpan, S., Alexandrovky, D., Baalsrud Hauge, J., and Malaka, R. (2019). Exploring the effect of game premise in cooperative digital board games. In van der Spek, E., Göbel, S., Do, E. Y.-L., Clua, E., and Baalsrud Hauge, J., editors, *Entertainment Computing and Serious Games*, pages 214–227, Cham. Springer International Publishing.
- Grundy, Q., Chiu, K., Held, F., Continella, A., Bero, L., and Holz, R. (2019). Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. *BMJ*, 364.
- Guhr, N., Werth, O., Blacha, P. P. H., and Breitner, M. H. (2020). Privacy concerns in the smart home context. *SN Applied Sciences*, 2(2):247.
- Gunawan, J., Pradeep, A., Choffnes, D., Hartzog, W., and Wilson, C. (2021). A comparative study of dark patterns across web and mobile modalities. *Proc. ACM Hum.-Comput. Interact.*, 5(CSCW2).

REFERENCES

- Haan, Y. D., Kruikemeier, S., Lecheler, S., Smit, G., and van der Nat, R. (2018). When does an infographic say more than a thousand words? *Journalism Studies*, 19(9):1293–1312.
- Hahn, N., Chang, J. C., and Kittur, A. (2018). *Bento Browser: Complex Mobile Search Without Tabs*, page 1–12. Association for Computing Machinery, New York, NY, USA.
- Hamari, J., Koivisto, J., and Sarsa, H. (2014). Does gamification work? – a literature review of empirical studies on gamification. In *2014 47th Hawaii International Conference on System Sciences*, pages 3025–3034.
- Hamari, J., Shernoff, D. J., Rowe, E., Coller, B., Asbell-Clarke, J., and Edwards, T. (2016). Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning. *Computers in Human Behavior*, 54:170–179.
- Hammerschall, U. (2019). A gamification framework for long-term engagement in education based on self determination theory and the transtheoretical model of change. In *2019 IEEE Global Engineering Education Conference (EDUCON)*, pages 95–101.
- Hammi, B., Zeadally, S., Khatoun, R., and Nebhen, J. (2022). Survey on smart homes: Vulnerabilities, risks, and countermeasures. *Computers & Security*, 117:102677.
- Haney, J., Acar, Y., and Furman, S. (2021). "it's the company, the government, you and i": User perceptions of responsibility for smart home privacy and security. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 411–428, Berkeley, California, United States. USENIX Association.
- Haney, J. M., Furman, S. M., and Acar, Y. (2020). Smart home security and privacy mitigations: Consumer perceptions, practices, and challenges. In Moallem, A., editor, *HCI for Cybersecurity, Privacy and Trust*, pages 393–411, Cham. Springer International Publishing.
- Harbach, M., Hettig, M., Weber, S., and Smith, M. (2014). Using personal examples to improve risk communication for security & privacy decisions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, page 2647–2656, New York, NY, USA. Association for Computing Machinery.

REFERENCES

- Harkous, H., Fawaz, K., Lebret, R., Schaub, F., Shin, K. G., and Aberer, K. (2018). Polis: Automated analysis and presentation of privacy policies using deep learning. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 531–548, Baltimore, MD. USENIX Association.
- Harms, J., Kratky, M., Wimmer, C., Kappel, K., and Grechenig, T. (2015). Navigation in long forms on smartphones: Scrolling worse than tabs, menus, and collapsible fieldsets. In Abascal, J., Barbosa, S., Fetter, M., Gross, T., Palanque, P., and Winckler, M., editors, *Human-Computer Interaction – INTERACT 2015*, pages 333–340, Cham. Springer International Publishing.
- Hart, S. G. and Staveland, L. E. (1988). Development of nasa-tlx (task load index): Results of empirical and theoretical research. In Hancock, P. A. and Meshkati, N., editors, *Human Mental Workload*, volume 52 of *Advances in Psychology*, pages 139–183. North-Holland, Amsterdam.
- Hekler, E. B., Klasnja, P., Froehlich, J. E., and Buman, M. P. (2013). Mind the theoretical gap: Interpreting, using, and developing behavioral theory in hci research. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '13*, page 3307–3316, New York, NY, USA. Association for Computing Machinery.
- Hennessey, B., Moran, S., Altringer, B., and Amabile, T. M. (2015). Extrinsic and intrinsic motivation. *Wiley encyclopedia of management*, pages 1–4.
- Henze, M., Hermerschmidt, L., Kerpen, D., Häußling, R., Rumpe, B., and Wehrle, K. (2016). A comprehensive approach to privacy in the cloud-based internet of things. *Future Generation Computer Systems*, 56:701–718.
- Hewett, T. T., Baecker, R., Card, S., Carey, T., Gasen, J., Mantei, M., Perlman, G., Strong, G., and Verplank, W. (1992). *ACM SIGCHI curricula for human-computer interaction*. ACM.
- Hiebert, J. (2013). *Conceptual and procedural knowledge: The case of mathematics*. Routledge.
- Hinds, J., Williams, E. J., and Joinson, A. N. (2020). “it wouldn’t happen to me”: Privacy concerns and perspectives following the cambridge analytica scandal. *International Journal of Human-Computer Studies*, 143:102498.
- Hookham, G. and Meany, M. (2014). Perspective shifting: Humour and comedy in games. In *Proceedings of the 2014 Conference on Interactive Entertainment, IE2014*, pages 21:1–21:8, New York, NY, USA. ACM.

REFERENCES

- Hossain, M. M., Fotouhi, M., and Hasan, R. (2015). Towards an analysis of security issues, challenges, and open problems in the internet of things. In *2015 IEEE World Congress on Services*, pages 21–28.
- Hsieh, H.-F. and Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, 15(9):1277–1288. PMID: 16204405.
- Hsu, M.-H., Ju, T. L., Yen, C.-H., and Chang, C.-M. (2007). Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations. *International Journal of Human-Computer Studies*, 65(2):153–169.
- Huckvale, K., Torous, J., and Larsen, M. E. (2019). Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation. *JAMA network open*, 2(4):e192542–e192542.
- Hudders, L. and Lou, C. (2023). The rosy world of influencer marketing? its bright and dark sides, and future research recommendations. *International Journal of Advertising*, 42(1):151–161.
- Ijsselsteijn, W., Nap, H. H., de Kort, Y., and Poels, K. (2007). Digital game design for elderly users. In *Proceedings of the 2007 Conference on Future Play, Future Play '07*, page 17–22, New York, NY, USA. Association for Computing Machinery.
- Ineson, E. M., Jung, T., Hains, C., and Kim, M. (2013). The influence of prior subject knowledge, prior ability and work experience on self-efficacy. *Journal of Hospitality, Leisure, Sport & Tourism Education*, 12(1):59–69.
- ISO (2011). ISO/IEC 25010:2011: Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models. ISO Standard.
- ISO (2018). ISO 9241-11:2018: Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts. ISO Standard.
- ISO (2019). ISO 9241-210:2019: Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems. ISO Standard.
- Issa, T. and Isaias, P. (2022). *Usability and Human-Computer Interaction (HCI)*, pages 23–40. Springer London, London.
- IT Governance Privacy Team (2020). Eu general data protection regulation (gdpr) – an implementation and compliance guide, fourth edition.

REFERENCES

- Jensen, C. and Potts, C. (2004). Privacy policies as decision-making tools: An evaluation of online privacy notices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '04, page 471–478, New York, NY, USA. Association for Computing Machinery.
- Jiang, L., Jayatilaka, A., Nasim, M., Grobler, M., Zahedi, M., and Babar, M. A. (2022). Systematic literature review on cyber situational awareness visualizations. *IEEE Access*, 10:57525–57554.
- Jo, D. and Kim, G. J. (2019). Ar enabled iot for a smart and interactive environment: A survey and future directions. *Sensors*, 19(19).
- Joët, G., Usher, E. L., and Bressoux, P. (2011). Sources of self-efficacy: An investigation of elementary school students in france. *Journal of educational psychology*, 103(3):649–663.
- Johnson, C. I., Bailey, S. K. T., and Van Buskirk, W. L. (2017). *Designing Effective Feedback Messages in Serious Games and Simulations: A Research Review*, pages 119–140. Springer International Publishing, Cham.
- Juliussen, B. A., Kozyri, E., Johansen, D., and Rui, J. P. (2023). The third country problem under the GDPR: enhancing protection of data transfers with technology. *International Data Privacy Law*, 13(3):225–243.
- Juul, J. (2011). *Half-real: Video games between real rules and fictional worlds*. MIT press.
- Kaaz, K. J., Hoffer, A., Saeidi, M., Sarma, A., and Bobba, R. B. (2017). Understanding user perceptions of privacy, and configuration challenges in home automation. In *2017 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*, pages 297–301.
- Kacsmar, B., Tilbury, K., Mazmudar, M., and Kerschbaum, F. (2022). Caring about sharing: User perceptions of multiparty data sharing. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 899–916, Boston, MA. USENIX Association.
- Kaiser, J.-N., Marianski, T., Jung, F., Woźniak, M., and Boll, S. (2022). Informed shopper - visualizing privacy information in augmented reality. In *Proceedings of Mensch Und Computer 2022*, MuC '22, page 394–398, New York, NY, USA. Association for Computing Machinery.
- Kang, H. and 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.

REFERENCES

- Kang, R., Dabbish, L., Fruchter, N., and Kiesler, S. (2015). “My data just goes Everywhere:” user mental models of the internet and implications for privacy and security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 39–52, Ottawa. USENIX Association.
- Karagiannis, S., Papaioannou, T., Magkos, E., and Tsohou, A. (2020). Game-based information security/privacy education and awareness: Theory and practice. In Themistocleous, M., Papadaki, M., and Kamal, M. M., editors, *Information Systems*, pages 509–525, Cham. Springer International Publishing.
- Karagiorgas, D. N. and Niemann, S. (2017). Gamification and game-based learning. *Journal of Educational Technology Systems*, 45(4):499–519.
- Karoui, A., Marfisi-Schottman, I., and George, S. (2017). A nested design approach for mobile learning games. In *Proceedings of the 16th World Conference on Mobile and Contextual Learning*, mLearn 2017, New York, NY, USA. Association for Computing Machinery.
- Karthick, S. and Binu, S. (2017). Android security issues and solutions. In *2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, pages 686–689.
- Kay, M. and Terry, M. (2010). Textured agreements: Re-envisioning electronic consent. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS ’10, New York, NY, USA. Association for Computing Machinery.
- Kelley, P. G., Bresee, J., Cranor, L. F., and Reeder, R. W. (2009). A “nutrition label” for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, SOUPS ’09, New York, NY, USA. Association for Computing Machinery.
- Kelley, P. G., Cesca, L., Bresee, J., and Cranor, L. F. (2010). Standardizing privacy notices: An online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI ’10, page 1573–1582, New York, NY, USA. Association for Computing Machinery.
- Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N., and Wetherall, D. (2012). A conundrum of permissions: installing applications on an android smartphone. In *International conference on financial cryptography and data security*, pages 68–79. Springer.

REFERENCES

- Kelley, P. G., Cranor, L. F., and Sadeh, N. (2013). Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, pages 3393–3402, New York, NY, USA. ACM.
- Kerawalla, L., Luckin, R., Seljeflot, S., and Woolard, A. (2006). “making it real”: exploring the potential of augmented reality for teaching primary school science. *Virtual reality*, 10:163–174.
- Khodabandeh, F. and Mombini, A. (2024). Exploring the effect of augmented reality technology on high school students’ vocabulary learning, personality traits, and self-efficacy in flipped and blended classes. *Education and Information Technologies*.
- Kießling, S., Hanka, T., and Merli, D. (2021). Salt&pepper: Spice up security behavior with cognitive triggers. In *Proceedings of the 2021 European Interdisciplinary Cybersecurity Conference*, EICC '21, page 26–31, New York, NY, USA. Association for Computing Machinery.
- Kilsdonk, E., Peute, L., Riezebos, R., Kremer, L., and Jaspers, M. (2016). Uncovering healthcare practitioners’ information processing using the think-aloud method: From paper-based guideline to clinical decision support system. *International Journal of Medical Informatics*, 86:10–19.
- Kim, D. J., Ferrin, D. L., and Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, 44(2):544–564.
- Kitkowska, A., Shulman, Y., Martucci, L. A., and Wästlund, E. (2020a). Facilitating privacy attitudes and behaviors with affective visual design. In Hölbl, M., Rannenber, K., and Welzer, T., editors, *ICT Systems Security and Privacy Protection*, pages 109–123, Cham. Springer International Publishing.
- Kitkowska, A., Warner, M., Shulman, Y., Wästlund, E., and Martucci, L. A. (2020b). Enhancing privacy through the visual design of privacy notices: Exploring the interplay of curiosity, control and affect.
- Kizilcec, R. F. (2016). How much information? effects of transparency on trust in an algorithmic interface. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, page 2390–2395, New York, NY, USA. Association for Computing Machinery.

REFERENCES

- Klopfer, E. (2008). *Augmented learning: Research and design of mobile educational games*. MIT press.
- Knutzen, K., Weidner, F., and Broll, W. (2021). Exploring augmented reality privacy icons for smart home devices and their effect on users' privacy awareness. In *2021 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct)*, pages 409–414.
- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64:122–134.
- Kolb, D. A. (2014). *Experiential learning: Experience as the source of learning and development*. FT press.
- Kolter, J. and Pernul, G. (2009). Generating user-understandable privacy preferences.
- Komninos, N., Philippou, E., and Pitsillides, A. (2014). Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys & Tutorials*, 16(4):1933–1954.
- Korkiakoski, M., Antila, A., Annamaa, J., Sheikhi, S., Alavesa, P., and Kostakos, P. (2023). Hack the room: Exploring the potential of an augmented reality game for teaching cyber security. In *Proceedings of the Augmented Humans International Conference 2023, AHs '23*, page 349–353, New York, NY, USA. Association for Computing Machinery.
- Kortum, P. and Peres, S. C. (2014). The relationship between system effectiveness and subjective usability scores using the system usability scale. *International Journal of Human-Computer Interaction*, 30(7):575–584.
- Krath, J., Schürmann, L., and von Korfflesch, H. F. (2021). Revealing the theoretical basis of gamification: A systematic review and analysis of theory in research on gamification, serious games and game-based learning. *Computers in Human Behavior*, 125:106963.
- Krum, R. (2013). *Cool infographics: Effective communication with data visualization and design*. John Wiley & Sons.
- Krutz, D. E., Munaiah, N., Meneely, A., and Malachowsky, S. A. (2016). Examining the relationship between security metrics and user ratings of mobile apps: A case study. In *Proceedings of the International Workshop*

REFERENCES

- on App Market Analytics*, WAMA 2016, pages 8–14, New York, NY, USA. ACM.
- Kulkarni, P. and Khanai, R. (2015). Addressing mobile cloud computing security issues: A survey. In *2015 International Conference on Communications and Signal Processing (ICCSP)*, pages 1463–1467.
- Kushlev, K., Dwyer, R., and Dunn, E. W. (2019). The social price of constant connectivity: Smartphones impose subtle costs on well-being. *Current Directions in Psychological Science*, 28(4):347–352.
- Lallé, S. and Conati, C. (2019). The role of user differences in customization: a case study in personalization for infovis-based content. In *Proceedings of the 24th International Conference on Intelligent User Interfaces, IUI '19*, page 329–339, New York, NY, USA. Association for Computing Machinery.
- Lamb, R. L., Annetta, L., Firestone, J., and Etopio, E. (2018). A meta-analysis with examination of moderators of student cognition, affect, and learning outcomes while using serious educational games, serious games, and simulations. *Computers in Human Behavior*, 80:158–167.
- LaMonica, H. M., Roberts, A. E., Lee, G. Y., Davenport, T. A., and Hickie, I. B. (2021). Privacy practices of health information technologies: Privacy policy risk assessment study and proposed guidelines. *J Med Internet Res*, 23(9):e26317.
- Lampropoulos, G., Keramopoulos, E., Diamantaras, K., and Evangelidis, G. (2023). Integrating augmented reality, gamification, and serious games in computer science education. *Education Sciences*, 13(6).
- Langheinrich, M. (2018). Privacy in ubiquitous computing. In *Ubiquitous computing fundamentals*, pages 109–174. Chapman and Hall/CRC.
- Lankow, J., Ritchie, J., and Crooks, R. (2012). *Infographics: The power of visual storytelling*. John Wiley & Sons.
- Lau, J., Zimmerman, B., and Schaub, F. (2018). Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW).
- Laugwitz, B., Held, T., and Schrepp, M. (2008). Construction and evaluation of a user experience questionnaire. In Holzinger, A., editor, *HCI and Usability for Education and Work*, pages 63–76, Berlin, Heidelberg. Springer Berlin Heidelberg.

REFERENCES

- Lavie, T. and Meyer, J. (2010). Benefits and costs of adaptive user interfaces. *International Journal of Human-Computer Studies*, 68(8):508–524. Measuring the Impact of Personalization and Recommendation on User Behaviour.
- Lazarus, R. S. and Folkman, S. (1984). *Stress, appraisal, and coping*. Springer publishing company.
- Le Compte, A., Elizondo, D., and Watson, T. (2015). A renewed approach to serious games for cyber security. In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, pages 203–216.
- Leah Zhang-Kennedy, S. C. and Biddle, R. (2016). The role of instructional design in persuasion: A comics approach for improving cybersecurity. *International Journal of Human-Computer Interaction*, 32(3):215–257.
- Lederer, S., Mankoff, J., and Dey, A. K. (2003). Who wants to know what when? privacy preference determinants in ubiquitous computing. In *CHI '03 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '03, page 724–725, New York, NY, USA. Association for Computing Machinery.
- Lee, H. and Kobsa, A. (2019). Confident privacy decision-making in iot environments. *ACM Trans. Comput.-Hum. Interact.*, 27(1).
- Li, K., Cheng, L., and Teng, C.-I. (2020). Voluntary sharing and mandatory provision: Private information disclosure on social networking sites. *Information Processing & Management*, 57(1):102128.
- Liang, H. and Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 33(1):71–90. <http://www.jstor.org/stable/20650279>.
- Liao, Y., Vitak, J., Kumar, P., Zimmer, M., and Kritikos, K. (2019). Understanding the role of privacy and trust in intelligent personal assistant adoption. In Taylor, N. G., Christian-Lamb, C., Martin, M. H., and Nardi, B., editors, *Information in Contemporary Society*, pages 102–113, Cham. Springer International Publishing.
- Liccardi, I., Pato, J., Weitzner, D. J., Abelson, H., and De Roure, D. (2014). No technical understanding required: helping users make informed choices about access to their personal data. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking*

REFERENCES

- and Services*, MOBIQUITOUS '14, page 140–150, Brussels, BEL. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
- Lim, S. and Reeves, B. (2010). Computer agents versus avatars: Responses to interactive game characters controlled by a computer or other player. *International Journal of Human-Computer Studies*, 68(1):57–68.
- Lin, H. and Bergmann, N. W. (2016). Iot privacy and security challenges for smart home environments. *Information*, 7(3).
- Lin, J., Liu, B., Sadeh, N., and Hong, J. I. (2014). Modeling Users' mobile app privacy preferences: Restoring usability in a sea of permission settings. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 199–212, Menlo Park, CA. USENIX Association.
- Linden, T., Khandelwal, R., Harkous, H., and Fawaz, K. (2018). The privacy policy landscape after the gdpr.
- Lindorfer, M., Neugschwandtner, M., and Platzner, C. (2015). Marvin: Efficient and comprehensive mobile app classification through static and dynamic analysis. In *2015 IEEE 39th Annual Computer Software and Applications Conference*, volume 2, pages 422–433.
- Linehan, C., Kirman, B., Lawson, S., and Chan, G. (2011). Practical, appropriate, empirically-validated guidelines for designing educational games. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, page 1979–1988, New York, NY, USA. Association for Computing Machinery.
- Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K., and Fu, X. (2017). Security vulnerabilities of internet of things: A case study of the smart plug system. *IEEE Internet of Things Journal*, 4(6):1899–1909.
- Lipford, H. R., Watson, J., Whitney, M., Froiland, K., and Reeder, R. W. (2010). Visual vs. compact: A comparison of privacy policy interfaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, page 1111–1114, New York, NY, USA. Association for Computing Machinery.
- Liu, B., Andersen, M. S., Schaub, F., Almuhammedi, H., Zhang, S. A., Sadeh, N., Agarwal, Y., and Acquisti, A. (2016). Follow my recommendations: A personalized privacy assistant for mobile app permissions. In *Twelfth*

REFERENCES

- Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 27–41, Denver, CO. USENIX Association.
- Lombardi, I. (2012). Not-so-serious games for language learning. now with 99,9% more humour on top. *Procedia Computer Science*, 15:148 – 158. 4th International Conference on Games and Virtual Worlds for Serious Applications(VS-GAMES'12).
- Lope, R. P. D. and Medina, N. M. (2017). A comprehensive taxonomy for serious games. *Journal of Educational Computing Research*, 55(5):629–672.
- Luger, E., Moran, S., and Rodden, T. (2013). Consent for all: Revealing the hidden complexity of terms and conditions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '13*, page 2687–2696, New York, NY, USA. Association for Computing Machinery.
- Luguri, J. and Strahilevitz, L. J. (2021). Shining a Light on Dark Patterns. *Journal of Legal Analysis*, 13(1):43–109.
- Lunenburg, F. C. (2011). Self-efficacy in the workplace: Implications for motivation and performance. *International journal of management, business, and administration*, 14:1–6.
- Lupton, D. (2017). Feeling your data: Touch and making sense of personal digital data. *New Media & Society*, 19(10):1599–1614.
- Lupton, D. (2018). How do data come to matter? living and becoming with personal data. *Big Data & Society*, 5(2):1–11.
- Lyons, J. B. and Havig, P. R. (2014). Transparency in a human-machine context: Approaches for fostering shared awareness/intent. In Shumaker, R. and Lackey, S., editors, *Virtual, Augmented and Mixed Reality. Designing and Developing Virtual and Augmented Environments*, pages 181–190, Cham. Springer International Publishing.
- Lyra, K. T., Isotani, S., Reis, R. C. D., Marques, L. B., Pedro, L. Z., Jaques, P. A., and Bitencourt, I. I. (2016). Infographics or graphics+text: Which material is best for robust learning? *2016 IEEE 16th International Conference on Advanced Learning Technologies (ICALT)*.
- Malgieri, G. and Custers, B. (2018). Pricing privacy – the right to know the value of your personal data. *Computer Law & Security Review*, 34(2):289–303.

REFERENCES

- Malhotra, N. K., Kim, S. S., and Agarwal, J. (2004). Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information Systems Research*, 15(4):336–355.
- Marky, K., Prange, S., Mühlhäuser, M., and Alt, F. (2022). Roles matter! understanding differences in the privacy mental models of smart home visitors and residents. In *Proceedings of the 20th International Conference on Mobile and Ubiquitous Multimedia*, MUM '21, page 108–122, New York, NY, USA. Association for Computing Machinery.
- Mathur, A., Kshirsagar, M., and Mayer, J. (2021). 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*, CHI '21, New York, NY, USA. Association for Computing Machinery.
- Mayring, P. et al. (2004). Qualitative content analysis. *A companion to qualitative research*, 1(2):159–176.
- McCormick, R. (1997). Conceptual and procedural knowledge. *International journal of technology and design education*, 7:141–159.
- Meijer, A. (2009). Understanding modern transparency. *International Review of Administrative Sciences*, 75(2):255–269.
- Mekler, E. D., Bopp, J. A., Tuch, A. N., and Opwis, K. (2014). A systematic review of quantitative studies on the enjoyment of digital entertainment games. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, page 927–936, New York, NY, USA. Association for Computing Machinery.
- Merrill Warkentin, A. C. J. and Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, 20(3):267–284.
- Michel, M. C. K. and King, M. C. (2019). Cyber influence of human behavior: Personal and national security, privacy, and fraud awareness to prevent harm. In *2019 IEEE International Symposium on Technology and Society (ISTAS)*, pages 1–7.
- Milne, G. R. and Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of interactive marketing*, 18(3):15–29.

REFERENCES

- Milne, G. R., Labrecque, L. I., and Cromer, C. (2009). Toward an understanding of the online consumer’s risky behavior and protection practices. *Journal of Consumer Affairs*, 43(3):449–473.
- Minssen, T., Rajam, N., and Bogers, M. (2020). Clinical trial data transparency and gdpr compliance: Implications for data sharing and open innovation. *Science and Public Policy*, 47(5):616–626.
- Miraz, M. H., Ali, M., and Excell, P. S. (2021). Adaptive user interfaces and universal usability through plasticity of user interface design. *Computer Science Review*, 40:100363.
- Mishra, A., Shukla, A., Rana, N. P., and Dwivedi, Y. K. (2021). From “touch” to a “multisensory” experience: The impact of technology interface and product type on consumer responses. *Psychology & Marketing*, 38(3):385–396.
- Mocrii, D., Chen, Y., and Musilek, P. (2018). Iot-based smart homes: A review of system architecture, software, communications, privacy and security. *Internet of Things*, 1-2:81–98.
- Molina, M. D., Gambino, A., and Sundar, S. S. (2019). Online privacy in public places: How do location, terms and conditions and vpn influence disclosure? In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI EA ’19, New York, NY, USA. Association for Computing Machinery.
- Mollah, M. B., Azad, M. A. K., and Vasilakos, A. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. *Journal of Network and Computer Applications*, 84:38–54.
- Monterrat, B., Lavoué, É., and George, S. (2015). Toward an adaptive gamification system for learning environments. In Zvacek, S., Restivo, M. T., Uhomobhi, J., and Helfert, M., editors, *Computer Supported Education*, pages 115–129, Cham. Springer International Publishing.
- Moonsamy, V., Rong, J., and Liu, S. (2014). Mining permission patterns for contrasting clean and malicious android applications. *Future Generation Computer Systems*, 36:122–132.
- Morgner, P., Mattejat, S., and Benenson, Z. (2016). All your bulbs are belong to us: Investigating the current state of security in connected lighting systems. *ArXiv*, abs/1608.03732.

REFERENCES

- Morris, J. D. (1995). Observations: Sam: the self-assessment manikin; an efficient cross-cultural measurement of emotional response. *Journal of advertising research*, 35(6):63–68.
- Mourey, J. A. and Waldman, A. E. (2020). Past the privacy paradox: The importance of privacy changes as a function of control and complexity. *Journal of the Association for Consumer Research*, 5(2):162–180.
- Muchagata, J. and Ferreira, A. (2018). How can visualization affect security? In *ICEIS (2)*, pages 503–510.
- Mujeje, S. and Levy, Y. (2013). Complex passwords: How far is too far? the role of cognitive load on employee productivity. *Online Journal of Applied Knowledge Management (OJAKM)*, 1(1):122–132.
- Muro, M. and Jeffrey, P. (2008). A critical review of the theory and application of social learning in participatory natural resource management processes. *Journal of Environmental Planning and Management*, 51(3):325–344.
- Murphy, C. A., Coover, D., and Owen, S. V. (1989). Development and validation of the computer self-efficacy scale. *Educational and Psychological Measurement*, 49(4):893–899.
- Nabavi, R. T. (2012). Bandura’s social learning theory & social cognitive learning theory. *Theory of Developmental Psychology*, 1(1):1–24.
- Naeini, P. E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L. F., and Sadeh, N. (2017). Privacy expectations and preferences in an IoT world. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 399–412, Santa Clara, CA. USENIX Association.
- Nagarajan, A., Allbeck, J. M., Sood, A., and Janssen, T. L. (2012). Exploring game design for cybersecurity training. In *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, pages 256–262.
- Naqvi, B. and Seffah, A. (2019). Interdependencies, conflicts and trade-offs between security and usability: Why and how should we engineer them? In Moallem, A., editor, *HCI for Cybersecurity, Privacy and Trust*, pages 314–324, Cham. Springer International Publishing.
- Nauman, M., Khan, S., and Zhang, X. (2010). Apex: Extending android permission model and enforcement with user-defined runtime constraints. In *Proceedings of the 5th ACM Symposium on Information, Computer and*

REFERENCES

- Communications Security*, ASIACCS '10, pages 328–332, New York, NY, USA. ACM.
- Needham, C. (2011). *Personalising public services: Understanding the personalisation narrative*. Policy Press, Bristol, United Kingdom.
- Nguyen, D. C., Wermke, D., Acar, Y., Backes, M., Weir, C., and Fahl, S. (2017). A stitch in time: Supporting android developers in writing secure code. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, page 1065–1077, New York, NY, USA. Association for Computing Machinery.
- Nielsen, J. (1994). Enhancing the explanatory power of usability heuristics. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '94, page 152–158, New York, NY, USA. Association for Computing Machinery.
- Nielsen, J., Clemmensen, T., and Yssing, C. (2002). Getting access to what goes on in people's heads? reflections on the think-aloud technique. In *Proceedings of the Second Nordic Conference on Human-Computer Interaction*, NordiCHI '02, page 101–110, New York, NY, USA. Association for Computing Machinery.
- Nikhashemi, S., Knight, H. H., Nusair, K., and Liat, C. B. (2021). Augmented reality in smart retailing: A (n) (a) symmetric approach to continuous intention to use retail brands' mobile ar apps. *Journal of Retailing and Consumer Services*, 60:102464.
- Nikou, S. (2019). Factors driving the adoption of smart home technology: An empirical assessment. *Telematics and Informatics*, 45:101283.
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, 79:119.
- Obar, J. A. and 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.
- O'Connor, Y. and Mahony, C. (2023). Exploring the impact of augmented reality on student academic self-efficacy in higher education. *Computers in Human Behavior*, 149:107963.
- Oh, S., Woo, W., et al. (2009). Camar: Context-aware mobile augmented reality in smart space. *Proc. of IWUVR*, 9:48–51.

REFERENCES

- Oliveira, W., Hamari, J., Shi, L., Toda, A. M., Rodrigues, L., Palomino, P. T., and Isotani, S. (2023). Tailored gamification in education: A literature review and future agenda. *Education and Information Technologies*, 28(1):373–406.
- Oliver, M. B., Bowman, N. D., Woolley, J. K., Rogers, R., Sherrick, B. I., and Chung, M.-Y. (2016). Video games as meaningful entertainment experiences. *Psychology of popular media culture*, 5(4):390–405.
- Olsen, D. and Mateas, M. (2009). Beep! beep! boom!: Towards a planning model of coyote and road runner cartoons. In *Proceedings of the 4th International Conference on Foundations of Digital Games*, FDG '09, pages 145–152, New York, NY, USA. ACM.
- Orji, R., Nacke, L. E., and Di Marco, C. (2017). Towards personality-driven persuasive health games and gamified systems. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, page 1015–1027, New York, NY, USA. Association for Computing Machinery.
- Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security*, 31(5):673–680.
- Pan, Y., Ge, X., Fang, C., and Fan, Y. (2020). A systematic literature review of android malware detection using static analysis. *IEEE Access*, 8:116363–116379.
- Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., and Patsakis, C. (2018). Security and privacy analysis of mobile health applications: The alarming state of practice. *IEEE Access*, 6:9390–9403.
- Peruma, A., Palmerino, J., and Krutz, D. E. (2018). Investigating user perception and comprehension of android permission models. In *Proceedings of the 5th International Conference on Mobile Software Engineering and Systems*, MOBILESoft '18, page 56–66, New York, NY, USA. Association for Computing Machinery.
- Plass, J. L. (2020). *Handbook of Game-Based Learning*. Mit Press.
- Polimeni, J. and Reiss, J. P. (2006). The first joke: Exploring the evolutionary origins of humor. *Evolutionary Psychology*, 4(1).
- Politou, E., Alepis, E., Virvou, M., and Patsakis, C. (2022). *Privacy in Ubiquitous Mobile Computing*, pages 93–131. Springer International Publishing, Cham.

REFERENCES

- Poneres, K., Hamidi, F., Massey, A., and Hurst, A. (2018). Using icons to communicate privacy characteristics of adaptive assistive technologies. In *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility*, ASSETS '18, page 388–390, New York, NY, USA. Association for Computing Machinery.
- Poslad, S. (2011). *Ubiquitous computing: smart devices, environments and interactions*. John Wiley & Sons.
- Prange, S., Shams, A., Piening, R., Abdelrahman, Y., and Alt, F. (2021). Priview– exploring visualisations to support users’ privacy awareness. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA. Association for Computing Machinery.
- Prange, S., Thiem, N., Fröhlich, M., and Alt, F. (2022). “secure settings are quick and easy!” – motivating end-users to choose secure smart home configurations. In *Proceedings of the 2022 International Conference on Advanced Visual Interfaces*, AVI '22, New York, NY, USA. Association for Computing Machinery.
- Prensky, M. (2003). Digital game-based learning. *Comput. Entertain.*, 1(1):21.
- Prior, D. D., Mazanov, J., Meacheam, D., Heaslip, G., and Hanson, J. (2016). Attitude, digital literacy and self efficacy: Flow-on effects for online learning behavior. *The Internet and Higher Education*, 29:91–97.
- Prochaska, J. O. and Velicer, W. F. (1997). The transtheoretical model of health behavior change. *American Journal of Health Promotion*, 12(1):38–48. PMID: 10170434.
- Punchoojit, L. and Hongwarittorn, N. (2017). Usability Studies on Mobile User Interface Design Patterns: A Systematic Literature Review. *Advances in Human-Computer Interaction*, 2017:6787504. Publisher: Hindawi.
- Pyae, A. and Joelsson, T. N. (2018). Investigating the usability and user experiences of voice user interface: a case of google home smart speaker. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct*, MobileHCI '18, page 127–131, New York, NY, USA. Association for Computing Machinery.
- Qi, H. and Gani, A. (2012). Research on mobile cloud computing: Review, trend and perspectives. In *2012 Second International Conference on*

REFERENCES

- Digital Information and Communication Technology and it's Applications (DICTAP)*, pages 195–202.
- Ramachandran, S., Dimitri, A., Galinium, M., Tahir, M., Ananth, I. V., Schunck, C. H., and Talamo, M. (2017). Understanding and granting android permissions: A user survey. In *2017 International Carnahan Conference on Security Technology (ICCST)*, pages 1–6.
- Raneburger, D., Alonso-Ríos, D., Popp, R., Kaindl, H., and Falb, J. (2013). A user study with guis tailored for smartphones. In Kotzé, P., Marsden, G., Lindgaard, G., Wesson, J., and Winckler, M., editors, *Human-Computer Interaction – INTERACT 2013*, pages 505–512, Berlin, Heidelberg. Springer Berlin Heidelberg.
- Raptis, D., Tselios, N., Kjeldskov, J., and Skov, M. B. (2013). Does size matter? investigating the impact of mobile phone screen size on users' perceived usability, effectiveness and efficiency. In *Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services, MobileHCI '13*, page 127–136, New York, NY, USA. Association for Computing Machinery.
- Redmiles, E. M., Liu, E., and Mazurek, M. L. (2017). You want me to do what? a design study of two-factor authentication messages. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, Santa Clara, CA. USENIX Association.
- Reeder, R. W., Kelley, P. G., McDonald, A. M., and Cranor, L. F. (2008). A user study of the expandable grid applied to p3p privacy policy visualization. In *Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society, WPES '08*, page 45–54, New York, NY, USA. Association for Computing Machinery.
- Rehman, S. and Gruhn, V. (2018). An approach to secure smart homes in cyber-physical systems/internet-of-things. In *2018 Fifth International Conference on Software Defined Systems (SDS)*, pages 126–129.
- Reinhardt, D., Borchard, J., and Hurtienne, J. (2021). Visual interactive privacy policy: The better choice? In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, CHI '21*, New York, NY, USA. Association for Computing Machinery.
- Renaud, K. and Shepherd, L. A. (2018). How to make privacy policies both gdpr-compliant and usable. In *2018 International Conference On Cyber*

REFERENCES

- Situational Awareness, Data Analytics And Assessment (Cyber SA)*, pages 1–8, USA. IEEE.
- Rhee, H.-S., Kim, C., and Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28(8):816–826.
- Richards, N. (2022). What Privacy Is. In *Why Privacy Matters*. Oxford University Press.
- Richter, G., Raban, D. R., and Rafaeli, S. (2015). *Studying Gamification: The Effect of Rewards and Incentives on Motivation*, pages 21–46. Springer International Publishing, Cham.
- Rittle-Johnson, B., Siegler, R. S., and Alibali, M. W. (2001). Developing conceptual understanding and procedural skill in mathematics: An iterative process. *Journal of educational psychology*, 93(2):346–362.
- Rodriguez-Hevía, L. F., Navío-Marco, J., and Ruiz-Gómez, L. M. (2020). Citizens' involvement in e-government in the european union: The rising importance of the digital skills. *Sustainability*, 12(17).
- Rogers, R. (2017). The motivational pull of video game feedback, rules, and social interaction: Another self-determination theory approach. *Computers in Human Behavior*, 73:446–450.
- Rogers, Y. (2022). *HCI theory: classical, modern, and contemporary*. Springer Nature.
- Rosenbaum, E., Klopfer, E., and Perry, J. (2007). On location learning: Authentic applied science with networked augmented realities. *Journal of Science Education and Technology*, 16:31–45.
- Rossi, A. and Palmirani, M. (2019). Dapis: A data protection icon set to improve information transparency under the gdpr. *Knowledge of the Law in the Big Data Age*, 252(181-195):5–5.
- Rudolph, M., Feth, D., and Polst, S. (2018). Why users ignore privacy policies – a survey and intention model for explaining user privacy behavior. In Kurosu, M., editor, *Human-Computer Interaction. Theories, Methods, and Human Issues*, pages 587–598, Cham. Springer International Publishing.
- Ryan, R. M. (1982). Control and information in the intrapersonal sphere: An extension of cognitive evaluation theory. *Journal of personality and social psychology*, 43(3):450–461.

REFERENCES

- Ryan, R. M. and Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American psychologist*, 55(1):68–78.
- Sailer, M., Hense, J., Mandl, H., and Klevers, M. (2013). Psychological perspectives on motivation through gamification. *Ixd&a*, 19(1):28–37.
- Samonas, S. and Coss, D. (2014). The cia strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, 10(3).
- Satyanarayanan, M. (2011). Mobile computing: the next decade. *SIGMOBILE Mob. Comput. Commun. Rev.*, 15(2):2–10.
- Sauro, J. and Lewis, J. R. (2016). *Quantifying the user experience: Practical statistics for user research*. Morgan Kaufmann.
- Schaub, F., Balebako, R., Durity, A. L., and Cranor, L. F. (2015). A design space for effective privacy notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 1–17, Ottawa. USENIX Association.
- Schiefer, M. (2015). Smart home definition and security threats. In *2015 Ninth International Conference on IT Security Incident Management IT Forensics*, pages 114–118.
- Schmidt, J. T. and Tang, M. (2020). *Digitalization in Education: Challenges, Trends and Transformative Potential*, pages 287–312. Springer Fachmedien Wiesbaden, Wiesbaden.
- Scholefield, S. and Shepherd, L. A. (2019). Gamification techniques for raising cyber security awareness. In Moallem, A., editor, *HCI for Cybersecurity, Privacy and Trust*, pages 191–203, Cham. Springer International Publishing.
- Schrepp, M., Hinderks, A., and Thomaschewski, J. (2014). Applying the user experience questionnaire (ueq) in different evaluation scenarios. In Marcus, A., editor, *Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience*, pages 383–392, Cham. Springer International Publishing.
- Schroeder, T., Haug, M., and Gewalt, H. (2022). Data privacy concerns using mhealth apps and smart speakers: Comparative interview study among mature adults. *JMIR Form Res*, 6(6):e28025.

REFERENCES

- Schwarzer, R. and Jerusalem, M. (1995). Generalized self-efficacy scale. *J. Weinman, S. Wright, & M. Johnston, Measures in health psychology: A user's portfolio. Causal and control beliefs*, 35(37):82–003.
- Scoccia, G. L., Malavolta, I., Autili, M., Di Salle, A., and Inverardi, P. (2021). Enhancing trustability of android applications via user-centric flexible permissions. *IEEE Transactions on Software Engineering*, 47(10):2032–2051.
- Senanayake, J., Kalutarage, H., Al-Kadri, M. O., Petrovski, A., and Piras, L. (2023). Android source code vulnerability detection: A systematic literature review. *ACM Comput. Surv.*, 55(9).
- Seo, D. W., Kim, H., Kim, J. S., and Lee, J. Y. (2016). Hybrid reality-based user experience and evaluation of a context-aware smart home. *Computers in Industry*, 76:11–23.
- Sheng, H., Nah, F. F.-H., and Siau, K. (2008). An experimental study on ubiquitous commerce adoption: Impact of personalization and privacy concerns. *Journal of the Association for Information Systems*, 9(6):1.
- Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., and Nunge, E. (2007). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, SOUPS '07, page 88–99, New York, NY, USA. Association for Computing Machinery.
- Shin, J., Park, Y., and Lee, D. (2018). Who will be smart home users? an analysis of adoption and diffusion of smart homes. *Technological Forecasting and Social Change*, 134:246–253.
- Shuhaiber, A. and Mashal, I. (2019). Understanding users' acceptance of smart homes. *Technology in Society*, 58:101110.
- Shute, V. (2008). Focus on formative feedback. *Review of Educational Research*, 78:153–189.
- Sivaraman, V., Chan, D., Earl, D., and Boreli, R. (2016). Smart-phones attacking smart-homes. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, WiSec '16, page 195–200, New York, NY, USA. Association for Computing Machinery.
- Skinner, B. F. (1953). *Science and human behavior*. New York: Free Press.

REFERENCES

- Smiciklas, M. (2012). *The power of infographics: Using pictures to communicate and connect with your audiences*. Que publishing.
- Smith, H. J., Dinev, T., and Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4):989–1015.
- Smith, S. P., Blackmore, K., and Nesbitt, K. (2015). *A Meta-Analysis of Data Collection in Serious Games Research*, pages 31–55. Springer International Publishing, Cham.
- Solove, D. J. (2002). Conceptualizing privacy. *Calif. L. Rev.*, 90:1087.
- Sotiriou, S. and Bogner, F. X. (2008). Visualizing the invisible: augmented reality as an innovative science education scheme. *Advanced Science Letters*, 1(1):114–122.
- Sotoudeh, S., Hashemi, S., and Garakani, H. G. (2020). Security framework of iot-based smart home. In *2020 10th International Symposium on Telecommunications (IST)*, pages 251–256.
- Squire, K. and Klopfer, E. (2007). Augmented reality simulations on handheld computers. *Journal of the Learning Sciences*, 16(3):371–413.
- Squire, K. D. and Jan, M. (2007). Mad city mystery: Developing scientific argumentation skills with a place-based augmented reality game on handheld computers. *Journal of science education and technology*, 16:5–29.
- Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, 24(2):124–133.
- Student (1908). The probable error of a mean. *Biometrika*, pages 1–25.
- Sweet, S. N., Fortier, M. S., Strachan, S. M., and Blanchard, C. M. (2012). Testing and integrating self-determination theory and self-efficacy theory in a physical activity context. *Canadian Psychology/Psychologie Canadienne*, 53(4):319–327.
- Sweetser, P. and Wyeth, P. (2005). Gameflow: a model for evaluating player enjoyment in games. *Comput. Entertain.*, 3(3):3.
- Sweller, J. (1988). Cognitive load during problem solving: Effects on learning. *Cognitive science*, 12(2):257–285.
- Tabassum, M., Alqhatani, A., Aldossari, M., and Richter Lipford, H. (2018). Increasing user attention with a comic-based policy. In *Proceedings of the*

REFERENCES

- 2018 CHI Conference on Human Factors in Computing Systems, CHI '18, New York, NY, USA. Association for Computing Machinery.
- Tabassum, M., Kosinski, T., and Lipford, H. R. (2019). "i don't own the data": End user perceptions of smart home device data practices and risks. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 435–450, Santa Clara, CA. USENIX Association.
- Taha, N. and Dahabiyeh, L. (2021). College students information security awareness: A comparison between smartphones and computers. *Education and Information Technologies*, 26(2):1721–1736.
- Tam, K., Feizollah, A., Anuar, N. B., Salleh, R., and Cavallaro, L. (2017). The evolution of android malware and android analysis techniques. *ACM Comput. Surv.*, 49(4).
- Tavakol, M. and Dennick, R. (2011). Making sense of cronbach's alpha. *Int J Med Educ*, 2:53–55.
- Tavinor, G. (2009). *The art of videogames*. John Wiley & Sons.
- Tekinbas, K. S. and Zimmerman, E. (2005). *The Game Design Reader: A Rules of Play Anthology*. MIT press.
- Thompson, N., McGill, T. J., and Wang, X. (2017). "security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, 70:376–391.
- Tikkinen-Piri, C., Rohunen, A., and Markkula, J. (2018). Eu general data protection regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1):134–153.
- Torkzadeh, G. and van Dyke, T. P. (2001). Development and validation of an internet self-efficacy scale. *Behaviour & Information Technology*, 20(4):275–280.
- Torre, I., Sanchez, O. R., Koceva, F., and Adorni, G. (2018). Supporting users to take informed decisions on privacy settings of personal devices. *Personal and Ubiquitous Computing*, 22(2):345–364.
- Torrente, J., Borro-Escribano, B., Freire, M., del Blanco, Á., J. Marchiori, E., Martínez-Ortiz, I., Moreno-Ger, P., and Fernández-Manjón, B. (2014). Development of game-like simulations for procedural knowledge in healthcare education. *IEEE Transactions on Learning Technologies*, 7(1):69–82.

REFERENCES

- Tsai, H.-T. and Bagozzi, R. P. (2014). Contribution behavior in virtual communities: Cognitive, emotional, and social influences. *MIS Quarterly*, 38(1):143–164.
- Turland, J., Coventry, L., Jeske, D., Briggs, P., and van Moorsel, A. (2015). Nudging towards security: developing an application for wireless network selection for android phones. In *Proceedings of the 2015 British HCI Conference*, British HCI '15, page 193–201, New York, NY, USA. Association for Computing Machinery.
- Tyack, A. and Mekler, E. D. (2020). Self-determination theory in hci games research: Current uses and open questions. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–22, New York, NY, USA. Association for Computing Machinery.
- Ullah, A. M., Islam, M. R., Aktar, S. F., and Hossain, S. K. A. (2012). Remote-touch: Augmented reality based marker tracking for smart home control. In *2012 15th International Conference on Computer and Information Technology (ICCIT)*, pages 473–477.
- Usher, E. L. and Pajares, F. (2008). Sources of self-efficacy in school: Critical review of the literature and future directions. *Review of Educational Research*, 78(4):751–796.
- Van Dijk, J. A. (2017). Digital divide: Impact of access. *The international encyclopedia of media effects*, pages 1–11.
- Van Dinther, M., Dochy, F., and Segers, M. (2011). Factors affecting students' self-efficacy in higher education. *Educational Research Review*, 6(2):95–108.
- Van Kleek, M., Liccardi, I., Binns, R., Zhao, J., Weitzner, D. J., and Shadbolt, N. (2017). Better the devil you know: Exposing the data sharing practices of smartphone apps. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, page 5208–5220, New York, NY, USA. Association for Computing Machinery.
- Vargas-Murillo, A. R., Pari-Bedoya, I. N. M. d. l. A., and Guevara-Soto, F. d. J. (2023). Virtual gamification strategies and their impact on legal education experiences: a systematic review. In *Proceedings of the 2023 8th International Conference on Distance Education and Learning*, ICDEL '23, page 85–90, New York, NY, USA. Association for Computing Machinery.

REFERENCES

- Vermeulen, H., Gain, J., Marais, P., and ODonovan, S. (2016). Reimagining gamification through the lens of activity theory. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pages 1328–1337.
- Vlachogianni, P. and Tselios, N. (2022). Perceived usability evaluation of educational technology using the system usability scale (sus): A systematic review. *Journal of Research on Technology in Education*, 54(3):392–409.
- Vlachopoulos, D. and Makri, A. (2017). The effect of games and simulations on higher education: a systematic literature review. *International Journal of Educational Technology in Higher Education*, 14(1):1–33.
- Voigt, P. and Von dem Bussche, A. (2017). The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 10.
- Von Ahn, L. and Dabbish, L. (2008). Designing games with a purpose. *Communications of the ACM*, 51(8):58–67.
- Vygotsky, L. S. and Cole, M. (1978). *Mind in society: Development of higher psychological processes*. Harvard university press.
- Wagner, J. (2018). The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection? *International Data Privacy Law*, 8(4):318–337.
- Wang, D., Xiang, Z., and Fesenmaier, D. R. (2016). Smartphone use in everyday life and travel. *Journal of Travel Research*, 55(1):52–63.
- Warren, S. and Brandeis, L. (1989). The right to privacy. In Goldstein, T., editor, *Killing the Messenger: 100 Years of Media Criticism*, pages 1–21. Columbia University Press, New York Chichester, West Sussex.
- Weiser, M. (1991). The computer for the 21st century. *Scientific American*, pages 94–104.
- West, D. M. (2015). Digital divide: Improving internet access in the developing world through affordable services and diverse content. *Center for Technology Innovation at Brookings*, pages 1–30.
- Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, 25(1):166.
- Wigand, C. and Soumilion, S. (2019). Data protection regulation one year on: 73% of europeans have heard of at least one of their rights. <https://>

REFERENCES

- ec.europa.eu/commission/presscorner/detail/en/IP_19_2956. European Commission - Press release, Accessed: 2024.05.12.
- Wijesekera, P., Baokar, A., Hosseini, A., Egelman, S., Wagner, D., and Beznosov, K. (2015). Android permissions remystified: A field study on contextual integrity. In *Proceedings of the 24th USENIX Conference on Security Symposium, SEC'15*, pages 499–514, Berkeley, CA, USA. USENIX Association.
- Willingham, D. B., Nissen, M. J., and Bullemer, P. (1989). On the development of procedural knowledge. *Journal of experimental psychology: learning, memory, and cognition*, 15(6):1047–1060.
- Wong, E. (2023). Shneiderman’s eight golden rules will help you design better interfaces. last retrieved 15-06-2024.
- Wong, R. Y. and Mulligan, D. K. (2019). Bringing design to the privacy table: Broadening “design” in “privacy by design” through the lens of hci. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, CHI '19*, page 1–17, New York, NY, USA. Association for Computing Machinery.
- Wottrich, V. M., van Reijmersdal, E. A., and Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, 106:44–52.
- Wu, T., Tien, K.-Y., Hsu, W.-C., and Wen, F.-H. (2021). Assessing the effects of gamification on enhancing information security awareness knowledge. *Applied Sciences*, 11(19).
- Wykes, T. and Schueller, S. (2019). Why reviewing apps is not enough: Transparency for trust (t4t) principles of responsible health app marketplaces. *J Med Internet Res*, 21(5):e12390.
- Yao, Y., Basdeo, J. R., Kaushik, S., and Wang, Y. (2019). Defending my castle: A co-design study of privacy mechanisms for smart homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, CHI '19*, page 1–12, New York, NY, USA. Association for Computing Machinery.
- Zaeem, R. N. and Barber, K. S. (2020). The effect of the gdpr on privacy policies: Recent progress and future promise. *ACM Trans. Manage. Inf. Syst.*, 12(1).

REFERENCES

- Zaeem, R. N., German, R. L., and Barber, K. S. (2018). Privacycheck: Automatic summarization of privacy policies using data mining. *ACM Trans. Internet Technol.*, 18(4).
- Zeng, E., Mare, S., and Roesner, F. (2017). End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 65–80, Santa Clara, CA. USENIX Association.
- Zhang, D. and Adipat, B. (2005). Challenges, methodologies, and issues in the usability testing of mobile applications. *International Journal of Human-Computer Interaction*, 18(3):293–308.
- Zhou, Y., Wang, Z., Zhou, W., and Jiang, X. (2012). Hey, you, get off of my market: Detecting malicious apps in official and alternative android markets. In *19th Annual Network and Distributed System Security Symposium, NDSS 2012, San Diego, California, USA, February 5-8, 2012*.
- Zhou, Y., Zhang, X., Jiang, X., and Freeh, V. W. (2011). Taming information-stealing smartphone applications (on android). In *Proceedings of the 4th International Conference on Trust and Trustworthy Computing, TRUST’11*, pages 93–107, Berlin, Heidelberg. Springer-Verlag.
- Zimmeck, S. and Bellovin, S. M. (2014). Privee: An architecture for automatically analyzing web privacy policies. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 1–16, San Diego, CA. USENIX Association.
- Zimmeck, S., Story, P., Smullen, D., Ravichander, A., Wang, Z., Reidenberg, J., Russell, N. C., and Sadeh, N. (2019). Maps: Scaling privacy compliance analysis to a million apps. *Proceedings on Privacy Enhancing Technologies*, pages 66–86.
- Zimmermann, V., Gerber, P., Marky, K., Böck, L., and Kirchbuchner, F. (2019). Assessing users’ privacy and security concerns of smart home technologies. *i-com*, 18(3):197–216.
- Zimmermann, V. and Renaud, K. (2021). The nudge puzzle: Matching nudge interventions to cybersecurity decisions. *ACM Trans. Comput.-Hum. Interact.*, 28(1).
- Zwilling, M., Klien, G., Lesjak, D., Łukasz Wiechetek, Cetin, F., and Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1):82–97.