Privacy-aware Smart Home Interface Framework

Thesis

School of Computing and Communications
Faculty of Science, Technology, Engineering and Mathematics
The Open University, UK

Privacy-aware Smart Home Interface Framework

R. A. A. V. A. Wijesundara

A thesis submitted in fulfilment of the requirements for the degree of
Doctor of Philosophy

Abstract

Smart home user interfaces are pervasive and shared by multiple users who occupy the space. Therefore, they pose a risk to interpersonal privacy of occupants because an individual's sensitive information can be leaked to other co-occupants (information privacy), or they can be disturbed by intrusions into their personal space (physical privacy) when the co-occupant interacts with the smart home user interfaces. This thesis hypothesises that interpersonal privacy violations can be mitigated by adapting the user interface layer and presents insights into how to achieve usable user interface adaptation to mitigate or minimise interpersonal privacy violations in smart homes.

The thesis reports two case studies and two user studies. The first case study identifies the key **characteristics** needed to model the rich context of interpersonal privacy violations scenarios. Then it presents **knowledge representation models** that are required to represent the identified characteristics and evaluates them for adequacy in modelling the context information of interpersonal privacy violation scenarios. The second case study presents a **software architecture and a set of algorithms** that can detect interpersonal privacy violations and generate usable user interface adaptations. Then it evaluates the architecture and the algorithms for adequacy in generating usable privacy-aware user interface adaptations. The first user study (N=15) evaluates the **usability** of the adaptive user interfaces generated from the framework where storyboards were used as the stimulant. Extending the findings from the usability study and expanding the coverage of example scenarios, the second user study (N=23) evaluates the overall **user experience** of the adaptive user interfaces, using video prototypes as the stimulant.

The research demonstrates that the characteristics identified, and the respective knowledge representation models adequately captured the context of interpersonal privacy violation scenarios. Furthermore, the software architecture and the algorithms could detect possible interpersonal privacy violations and generate usable user interface adaptations to mitigate them. The two user studies demonstrate that the adaptive user interfaces, when used in appropriate situations, were a suitable solution for addressing interpersonal privacy violations while providing high usability and a positive user experience. The thesis concludes by providing recommendations for developing privacy-aware user interface adaptations and suggesting future work that can extend this research.

This thesis is dedicated to my family,

My mother ***Chrishanthi*** *and father* ***Rohitha****,*

My brothers ***Desira*** *and* ***Danuka****.*

Acknowledgements

I am extremely grateful to my supervisors Professor Arosha Bandara, Professor Blaine Price, and Professor Bashar Nuseibeh for having faith in me, guiding me, and challenging my thinking with utmost care and patience throughout my PhD journey. I am truly honoured and privileged to have them as my supervisors. Alongside my supervisors, Professor Marian Petre was instrumental in the completion of my PhD, and I am deeply indebted to her kindness, guidance, and critical feedback. I would also like to thank Dr. Amel Bennaceur and Professor Andrea Zisman for their invaluable advice during my doctoral studies.

Next, I would like to thank the Open University's Computing Research PG-Forum community for teaching me the fundamentals of research and for making my PhD a memorable one. The SEAD research group for providing me with the chance to engage and network with a number of scholars and the chance to present my work and receive valuable feedback. From these communities, I would particularly like to thank Daniel, Dmitri, Ciaran, Tamara, Stewart, David, Matthew and Vikram, for supporting me at different stages of my PhD. I also appreciate the efficient Open University administration for swiftly handling all my requests and making my PhD journey a comfortable one.

Doing a PhD during a global pandemic was not easy, but my friends made the difference. The *Easy Peasy Lemon Squeezy* group, *Avenismo* football team, friends at *No: 23*, the *#100Daysofwriting* group, friends at the *University of Cambridge*, and the *Sustainable Education Foundation* were some of the communities that supported me during my PhD. In particular, I would like to highlight some friends: Sumudu, Minuri, Danny, Vinuri, Senuri, Kasun, Yasiru, Perla, Agnese, Matteo, Matthew, Anna, Vibha, and Margaret. Thank you for being there for me during the toughest times of my PhD. Next, I would like to extend my gratitude to my family for their inspiration, courage, and support. My parents for instilling the importance of education and hard work through their exemplary lives and parenting; and my brothers for their love and encouragement.

Finally, I would like to extend my gratitude to the Open University for funding my PhD and travels; and everyone who participated in my studies.

Authors Declaration

This thesis is an original contribution of the author. The following has been published and made publicly available.

Doctoral Consortium

Wijesundara, A. (2020) 'Engineering privacy-aware smart home environments', in *Companion Proceedings of the 12th ACM SIGCHI Symposium on Engineering Interactive Computing Systems*, pp. 1–3. doi: 10.1145/3393672.3398643. **(Chapter 5)**

Public Datasets and Resources

Wijesundara, A. (2021b) 'PASHI-framework Usability Evaluation Study Storyboards'. The Open University. doi: 10.21954/ou.rd.14812578.v1. **(Chapter 5)**

Wijesundara, A. (2021a) 'PASHI-framework Usability Evaluation Study Interview Transcripts'. The Open University. doi: 10.21954/ou.rd.14812575.v1. **(Chapter 5)**

Wijesundara, A. (2021d) 'PASHI-framework User Experience Evaluation Study Video Prototypes'. The Open University. doi: 10.21954/ou.rd.14812584.v1. **(Chapter 6)**

Wijesundara, A. (2021c) 'PASHI-framework User Experience Evaluation Study Interview Transcripts'. The Open University. doi: 10.21954/ou.rd.14812587.v1. **(Chapter 6)**

Table of Contents

List of Figures

List of Code Listings

List of Tables

List of Abbreviations

IoT = Internet of Things

UI(s) = User Interface(s)

AUI(s) = Adaptive User Interface(s)

CAUI = Choice-based Adaptive User Interface

AAUI = Automatic Adaptive User Interface

NAUI = Non-Adaptive User Interface

1. Introduction

1.1 Problem and Motivation

Advances in embedded systems, network connectivity and data analysis technologies based on artificial intelligence have enabled Weiser's vision of ubiquitous computing (Weiser, Gold and Brown, 1999). Increasingly, our homes are evolving into smart spaces, where sensors detect occupants' activities, and where AI-based analysis techniques process this sensor data and trigger adaptations in the environment to help occupants in different ways (Youngblood *et al.*, 2005). Smart homes provide numerous benefits to their users, including security, assisted living, health, entertainment, communication, convenience and comfort, and energy efficiency (Balta-Ozkan *et al.*, 2013). At the same time, there are various challenges associated with smart homes, such as the difficulty of integrating new devices into the existing system, difficulty adjusting the user interface layer according to the existing and ever-changing needs of the users, management of smart home services, reliability, security and privacy (Balta-Ozkan *et al.*, 2013).

Of these challenges, privacy has become a major concern for smart home devices that continuously sense the smart home and its users (Dasgupta, Gill and Hussain, 2019). Current adoption trends suggest that smart home users are generally unaware of, or undeterred by, the privacy concerns of these technologies. Leading technology companies promote and sell their smart home devices such as the Amazon Echo product suite (Amazon Press Room, 2020), Google Home product suite (https://store.google.com/category/connected_home), Facebook Portal (https://portal.facebook.com/), Apple Home pod (https://www.apple.com/homepod/), and Apple Home Kit (https://www.apple.com/shop/accessories/all/homekit). The speed of adoption of smart home devices suggests that convenience outweighs privacy concerns (Zheng *et al.*, 2018). Therefore, the benefits of addressing smart home privacy concerns are two-fold: smart home users could protect their privacy while experiencing the benefits of smart home technology; and smart home vendors could provide privacy-protected smart home devices and services, consequently increasing smart home technology adoption and their profits.

Although extensive research has been conducted to explore the privacy implications of smart home devices, the majority of this work has focused on the privacy violations that happen between the smart home user and the service provider. Some examples include privacy implications of smart speakers and their usage of user data (Jackson and Orebaugh, 2018), privacy violations at the smart grid (Cárdenas and Safavi-Naini, 2012), privacy violations due to smart home surveillance (Alharbi

and Aspinall, 2018), and data aggregation which happens outside the smart home (Zheng, Cai and Li, 2018). In addition, Abdi et al. (2020) explored the privacy norms of using smart home personal assistants (mostly commonly integrated into smart speakers). The authors reported how user's privacy concerns were associated with the recipient of the data and the type of data. Sharing information with trusted stakeholders tend to improve the acceptability of the information flows where sharing information for non-relevant purposes was unacceptable. Another aspect of smart home privacy, which is less explored, is the privacy violation that happens between smart home users due to the shared nature of smart home devices, i.e., interpersonal privacy. Studies have shown that smart home users are concerned that their personal information can be leaked to other users of shared smart home user interfaces, i.e., violation of interpersonal *information* privacy (Kray, Kortuem and Wasinger, 2004), and (Kraemer, 2018). Apart from privacy violations caused by information leakages, the notion of the "right to be let alone" (Warren and Brandeis, 1890) can also be violated due to the pervasive nature of user interfaces within the smart home. This has been discussed with the concept of *territorial* privacy (Konings and Schaub, 2011) where users can be disturbed by the broadcast functions of public user interfaces such as smart speakers and smart displays, i.e., violating interpersonal *physical* privacy.

Interpersonal privacy violations happen at the intersection of the smart home user interface layer and the smart home users as a result of multiple users sharing the user interfaces. Therefore, adapting the user interface layer appropriately may minimise possible interpersonal privacy violations. However, the smart home user interface layer is multimodal, distributed and shared among multiple smart home users (Blumendorf, 2009). In addition, smart users may have different privacy preferences (Karami *et al.*, 2016), user interface preferences (Casas *et al.*, 2008) and capabilities (Smirek, Zimmermann and Ziegler, 2014). Due to these challenges, implementing, deploying, and maintaining a user interface layer that can detect interpersonal privacy violations and generate usable user interface adaptations becomes a complex task. The research presented in this thesis aims to address some of these complexities by developing an engineering framework for a robust and adaptive smart home user interface layer.

Existing smart home user interface frameworks covered different aspects required for smart home user interface generation, but none of them fully supported privacy-aware user interface generation. For example, MASP (Blumendorf, 2009), GPII (Loitsch *et al.*, 2017), MIODMIT (Cronel *et al.*, 2019), and AM4I (Almeida *et al.*, 2019) provided support for generating multimodal and adaptive user interfaces where all of them (except GPII) provided an engineering framework. On the other hand, GPII provided sufficient user modelling capabilities to cover different user preferences and user capabilities, where MASP, MIODMIT, and AM4I only provided limited user modelling capabilities. However, none of the user models covered users' privacy preferences. Furthermore, none of the frameworks included:

- the ability to understand the rich context of interpersonal privacy-violating scenarios,

- representation of the user's interpersonal privacy preferences,
- the ability to detect interpersonal privacy violations, and
- the ability to generate usable user interface adaptations minimising or mitigating possible interpersonal privacy violations.

This motivated development of a smart home user interface framework that can address these research gaps. The proposed framework is called the Privacy-Aware Smart Home Interface Framework (PASHI Framework). The next section provides two motivating examples to illustrate interpersonal privacy violations and consider how adaptive user interfaces could mitigate such violations.

1.2 Motivating Examples

This section provides two hypothetical scenarios depicting interpersonal privacy violations (information privacy and physical privacy). First, the context for both the scenarios is provided, followed by two example scenarios. Under each example, a version of the scenario with the standard smart home user interface is provided; this is followed by a version with adaptive user interfaces.

Context

Sally is an older woman who lives alone in her own smart home. She has a circle of support which is comprised of her adult son Zack and a caregiver Yasmin. Sally also has a set of privacy preferences: Sally's health data will only be shared with her caregiver, and she does not want to be disturbed while she is meditating. Caregiver Yasmin has a set of user interface preferences that she would like to use when doing her tasks, her preferred interface being a smart speaker, and her second choice a smartwatch. Zack has a set of user preferences when listening to music; he likes to use a Bluetooth headset when the smart speaker is unavailable.

1.2.1 Information Privacy Scenario

With standard user interfaces

One day, while Yasmin (caregiver) is taking vitals of Sally (care receiver) over the smart speaker in the living room, her son Zack enters the room. Sally's blood glucose levels have increased. There is no detection of Zack entering, and the broadcast of Sally's blood glucose over the smart speaker continues. Zack hears Sally's sensitive information.

With adaptive user interfaces

When the smart home senses Zack's presence, it could pause the broadcast of Sally's health data. The broadcast can be switched automatically to a graphical display on Yasmin's smartwatch, protecting Sally's while maintaining the usability of the smart home system for Yasmin.

1.2.2 Physical Privacy Scenario

With standard user interfaces

One day, while Sally (care receiver) is meditating in her room, her son Zack plays music loudly on his smart speaker. The smart home is not aware of Sally's privacy preferences and lets Zack play his music loudly. Sally is disturbed while meditating and becomes upset with her son.

With adaptive user interfaces

When Zack tries to play music, the smart home realises the privacy violation that is about to happen and either restricts the volume or switches the music automatically to the Bluetooth headset after making a quiet announcement regarding the change on the speaker. Therefore, Zack listening to music won't disturb Sally.

The two scenarios highlight how adaptive user interfaces can help protect interpersonal privacy while maintaining usability. This motivates further examination of different types of interpersonal privacy violating scenarios to develop a mechanism (in this case the PASHI framework) that can generate usable privacy-aware user interface adaptations. The following section articulates the research questions that frame the research.

1.3 Research Questions

The aim of this research is to understand how to engineer adaptive smart home user interfaces to address interpersonal privacy. This is captured in **RQ0**: *How can smart home user interfaces be engineered to adapt their configuration and behaviour to preserve privacy between users in multi occupancy contexts?*

To address **RQ0,** three key sub-questions were identified, as follows. The first two questions address the technical challenges; the third evaluates whether the AUI worked, from the users' perspective.

- **RQ1(model evaluation):** *How can we characterise the smart home environment adequately to drive privacy-aware user interface adaptations?*
  As with all adaptive systems, the PASHI framework must understand the context to generate effective and usable privacy-aware user interface adaptations. Therefore, the first research objective was to identify the characteristics that defined the rich context in which interpersonal privacy must operate, to identify scenarios of representative privacy violations and their mitigation, and to develop models that can represent these knowledge requirements.

- **RQ2 (architecture and algorithm testing):** *What is an appropriate software architecture for a privacy-aware adaptive smart home interface framework?*
  As the second step, the PASHI framework needed a software architecture and a set of algorithms that enabled the generation of privacy-aware user interface adaptations.

- **RQ3 (user experience evaluation):** *What is the user experience of privacy-aware adaptive user interfaces?*
  The final step was to evaluate the PASHI framework from the users' perspective and to understand the user experience of the adaptive user interfaces that were generated by the PASHI framework.

These questions framed the research, as reflected in the thesis structure that follows.

1.4 Thesis Structure

This thesis is organised into 8 chapters that describe research, including the relevant literature, methods used to investigate the research questions and the studies conducted. An overview of the chapters is presented below.

Chapter 2 - Literature Review: This chapter critically evaluates the state of the art of smart home privacy and of the smart home user interface frameworks. In doing so, the chapter highlights a gap in the literature regarding interpersonal privacy protection, where existing smart home user interface frameworks fail to address this aspect. Further, this chapter critically reviews the literature to identify suitable knowledge representation models (i.e., user interface preference models and privacy preference models) that are required for capturing the rich context of interpersonal privacy violation scenarios.

Chapter 3 - Research Design: This chapter outlines the research methodologies used to answer the research questions while grounding them in core software engineering and HCI research methods. In addition, this chapter discusses possible threats to validity and reliability for each research method chosen and presents the steps that were taken to mitigate those limitations.

Chapter 4 - Modelling Privacy-aware Smart Home User Interfaces: This chapter focuses on two tasks that were achieved via a case study. First was identifying the key characteristics required for representing the context of interpersonal privacy-violating scenarios (i.e., user interface preferences, interpersonal privacy preferences, and the user interface layer). The second task was presenting and evaluating the adequacy of knowledge representation models to represent the identified key characteristics in a way that can be used by the PASHI framework.

Chapter 5 - Privacy-aware Smart Home Interface Framework: This chapter presents the PASHI framework's software architecture and the underlying algorithms. Then it evaluates (a) the adequacy of the software architecture and the algorithms to generate usable privacy-aware smart home user interface adaptations, and (b) the efficiency of the core algorithms that detect interpersonal privacy violations and generate usable user interface adaptations to mitigate those identified violations. This was done via a case study and then re-evaluated using a storyboard-based usability study.

Chapter 6 - User Experience Evaluation: This chapter presents a video-prototype based user experience study that increases the range of scenarios covered and improves the realism of the scenarios in comparison to the usability study presented in the previous chapter.

Chapter 7 - Discussion of Usability and User Experience Evidence: This chapter combines the key findings across the two studies, discussing them in relation to the literature to understand the holistic experience of the AUIs generated by the PASHI framework.

Chapter 8 - Conclusion and Future work: The final chapter wraps up the thesis, providing a summary of the key findings for the key research questions. The chapter also provides recommendations for developing privacy-aware AUIs and describes future work that can extend and build on this research.

2. Literature Review

The previous chapter introduced the research gap being addressed by this thesis, regarding smart home privacy and smart home user interface frameworks, together with the research questions that were formulated to address those research gaps. This chapter presents an in-depth literature review that formally identifies the research gaps. First, it will explore smart home privacy (§2.1) to better understand the concept of privacy and how it manifests within the domain of smart homes. This step explains in detail the research gap and motivates the need to adapt the user interface layer to protect privacy violations that happen within the smart home. Next, it will review the literature regarding smart home user interfaces (§2.2) to identify the appropriate tools to develop privacy-aware adaptive user interfaces and to identify outstanding research needs regarding smart home user interface frameworks. Finally, the chapter will provide a summary of the review (§2.3).

2.1 Smart Home Privacy

This section explores the literature regarding smart home privacy. First, it will provide a brief introduction to smart homes (§2.1.1) highlighting that privacy is a key challenge of this domain. After that, it will investigate the evolution of privacy (§2.1.2) and the types of smart home privacy. Under types of smart home privacy, it will discuss information privacy (§2.1.3.1) and physical privacy (§2.1.3.2). Then it will discuss the privacy violations that happen outside the smart home (§2.1.3.3) and privacy violations that happen within the smart home (§2.1.3.4).

2.1.1 Smart Homes

Weiser (1993), one of the first to discuss the subject, defined ubiquitous computing as "*the nonintrusive availability of computers throughout the physical environment, virtually, if not effectively, invisible to the user*". He highlighted how in ubiquitous computing inter-connected computing devices are seamlessly integrated into the environment enhancing the occupants' daily activities. He depicted a future in which ubiquitous computing environments do work on behalf of the occupants in the background while making the occupants feel like they have done the work themselves. He also highlighted three problems regarding ubiquitous computing: 1) inadequacy of communication networks' bandwidth capacity, 2) inadequacy of network protocols to handle mobile devices, and 3) the lack of support provided by operating systems. More than a decade later, Rogers (2006) argued that Weiser's vision of ubiquitous computing was not fulfilled due to the slow growth of artificial intelligence and claimed its direction needed a re-evaluation. Rogers also highlighted the ethical and privacy implications of Weiser's vision due to the continuous tracking and monitoring of individuals. Rogers proposed that ubiquitous computing should shift from being

proactive computing to supporting proactive individuals. According to Rogers, the environments should enable people and keep them aware of the contextual changes rather than controlling the environment on behalf of the user. However, even though Weiser's original vision is far from achieved, it inspired multiple domains of research with one prominent area being smart homes.

From a technical standpoint, smart homes have most of the characteristics of other ubiquitous computing environments but differ mainly due to their socio-cultural characteristics. Davidoff et al. (2006) discussed how smart homes were shared by family members, where tasks within a smart home can be shared activities rather than procedures. Furthermore, they reported that tasks within a smart home can be device and location independent, wherein ownership of the task can also be ambiguous. They highlighted how rules don't always work within a smart home setting and described how the smart home impacts the definition of a family and the individual. Therefore, developing usable and effective smart homes is a challenging task that needs a methodical approach that will consider the different technical, socio-cultural aspects of a smart home.

The technical challenges associated with Smart Homes are discussed extensively in the literature where Samuel (2016) highlighted some of the most common issues identified by researchers:

- *Interoperability*: Smart home devices are developed by multiple vendors which consist of different hardware components and software systems. Therefore, getting smart home devices seamlessly to work together in real time is a challenging task.
- *Self-management*: Smart home context constantly changes and after the initial setup smart home devices should have the ability to self-manage themselves to carry on their operations as normal.
- *Maintainability*: For the smart home to be reliable and durable, the smart home devices should be easily maintainable (i.e.: failing batteries, failing network connectivity, and context changes should be easily addressed).
- *Signalling*: Reliable two-way communication is a must for most smart home devices and supporting this in a distributed multi-device environment is a challenge.
- *Power consumption*: Most of the smart home devices are battery-powered and those devices need to have efficient power consumption and minimal battery drain.

These challenges are a focus of ongoing research and are expected to be addressed with time. For example, meSchup (Kubitza and Schmidt, 2017) is a programmable platform that developed for smart environments abstracting some of the underlying complexities. However, even when these challenges are addressed, there will still be important socio-cultural challenges to be addressed in smart homes. Of these socio-cultural dimensions, privacy is an important factor due to the increased sensing capabilities of smart devices (Rogers, 2006) and the value of privacy within the bounds of a home. Therefore, this research focuses on the privacy aspect within the smart home. The remainder of this section will investigate the literature regarding smart home privacy, starting with an exploration of the concept of privacy and its evolution.

2.1.2 The Evolution of Privacy

Researchers use the terms territory (Konings and Schaub, 2011), boundary (Altman, 1976), space (Edward, 1966) and sphere (DeCew, 2002) when describing privacy. These terms could have different individual meanings, but they are generally used within the privacy literature to represent an area to which access should be controlled. Therefore, these terms are used interchangeably to convey the same idea in this thesis. According to the Oxford English dictionary, a **territory** is *"an area that one person, group, animal, etc. considers as their own and defends against others who try to enter it"* and a **boundary** is *"a real or imagined line that marks the limits or edges of something and separates it from other things or places; a dividing line"*, (*Oxford Online Dictionary*, 2020). Trespassing a boundary creates tension between the trespasser and the owner of the territory. This act of trespassing is known as a violation of privacy (Marx, 2001). Privacy was a unidimensional concept at the beginning of humankind (Marx, 2001). According to the earlier definitions, privacy referred to the protection of physical territory from intruders. As humans evolved the meaning of the term privacy also evolved. With time, different types of boundaries emerged. These boundary types ranged from being wholly tangible to wholly intangible with some boundaries having both tangible and intangible features. This section explores how the definition of privacy evolved from a territorial standpoint. This progression spans from the dawn of humankind to the present-day ubiquitous computing environments.

2.1.2.1 Classical Theories of Privacy

The analogy of spheres was used in the past to explain the term privacy. Although privacy research has significant prominence in the computing field relatively recently, it has existed as a concept more than a couple of millennia ago. An early historical recording of privacy was put forward by the philosopher Aristotle when he argued that an individual has two distinct spheres in his life. First is the public sphere (*polis*) which referred to the political activities of the individual. The second sphere is the private sphere (*oikos*) which referred to the family activities of the individual (DeCew, 2002). Even though Aristotle did not coin the term *privacy*, he introduced the idea of a person having a private sphere that consists of information that the person does not want to share with the public. Aristotle's idea of private and public spheres did not cover the aspects related to physical disturbances that could happen to an individual, but it highlighted the important distinction between personal information and public information. In the present day, Aristotle's notion of private and public spheres can be observed to a certain extent, but his idea fails to fully define these private spheres within complex digital systems. For example, an individual's privacy can be violated when participating in online social networks due to the difficulty in managing the audience of the shared information (Calikli *et al.*, 2016). Similarly, smart homes have also disrupted personal boundaries due to the pervasive and intrusive nature of smart devices.

Therefore, it is important to re-visit the definition of private and public spheres in the age of smart homes and thus to find ways to protect the smart home users' private sphere.

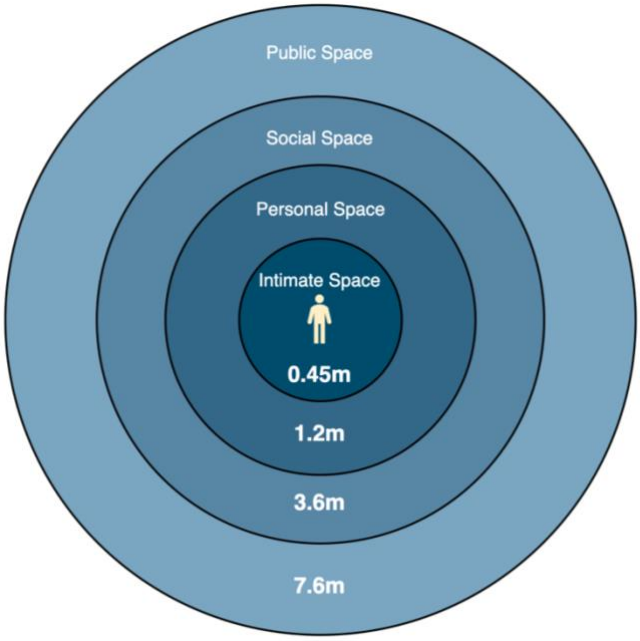

Figure 2.1: E.T Hall's Distance-based Space Representation (Hall, 1973)

Another aspect of privacy is the protection of physical space in which humans use the space around them to mark their boundaries. These hypothetical boundaries also act as an elaboration of the socio-cultural practices of the individual. Anthropologist E.T. Hall (1973) explored this phenomenon in his book, coining the term *proxemics* as the study of humans or animals use of space around them as a representation of the culture that they live in. Hall argued that individuals perceive space via their basic senses such as visual, auditory, tactile, and olfactory. As a result of his study, Hall identified four types of physical boundaries based on the distance from a person (Figure 2.1).

The immediate is the intimate boundary which has a range of 0.45 meters where an individual would have intimacy. This could be intimacy with their partners or even a contact sport like wrestling. The second space identified was personal space (range is 1.2m) which humans considered as an extension of their selves. In this space, an individual would not have skin to skin contact but would have a very close interaction with other people. These interactions could be with a trusted partner or with a person where you must discuss something discreetly. The third space identified is social space (range is 3.6m). In this space, individuals would have social interactions such as communication that happens between work colleagues. The fourth space identified was public space (range is 7.6m) in which an individual would have an interaction with a stranger. Hall discovered that if there is an intrusion to one of these spaces, it creates tension. Therefore, these boundary crossings are considered privacy violations. A stranger could intrude the intimate-space and the personal-space when using public transportation due to the constraints of the environment. This intrusion causes stress, and it is considered a privacy violation.

Hall's representation of distance-based spaces helped to understand the physical privacy (§2.1.3.2) aspect within the smart home but it does not explain privacy related to intangible boundaries such as information privacy (§2.1.3.1). His representation can be extended to understand disturbances experienced by smart home users via visual, auditory, olfactory, or tactile senses from the smart devices in the environment. Therefore, defining distance-based spaces based on sensory perception and how they will be impacted by different smart devices will support the protection of physical privacy within the smart home.

Privacy can also be explained as a hypothetical boundary control act done to attain the ideal level of solitude. Altman's privacy regulation theory (1976) described how individuals or groups control privacy. The theory defined privacy as a dialectic boundary controlling mechanism where individuals were motivated towards achieving the optimal level of privacy by controlling access to themselves or their group. The dialectic nature of privacy was defined as the openness or the closeness of the boundary between a person (or a group) with the external parties where an individual would seek or avoid social interaction depending on the desired level of privacy. It also discussed the non-monotonic nature of privacy where individuals try to optimise the level of privacy, which they achieve using different mechanisms such as verbal cues, non-verbal cues and controlling the physical environment. When the desired privacy is less than the achieved privacy it will lead to *crowding*. When the desired privacy is more than the achieved privacy it will lead to *isolation*. Therefore, privacy is non-monotonic in nature. Smart home devices invade the personal space of smart home users due to their pervasive and intrusive nature disrupting Altman's definition of boundary control and crowding. Altman's theory of controlling access to one's self provided a good foundation for understanding physical privacy regulation within the smart home, but it was not sufficient to fully explain the physical privacy aspect within the smart home as at the time, the author didn't envision the privacy violations that happen due to the shared nature of smart devices Apart from that, it also lacked the information privacy regulation aspect —This is discussed further in §2.1.3. Therefore, it motivates a re-evaluation of privacy regulation theory situated within the space of smart homes while utilising some of the valuable concepts such as boundary control to protect privacy.

2.1.2.2 Privacy in the Digital Age

The introduction of novel technologies disrupted the traditional definition of privacy. During the 19th century, the development of portable cameras allowed journalists to take photographs of individuals without their consent. This novel phenomenon was not directly addressed by the laws at that time. In response, Warren and Brandeis (1890) wrote the seminal *right to privacy* paper in the Harvard Law Review. They argued that the *right to privacy* can be based on the common law, which is used to protect individuals and their property. Furthermore, they explained how the concept of property has progressed from tangible assets to intangible assets due to the political,

societal, and economical changes of the day. Therefore, the authors iterated the need for revisions of these laws protecting the individuals and their property (both tangible and intangible). They highlighted the need for the *right to privacy* as a legal construct and emphasised the need to re-evaluate the definition of privacy as time evolves.

With the development of digital technologies, personal information sharing practices have evolved from Aristotle's definition of private and public spheres (DeCew, 2002) to a more complex problem. To explore this progression and address the shortcomings in the existing theories, Petronio (1991) defined the communication boundary management theory which was later named communication privacy management (CPM) theory (2002). The CPM theory explained how individuals share their personal information with others in the digital age. The theory described how individuals maintain a hypothetical boundary when sharing their personal information with other individuals (Petronio, 2015). It presented two types of boundaries: the *private-boundary*, which holds personal information, and *public-boundary* which holds public information. The decision to share personal information is decided by the individual using a rule-based system that assesses the benefits and costs of sharing. As the person evolves with time, their rules also tend to change depending on their experiences. When personal information is shared, individuals create a boundary linkage with the other parties making them co-owners of the boundary. They also agree on privacy rules when sharing personal information. The higher the number of people that a person shares personal information with, the thinner the personal boundary becomes. This may lead to *boundary turbulence* which refers to the intentional or unintentional disclosure of personal information to parties outside the boundary.

The CPM theory explained information sharing practices in domains such as social media, health care, relationship, family communication and, to a certain extent, the work environment. One of the limitations of the CPM theory is that it assumes the individual is aware of all their personal information that is available. But scenarios like surveillance (intentional capture), capturing bystanders when vlogging (unintentional capture), data mining and linkage attacks (novel discovery) leads to capturing and synthesizing personal data of which the individual is unaware. These aspects were not covered by the CPM theory. When applied in the smart home context, the CPM theory struggles to explain some aspects of information sharing practices. For example, smart home users share devices with each other, and these devices could unintentionally disclose the personal information of a specific user with others leading to *boundary turbulence*. But these situations cannot be addressed with the CPM theory as it assumes the individual can control the information flow. The CPM theory needs to be improved to fully explain information sharing practices in a smart home setting, but it inspires the use of a rule-based mechanism to control information flows and to consider boundary turbulence conditions within the smart home space, consequently, controlling privacy.

Improvement of technology impacted the traditional boundaries that were used to explain privacy regulation which motivated a re-evaluation of privacy regulation boundaries. Palen and Dourish (2003) explored the technology disruption on Altman's privacy regulation theory (1976). They explored three boundaries that were affected by technology and the tensions that arose among each of those boundaries.

The first boundary was the *disclosure boundary*. This explained how a person would disclose some of their personal information to function in present-day society. For example, during online shopping, the shopper must provide their payment details to the consumer website that they use. They also argued that individuals might not always be motivated to safeguard their information as mentioned in Altman's theory wherein they would deliberately make information public. This argument is described by using an example of a researcher who demonstrates their work publicly on their website, arguing that this type of disclosure controls unwanted access to the researcher by providing necessary information online. Palen and Dourish discussed the dimension of unintentional disclosure of information which was missing from Altman's privacy regulation theory. They brought forward the example of Google's search history where someone's search queries can be stored by Google and also mentioned other online public records of an individual. Another example was on social media usage where someone's friend might share a photo from a party everyone attended on social media. This photo might have revealed unnecessary information to everyone on the social media platform violating the privacy of the people in the photograph.

The second boundary was the *identity boundary*. In technology-mediated communication it can be difficult to determine who the recipient of information gathered is, making it hard to regulate how a person shares their information. This phenomenon is called *"recipient design"* where individuals adjust their behaviour depending on the person who receives the information. Humans also tend to change their action (disclosure of information) depending on the reaction of the receiver. This behaviour is called *"reflexive interoperability of action"*. The authors argued that technology has blurred the boundary between the user and external parties, hence users have lost control over their identity thus disrupting personal privacy management.

The third boundary was the *temporal boundary*. The authors argued that past events influence present and future privacy regulation mechanisms, resulting in the temporal boundary. The permanent and impermanent nature of technology-mediated information storage and sharing have impacted privacy regulation mechanisms. One good example provided by the authors was the way we share documents as PDFs instead of Word documents allowing us to have some level of control over possible altercations in the future.

Palen and Dourish mainly addressed information privacy regulation in the technological area. Therefore, their analysis didn't address physical privacy violations that arise within the smart home

and interpersonal privacy violations that occur due to shared devices. These aspects of smart home privacy will be explored in §2.1.3. Another aspect that was missing was the applicability of this theory in real-life settings: most of their case studies were hypothetical and may or may not represent real-life applicability. Even though some aspects of their analysis are no longer relevant it provided an understanding of how technology has disrupted information-sharing mechanisms.

Technology use has pushed physical boundaries to merge with virtual boundaries creating new boundaries as well as blurring the already defined physical boundaries. Mancini et al. (2009) argued that the definition of boundaries has moved from spaces to places. The authors explored mobile privacy while using social networking and their study found that a physical boundary defined a space where socio-cultural knowledge, functions and rules defined a place. From the study, they identified five boundaries that were socio-culturally motivated: 1) *personal policy*, 2) *inside knowledge*, 3) *etiquette*, 4) *proxemic*, and 5) *aggregation*.

The *personal-policy* b*oundary* explained the usage of privacy settings on the Facebook app and user behaviour about disclosing personal information to certain people. Facebook users might share information specifically targeted to a person excluding everyone else in their friends' list. *Inside knowledge boundaries* were defined to exclusively share with or withhold information from certain groups of people based on contextual knowledge. A person might safely share information on Facebook knowing that their parents are not on Facebook. *Etiquette boundaries* were boundaries that were defined out of respect to the people in the surrounding. Different ethics related to how individuals interact with social media when there are other people around is different. When someone goes out for dinner with friends, that person will not use Facebook out of respect to his friends. *Physical proximity* defined the proxemic boundary. A Facebook user might cover their phone using their handset or entirely refrain from using Facebook when there are other people around. *Aggregation boundaries* spanned across the physical world and the virtual world of Facebook. When there is a mismatch between what happens in the physical world and the virtual world there could be tension. An individual might not want to have their relatives on the Facebook page due to multiple reasons. If their relatives find out about this, it could create tension. The authors showed how technology usage has blurred the physical and virtual borders.

One of the drawbacks of this analysis is that it is based on an individual's Facebook usage. There are many other technology-based services (even social networks) which people use these days other than Facebook. These individual services can have their own set of mobile privacy violations and could create new privacy related boundaries. Another drawback is that this analysis focused on the interpersonal interaction side of privacy. Therefore, the study might have missed out some boundaries that were within the social network. For example, the authors did not explore boundaries such as *temporal boundaries* which applies to Facebook users. An individual might have something embarrassing posted in their youth, which, if seen later in life by work colleagues

could affect their reputation as well as have financial consequence. Mancini et al.'s analysis showed the importance of incorporating the socio-cultural lens when exploring mobile privacy which then can be extended to smart home privacy. The high number of smart home devices in our homes have infiltrated our physical boundaries infusing with our cyber boundaries. These new boundaries are not only bounded by physical or cyber boundaries but also socio-cultural knowledge, functions, and rules. Furthermore, they highlighted the importance of having flexibility when regulating privacy by different granularity level of information to different groups of people.

Privacy management on social networks can also be represented as a boundary management process. Karr-Wisniewski, Wilson and Richter-Lipford (2011) identified five virtual boundaries related to privacy when using social networks. They were *network*, *territorial*, *disclosure*, *relationship*, and *interactional* boundaries. *Network boundary* refers to the boundary that people use to separate different groups of connections from one another. Mainly two types of network boundaries were identified: whole and partial. As the name suggests, the whole network boundary allows the user to limit access to the entire friend list where the partial network boundary allows the user to hide individual connections on the friends' list. *Territorial boundaries* have two sub-boundaries: in-ward and out-ward boundaries. The in-ward boundary refers to what the user consumes. A prime example of an in-ward boundary highlighted by the authors was the *"News Feed"*. The out-ward boundary refers to the area in which the user shares information with their connections, such as the "Facebook Wall". *Disclosure boundary* regulates how and what information is shared with one's friend list. There were two types of disclosure boundaries identified. They were self-disclosure involving private information about oneself and confident disclosure of information that is co-owned by other people. *Relationship boundaries* define how users managed their friends on social networks. *Interactional boundaries* minimise direct access to a user. These could be the action of blocking a person (extreme case) or disabling certain features to minimise the interaction. The authors highlighted the differences that exist within social network usage. Even though this bought forward interesting findings, it lacked a few obvious boundaries concerning social network usages such as *temporal boundaries* and *communication boundaries*. Present-day smart homes are integrated with devices that have access to social media, consequently integrating them into our daily lives. Therefore, it is vital to examine the different virtual boundaries and how they integrate with physical boundaries. These analyses will lead to well-defined boundaries which can be used in smart homes with the effect of helping to better understand smart home privacy.

In the age of technology, analysing 'privacy as a function of context' helps to define a standard definition for privacy. Nissenbaum (2004) argued that existing privacy definitions did not cover the emerging challenges caused by the development of technology. One of the key arguments was that there is no universal definition of privacy, where it depends on the context specific norms and

values of information flows. She named this definition of privacy as *contextual integrity*. To present her case for *contextual integrity*, she analysed three existing privacy principles: (1) protecting the privacy of individuals against government surveillance, (2) restricting access to sensitive, personal or private information, and (3) protecting personal/private space. She highlighted how emerging technologies, such as sensing technologies (e.g., surveillance), might not fit into these existing principles. Furthermore, she used two informational norms to define *contextual integrity*: (1) *appropriateness*, and (2) *distribution* where both informational norms had to maintain integrity for *contextual integrity* to stand. As the name suggests, *appropriateness* defined if the disclosure of information is appropriate for the given context. She explained how sharing patients' medical information with their doctor is appropriate where vice versa is not appropriate. *Distribution* represents the integrity that needs to be protected when information has been transferred from one entity to another. Nissenbaum's idea of defining privacy as *contextual integrity* showed the need for flexible privacy definitions as well as the need to consider the context when addressing privacy issues. Therefore, *contextual integrity* sits well within the research scope as it motivates the need to analyse possible privacy violations within the smart home space with the help of the smart home context. The next section would explore how the concept of privacy manifests in ubiquitous computing.

2.1.2.3 Privacy in Ubiquitous Computing

Ubiquitous computing environments have created a new set of challenges in defining privacy due to their pervasive and intrusive nature. Konings and Schaubs'(2011) investigated privacy in ubiquitous computing environments and they defined the term *territorial privacy* using three territories: *physical* (T-phy), *extended* (T-ext) and *private* (T-prv) (Figure 2.2). The *physical territory* referred to the area indicated by physical boundaries around the user such as doors, walls, or curtains. The *extended territory* expanded from the physical space to the virtual space. Therefore, extended territory included both smart home communication devices that created an online space and the elements in the physical space that created the physical territory. They described the *private-territory* as a subset of the *extended-territory*. In this space, the user has the control to add/remove observers/disturbers as they see fit. They also highlighted the possible entities that could disrupt these boundaries. A user's privacy might be violated due to the entities observing or disturbing the user. These could be smart home devices such as embedded sensors, smart speakers, or smart TVs, as well as other co-occupants. The authors also discussed how people who live outside the environment can disturb the users via these networked devices. *Territorial privacy* filled a much-needed gap in the definition of privacy. Specifically, it improved the understanding of the term privacy in ubiquitous computing environments.

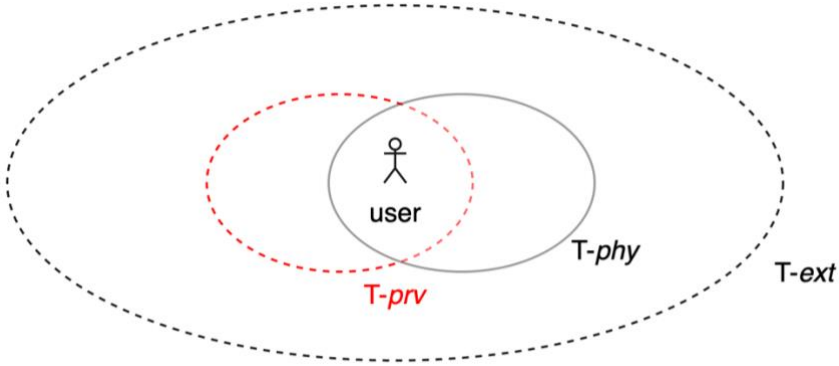

Figure 2.2: Territorial Privacy in Ubicomp Environments (Konings and Schaub, 2011)

One drawback of their work is that it failed to investigate interpersonal privacy violations. Smart home users share most of the smart devices such as smart speakers and smart TVs among the co-occupants. This shared nature of user interfaces could violate the interpersonal privacy of the smart home occupants: for example, using smart speakers to access personal information while another co-occupant is in the range of the smart speaker, thus disclosing personal information unintentionally. Another example is using smart TV to play a movie while everyone else is sleeping in the home, consequently disturbing other smart home users. These types of interpersonal privacy violations were not addressed in the *territorial privacy* definition. Therefore, it is vital to investigate the possible interpersonal privacy violations that happen at the user interface layer of the smart home to have a better understanding of privacy in smart homes.

Adding to the complexities of ubiquitous computing, multi-occupancy smart homes create a new set of challenges. Zeng and Roesner (2019) explored this aspect and identified that existing smart homes lack basic access control mechanisms and highlighted the possibility of creating adversarial situations due to such lack of controls. Zeng and Roesner evaluated a more flexible access control system to mitigate these challenges, however, their solutions had limited adoption due to high complexity and configuration overheads. This highlights the need for a simpler privacy authoring mechanism which could automatically accommodate users' privacy preferences and at the same time provide enough flexibility to personalise the experience. Furthermore, it also demonstrates the need to pay attention to the impact of smart home devices on interpersonal relationships.
Territories, boundaries, spheres, and spaces have helped to define the term privacy in multiple domains across time. From the inception of humankind to the development of social networks and ubiquitous computing, boundaries related to privacy have evolved from tangible to intangible and hybrid boundaries. The critical evaluation of the privacy literature provided in this section has shown the importance of revisiting the term privacy as technology evolves. One of the areas which has not yet been well explored is the interpersonal privacy violations that happen within a smart home due to the usage of shared public smart devices (user interfaces). Therefore, further investigation needs to be conducted to explore the implication of shared user interfaces in smart homes to its users' interpersonal privacy.

2.1.3 Types of Smart Home Privacy

As discussed earlier (§2.1.1), smart homes are a specific subset of smart environments where their distinct features impact the notion of privacy for their users. To understand smart home privacy, this section analyses the literature and categorises smart home privacy based on two factors as illustrated in Figure 2.3. One factor is based on the type of privacy where I have identified two categories: 1) information privacy, and 2) physical privacy. The other factor is based on the entity that is responsible for potential privacy violations where I have identified a further two categories: 1) user-service provider privacy violations, and 2) interpersonal privacy violations. The following section explores these high-level and sub-categories of smart home privacy violations.

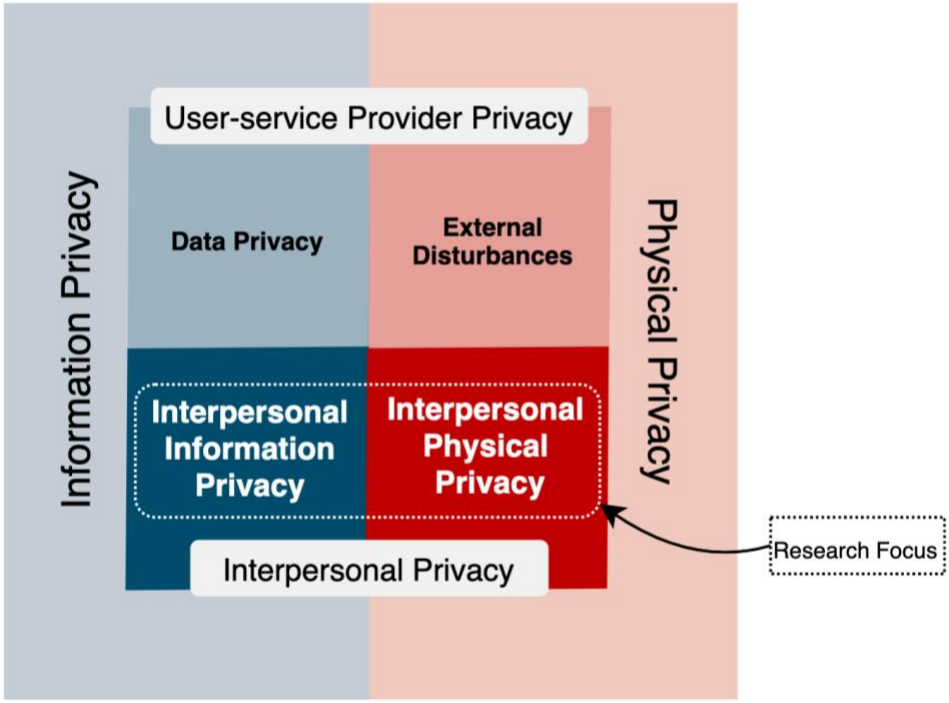

Figure 2.3: Smart Home Privacy Variations

2.1.3.1 Information Privacy

Information privacy refers to the individual's ability to control access to personal information. Information privacy aligns with Aristotle's concept of personal spheres where an individual considers certain aspects of his life to be personal (DeCew, 2002). Westin's (1967) definition of privacy gave a comprehensive summary of information privacy. He stated that privacy enables entities to control when, how and in what manner their personal information is shared with others. Information privacy has become a major focus within smart home privacy research due to the increased number of smart home device adoption. Information privacy is sub-divided into two areas for our ease of analysis: 1) data privacy (§2.1.3.3.1), 2) interpersonal information privacy (§2.1.3.4.1). These sub-categories would be discussed later in this section.

2.1.3.2 Physical Privacy

Physical privacy refers to an individual's ability to protect their solitude. The idea of physical privacy resonates with Hall's discussion of proxemics (1973). As he pointed out, an individual defines their personal boundaries based on socio-cultural practices. Aligned with Hall's argument, smart home users also define their personal boundaries based on socio-cultural practices where they perceive their space via their senses (visual, auditory, tactile, and olfactory). A disturbance that happens to any of these senses can be considered a physical privacy violation. Hall's idea provided a solid basis to define physical privacy in the smart home domain. The solitude of smart home users can be violated due to the smart devices in the space and the pervasive and shared nature of smart home devices brought a physical dimension to smart home privacy (Konings and Schaub, 2011). Therefore, safeguarding physical privacy is key for maintaining smart home privacy. For ease of analysis, physical privacy is sub-divided into two areas: 1) external disturbance (§2.1.3.3.2), 2) interpersonal physical privacy (§2.1.3.4.2). These sub-categories will be discussed later in this section.

2.1.3.3 User-Service Provider Privacy

User-service provider privacy focuses on the notion of privacy that arises between the smart home user and the smart home service providers. In the article *"A Taxonomy of Privacy"*, Solove (2006) presented four distinct areas where privacy could be violated : 1) *information collection*, 2) *information processing*, 3) *information dissemination* and 4) *invasions* (Figure 2.4). This categorisation focused on user-service provider privacy, and it didn't capture privacy violations that happen between smart home users (§2.1.3.4). From a smart home point of view, his first three categories can be used to explore the data privacy aspect (§2.1.3.3.1) while the fourth option can be used to explore external disturbances (§2.1.3.3.2) that can happen to smart home users. This section explores data privacy and the external disturbance related privacy.

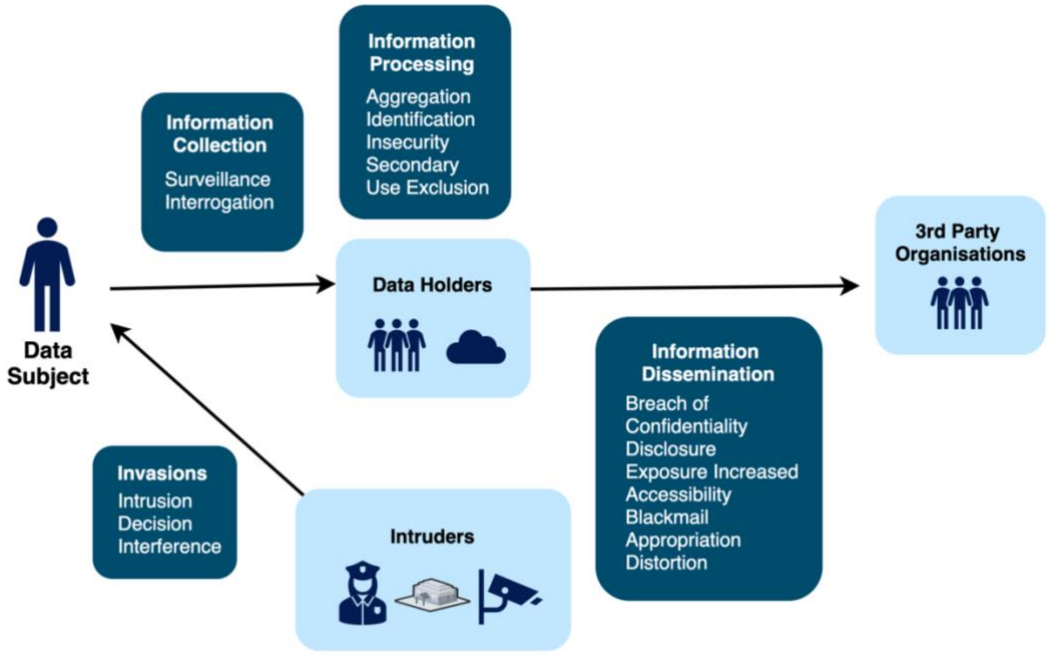

Figure 2.4: Solove's Taxonomy of Privacy (Solove, 2006)

2.1.3.3.1 Data Privacy

Data privacy refers to the safety and control that an individual has over their personal information when interacting with internet-based services. With increased availability and affordability, the rate of adoption of smart home devices has accelerated. These devices capture private data of the smart home uses and communicate them with the cloud service providers (Zheng *et al.*, 2018). Therefore, data privacy has become an important aspect of smart homes. This section explores data privacy violations within the smart home domain, data privacy laws and principles.

Data privacy has become a major concern within the smart home domain due to the accelerated rate of smart home device adoption (Zheng *et al.*, 2018). Solove's (2006) first three groups (Figure 2.4) help to investigate data privacy violations within the smart home space.

Information collection refers to the excessive data collection required to provide smart home services. For example, the Amazon Echo smart speaker's mic always listens and records the environment to identify the wake-word and it will send the recordings after the wake-word back to the cloud servers for processing (Jackson and Orebaugh, 2018). This operational behaviour can cause data privacy violations as it may record sensitive information and the saved recordings in the Amazon servers can be disclosed due to data breaches and possible misuse of data by Amazon. The adverse effects of privacy violations that happen due to information collection are amplified due to inaccurate mental models of smart home devices. For example, Abdi et al. (2019) highlighted that most of the smart home users had an inaccurate mental model of how smart home personal assistants operate.

Information processing refers to the processing of smart home user's data by the service providers. Netflix's data competition which shared movie rating data of half a million anonymised users were de-anonymised identified by aggregating movie rating data from IMDB (http://imdb.com/) (Shang *et al.*, 2014). Therefore, data processing conducted by smart home service providers may lead to data privacy violations.

Information disseminating refers to sharing smart home user's data with third parties without the consent of the users. Smart home devices share personal information of smart home users such as user habits and location data with third parties who are unrelated to the service provider (Ren *et al.*, 2019). The lack of transparency on how data is collected, processed, and shared with third parties makes data privacy a difficult problem to solve in the space of smart homes. However, government and regulatory bodies have started addressing data privacy issues by establishing necessary legal frameworks.

The General Data Protection Regulation (GDPR) (https://gdpr.eu) has become one of the most commonly used data privacy legal frameworks in the world. GDPR was passed by the European Union (EU) in 2016 and put in effect in 2018. Improving on its predecessors, Fair Information Practices (FIPs) (Commission, 1998) and European Data Protection Directive (https://eur-lex.europa.eu/eli/reg/2016/679/oj), its focus is on protecting user data of the European citizens.

Article 5.1-2 of GDPR presents 7 data protection principles. GDPR instructed that data should be processed in a *lawful, fair, and transparent* manner. Next, GDPR stated the data collections' *purpose should be limited.* Therefore, data processing should be in line with the original purpose stated at the collection and the data cannot be used for other purposes. In line with this principle, GDPR instructs organisations *to minimise the data collection* as well. The data collector should minimise the amount of data that they collect and the data they collect should be in line with their purpose of use. GDPR also instructed to keep *accurate information* of the data subject. It is the responsibility of the data controller to keep the data records up to date to maintain accuracy. Another important principle of GDPR is the *storage limitation* principle. According to this, personal data should not be stored more than the period needed for its purpose. Then, GDPR instructed to maintain *integrity and confidentiality*. This implies that personal data should be handled with adequate security measures as well as following the applicable laws. The last principle is *accountability*. GDPR instructs that the data controller should be able to show that organisations data practices are in line with GDPR compliance. If the data controller is unable to show this, the organisation is said to be non-compliant with GDPR. GDPR enforced smart home service providers and device manufacturers to put in place strong data protection mechanisms, but there was no incentive given or enforcement by GDPR for the smart home service providers to address interpersonal privacy violations (§2.1.3.4) or physical privacy violations (§2.1.3.2).

Therefore, interpersonal privacy and physical privacy protection is still an open problem that requires further attention from regulatory bodies.

2.1.3.3.2 External Disturbances

External disturbances refer to physical privacy (§2.1.3.2) violations that can be caused by external entities. Solove's (2006) fourth category, *invasions*, discusses possible disturbances to smart home users by external parties. He highlighted how an individual's solitude can be disturbed via junk emails and telemarketing calls. Furthermore, Konings and Schaub (2011) discussed how hackers can take control of smart home devices and physically disturb smart home users. As long as smart homes are connected to the internet, there is a risk of being disturbed by external entities. Hence, to protect the solitude of the smart home, it is required to have adequate privacy protection from external disturbances as well.

This section explored the privacy between smart home users and external entities, mainly focusing on smart home service providers. It explored the concept of data privacy and how it manifests in the space of smart homes. It also explored external disturbances within the smart home domain. Even though data privacy and external disturbances are not within the research focus of this thesis, they are important concepts that need to be understood when exploring privacy violations that happen within the smart home, which will be explored next.

2.1.3.4 Interpersonal Cyber-Physical Privacy

The adoption of smart home devices affects interpersonal privacy management between smart home users (Geeng and Roesner, 2019). This type of privacy is the other main sub-category of smart home privacy (Figure 2.3) which exists among smart home users due to the shared and pervasive nature of smart home devices (Luria *et al.*, 2020). I term this variation of privacy as *interpersonal cyber-physical privacy*. For brevity, the remainder of this thesis uses the term *interpersonal privacy*, omitting the '*cyber-physical'* component which is implicit in the context of smart homes. A sub-set of this type of privacy is also called bystander's privacy in the literature (Ahmad *et al.*, 2020) (Marky *et al.*, 2020) where it refers to the privacy of the users who aren't the primary user of the smart home device. My definition not only covers the bystander's privacy but also focus on how the bystanders impact the main user's privacy. Therefore, I define interpersonal privacy as: *"the ability of an individual in a cyber-physical space to safeguard their personal information and access to bodily senses while sharing devices and the space with other co-occupants"*. There are multiple factors that impact privacy between smart home users and careful investigation of those factors will help to fully understand the concept of *interpersonal privacy*.

The pervasive and shared nature of smart home devices impacts the interpersonal privacy of smart home users. Smart home devices can disrupt the individual's personal boundary (Konings and Schaub, 2011), consequently impacting the *interpersonal privacy* of smart home users (Marky *et*

al., 2020). Marky et al. highlighted how smart home devices can violate interpersonal information privacy. According to the authors, smart home devices such as sensors, microphones and cameras can readily capture occupants without their consent to provide smart home services. They also highlighted the problem of inadequate access control for shared smart home devices, which could lead to unauthorised access of personal information. Lastly, they reported how information can be leaked via shared devices such as smart speakers allowing bystanders to over-hear sensitive information of the main user. Konings and Schaub (2011) reported how smart home output devices, such as smart speakers, can disrupt the solitude of smart home users, violating interpersonal physical privacy. As Weiser (1993) stated, smart home devices tend to get invisible as they merge with the environment and with time. Therefore, traditional interpersonal physical privacy boundaries (Hall, 1973) tend to become ineffective in the space of ubiquitous computing. In addition, personal mobile devices can move across smart homes (Loitsch *et al.*, 2017), disrupting the personal boundaries of the smart home users and creating boundary turbulence (Petronio, 2015). This boundary turbulence influences how smart home users manage their privacy. Work presented in existing literature does not provide adequate means to manage *interpersonal privacy* violations which are caused by smart home devices. Therefore, an in-depth investigation regarding the impact of smart home devices on *interpersonal privacy* is needed to further understand the current status and to develop solutions for the protection of *interpersonal privacy*.

Apart from the direct impact of smart home devices, *interpersonal privacy* is also shaped by socio-cultural dynamics among smart home users, personal privacy preferences and user goals. Yao et al. (2019) highlighted how complex social relationships and power dynamics that exist within a smart home can affect privacy regulation among smart home users. They went on to explain how different social relationships among users can shape different privacy norms. For example, how smart home users change their behaviour when visitors are around and how certain members of the household have control over smart home device usage. Konrad et al. (2020) discussed how one smart home user's privacy preference might not align with another smart home user. They discussed how one of the smart home users might be flexible about sharing their personal information to acquire smart home services where another co-occupant might not be willing to share their personal information. The person who is not willing to share the information might not even know that their information is being collected via smart home devices for the main user to access smart home services. Zeng et al. (2017) also reported a similar idea where certain smart home users might have functional goals which are conflicting with another user's privacy goals. For example, the usability of the smart home can be a priority to the main user where the co-occupant might prioritise protecting their *interpersonal privacy*. This reviewed literature showed that that *interpersonal privacy* consists of distinct characteristics in comparison to user-service provider privacy (§2.1.3.3) due to the nature of smart homes. Therefore, it is necessary to factor in the impacts of socio-cultural dynamics among smart home users, personal privacy preferences and the goals of the smart home users when addressing *interpersonal privacy*.

This section looked at the definition of interpersonal privacy, factors the impact interpersonal privacy, and the value of interpersonal privacy. This motivated a re-examination of the concept of interpersonal privacy and interpersonal privacy protection mechanisms in the space of smart homes. Therefore, the rest of this section analyses two sub-categories of *interpersonal privacy*: 1) *Interpersonal information privacy*, and 2) *Interpersonal physical privacy*.

2.1.3.4.1 Interpersonal Information Privacy

Usage of shared smart home devices to access personal information can disrupt information privacy management among smart home users. I define this aspect of interpersonal privacy as *interpersonal information privacy* where it refers to the information privacy (§2.1.3.1) aspects that arise due to the shared nature of smart home devices among co-occupants. As mentioned earlier in this section, Marky et al. (2020) highlighted how interpersonal information privacy can be violated via shared devices due to unauthorised observations of the co-occupants and unauthorised access to smart home devices by co-occupants. They also discussed how unintentional information leakages that happen via output channels can be another way that *interpersonal information privacy* can be violated. Even though this is a major drawback, the existing smart home devices don't provide adequate mechanisms to safeguard *interpersonal information privacy* (Huang, Obada-Obieh and Beznosov, 2020) and the majority of the research focus has been only on the data privacy aspect (Zeng, Mare and Roesner, 2017). The rest of this section explores some variations of *interpersonal information privacy*.

Unauthorised observations

Input channels of smart home devices can continuously capture and store information of the smart home users. Smart home cameras can capture the smart home occupants without their consent, making them one of the most privacy invasive devices. Bernd et al. (2020) reported that domestic workers in households express privacy concerns regarding smart home cameras but they are not in a position to enact their privacy preferences. Smart speakers are another category of devices that can capture sensitive information of the co-occupants without their consent. As mentioned previously, a smart speaker functions by constantly listening for its wake-word and recording the audio input which follows the wake-word. Then it will send the recorded input to the cloud for further processing (Jackson and Orebaugh, 2018). Due to this operational behaviour of smart speakers, smart home users are concerned that their sensitive conversations are recorded and can be shared with external parties (Lau, Zimmerman and Schaub, 2018). Smart home devices which can capture multiple users, such as smart speaker microphones and smart home cameras, pose a significant threat to smart home users' interpersonal privacy. This is due to the personal boundary walls getting disrupted due to the permeability of smart home devices. Therefore, to protect the *interpersonal information privacy* of smart home users it is necessary to safeguard the users from unnecessary and unintentional observations of smart home input devices.

Unauthorised access

Most of the shared smart home devices lack strong access control, consequently allowing co-occupants of the smart homes to access the personal information of the smart home device's owner. Current smart speakers in the market do not provide strong authentication mechanisms to distinguish between smart home users, which leads to unauthorised access. Huang et al. (2020) reported some of the unauthorised access issues regarding smart speakers. They found that smart home users were concerned with unauthorised voice purchases that can be done via smart speakers. They also mentioned how smart home users were concerned with unauthorised access to their personal calendar and personal reminders which can also be accessed via the smart speaker. Lastly, they reported smart home users concerns regarding misuse by unintended users such as children living or visiting the smart home Therefore, managing unauthorised access to shared devices within the smart home space is quite important when protecting *interpersonal information privacy*.

Information leakages

Output channels of shared smart home devices may leak sensitive information of the main user to bystanders. Smart speakers are one of the commonly used smart home devices that are shared by smart home users. Due to the voice-based interaction mechanism, smart speakers can leak sensitive information to the other co-occupants. Huang et al. (2020) reported on smart home users concerns regarding the information leakages that can happen when interacting with smart speakers. The findings highlighted how the co-occupants who are nearby can hear the interactions with the smart speaker. Smart TVs and public displays also pose a similar threat due to information leakages. Brudy et al. (2014) reported how using shared public displays (not necessarily focused on smart TVs) for personal work can leak sensitive information to bystanders due to shoulder surfing. These acts can be intentional or unintentional, but the result will be the same with personal information being leaked to bystanders. Existing smart home devices such as smart speakers and smart TVs provide limited support for handling these type of information leakages as they are predominantly targeted at a single user (Huang, Obada-Obieh and Beznosov, 2020). Therefore, handling unintentional information leakages is critical for protecting *interpersonal information privacy*.

This section explored the definition of *interpersonal information privacy* and how it can be violated. It presented three ways in which *interpersonal information privacy* can be violated: 1) unauthorised observations, 2) unauthorised access 3) information leakages and motivated the need for smart home devices to provide necessary measures for handling *interpersonal information privacy*. The next section explores the physical privacy aspect of interpersonal privacy.

2.1.3.4.2 Interpersonal Physical Privacy

The capability of smart home devices to permeate through physical boundaries makes the physical aspect of privacy (Burgoon, 1982) relevant to smart home privacy (Konings and Schaub, 2011).

Smart home devices with public output channels can disrupt the solitude of smart home users (Konings and Schaub, 2011). I define this aspect of interpersonal privacy as *interpersonal physical privacy* which refers to the physical privacy (§2.1.3.2) aspect that arises due to sharing smart home devices among co-occupants. The rest of this section explores some of the *interpersonal physical privacy* violation variations within the smart home space.

Disturbances

Shared smart home devices can disrupt the solitude of smart home users. These disturbances could happen via human senses such as auditory senses, visual senses, tactile sense, and olfactory senses. Konings and Schaub (2011) discussed how ambient output devices and remote-controlled devices can violate the smart home user's solitude. Ambient devices are smart home devices that are embedded in the smart home. These could be public displays or blinking LEDs which can cause visual disturbances or speakers which can cause auditory disturbances. Remote controlled devices could be smart home smart curtains, temperature controllers or lights. Changing the state of these devices can disturb smart home users. Existing smart home devices provide minimal or no control and awareness regarding disturbances that they can cause to the co-occupants. Therefore, adequate mechanisms are needed for existing smart home devices to minimise the disturbances that they may cause when shared by smart home users.

Forced engagement

Smart home devices create communication channels that connect smart home users to the external world. This can be a virtue at times, but it also can be a burden as smart home users can be forced or expected to engage with external parties due to social obligations. Judge et al. (2011) reported how smart home users were expected to engage with their relatives as there was a mechanism to readily engage with them. This type of engagement can be a disturbance caused by a psychological point of view as smart home users might struggle to have peace of mind when needed. Therefore, smart home devices should accommodate smart home users to protect their solitude when needed.

This sub-section explored the definition of *interpersonal physical privacy* where two variations were discussed: 1) disturbances, and 2) forced engagement. The sub-section motivated the need for smart home devices to provide necessary measures for handling *interpersonal physical privacy*.

2.1.4 Summary

The major focus of smart home privacy research has been on privacy violations that happen between smart home users and the smart home service providers (§2.1.3.3). Therefore, there is a significant gap in the literature regarding privacy violations that happens among smart home users, which I termed *interpersonal privacy* (2.1.3.4). Since interpersonal privacy violations happen at the user interface layer of the smart home, it can be hypothesised that adapting the user interface layer will protect *interpersonal privacy*. This was further emphasised by the Zeng and Roesner's (2019) work where they highlighted the need for a simpler, automated privacy protection mechanism. Therefore, the next section explores the literature regarding smart home user interfaces to find adequate tools to develop a mechanism to adapt the user interface layer and to identify any research gaps.

2.2 Adaptive Smart Home User Interfaces

As the previous section identified, adapting the smart home user interface layer has the potential to protect the interpersonal privacy of smart home users. This requires the user interface layer to understand the context and adapt the user interface layer to mitigate interpersonal privacy violations, where the context refers to the information representing the users, the smart home environment, ambient and temporal features.

Capturing this knowledge and reasoning to drive user interface adaptations is a challenging task due to the nature of smart homes. Smart homes have multiple users with different privacy preferences (Karami *et al.*, 2016), user interface preferences (Casas *et al.*, 2008), and capabilities (Smirek, Zimmermann and Ziegler, 2014). Furthermore, smart homes and their users have multiple smart devices with different modalities and technologies (Blumendorf, 2009). Therefore, it is a common practice to use engineering frameworks to construct the user interface layer as it would manage the aforementioned complexities and develop a dependable, robust and extensible user interface layer. For example, MASP (Blumendorf, 2009) and MIODMIT (Cronel *et al.*, 2019) have used engineering frameworks to generate adaptive smart home user interfaces. This motivated a literature review of the adaptive smart home user interface frameworks to evaluate the state of the art and to identify any research gaps.

This section first provides the fundamentals of smart home user interfaces and adaptive user interface frameworks which will support the evaluation of the rest of the literature. This is followed by a review of the existing user interface frameworks and their research gaps. Finally, user modelling techniques will be reviewed to identify models to represent the user's user interface preferences, capabilities, and privacy preferences.

2.2.1 Background

This section explores the characteristics of smart homes and how it impacts the user interface layer. Then it will discuss the advantages and disadvantages of adaptive multimodal user interfaces in smart homes. Finally, it will present the fundamentals of adaptive user interface frameworks.

2.2.1.1 Characteristics of Smart Home User Interfaces

To better understand smart home user interfaces, it is important to understand the unique characteristics of smart homes and how they impact the user interface layer. Blumendorf (2009) discussed six different functional characteristics of smart environments. Since smart environments are a generalisation of smart homes which have similar functional characteristics, I will utilise Blumendorf's categories to evaluate smart homes.

Multiple users: In general, smart homes are shared by multiple users who may have varying capabilities and preferences. Existing smart home devices provide minimal support for shared usage and personalisation. Therefore, this creates a challenge when developing a user interface layer that is usable to all smart home users.

Multiple devices: Smart homes consist of multiple devices which are permanent within the smart home and semi-permanent or impermanent devices which are carried into and out of the smart home by the smart home users. This adds to the complexity of the user interface layer as it needs to represent these different devices that move across the environments and may have different underlying technologies.

Multiple modalities: In contrast to traditional single-modal user interfaces, multiple smart home devices provide users with multiple modalities to interact with the smart home. This enables the smart home to generate adaptive user interfaces catering for users with varying capabilities and preferences.

Multiple applications: A smart home provides multiple applications for its users. These can be provided via different user interface and modalities.

Multiple situations: Due to the dynamic nature of smart homes, there could be multiple situations that arise within the smart home. Therefore, the same application can be used by the same person in two different ways due to the context difference. This adds to the challenges of generating smart home user interfaces as evaluating the context is important to deliver the best user experience to the smart home users.

The aforementioned characteristics shaped the user interface layer of the smart home where Blumendorf (2009) discussed five of those features:

Adaptable: The smart home user interface layer can be adapted based on the context and the user needs. These adaptations can be feature adaptations (adapting the modality or the device in use) or modality switches (changing the interaction modality or the device). This enables the provision of a usable and preferred user interface to the smart home users with varying preferences, capabilities and need.

Distributable: The connected nature of smart homes allows having a distributed user interface layer where users can interact with the smart home via multiple devices at different locations. This enables ease of use as users can interact with the smart home while moving to different locations. An interaction started at one point in the smart home can be paused and resumed from another point in the smart home due to the distributed nature of smart home user interfaces.

Multimodal: The number of different user interfaces available in the space makes the smart home user interface layer multimodal. This could improve the user experience of the smart home as multimodal interactions promote more natural interactions with the smart home as well as provide affordance to user's preferences and capabilities.

Sharable: Due to the shared nature of the smart home, the user interface layer is shared among the smart home users. Devices such as smart speakers, smart TVs and thermostats are some of the devices that are generally shared by smart home users. This aspect of smart home UIs can create novel interactions among smart home users as it promotes and allows users to have a collaborative interaction with the smart home. It may also create possible interaction conflicts or privacy violations among the co-occupants.

Mergeable: Due to the connected nature of the smart home user interface layer, it provides the ability to merge certain user interactions. For example, users can combine input modalities to provide input using their voice and touch as well as combine output modalities to receive system outputs through audible and visible channels.

These features of smart home user interfaces impact interpersonal privacy (§2.1.3.4) in diverse ways. For example, the **sharable** nature of smart home user interfaces creates scenarios that could violate interpersonal privacy, such as when a shared smart speaker leaks sensitive information of the main user to the co-occupants, violating the information privacy aspect of interpersonal privacy (§2.1.3.4.1). Another example is that a smart TV can be played loudly disturbing another co-occupant who is sleeping in a nearby room violating the physical privacy aspect of interpersonal privacy (§2.1.3.4.2).

Similarly, while user interface features could induce interpersonal privacy violating scenarios, they can also mitigate or minimise those violations. For example, **adapting** the user interface layer will

allow the protection of interpersonal privacy. Sensitive information can be diverted from the smart speaker (public/shared user interface) to a smartwatch (private user interface) when someone can overhear the conversation, or the volume of the smart TV can be reduced when a co-occupant is sleeping. User interface adaptation is complemented by the **distributable**, **multimodal** and **mergeable** nature of smart home user interfaces as it provides the flexibility to generate privacy-aware usable user interface adaptations.

2.2.1.2 Opportunities and Challenges of Adaptive Multimodal User Interfaces

This section explores the positives and the negatives of adaptive multimodal user interfaces to further understand how they can be used for the protection of interpersonal privacy; and the possible challenges of doing so. Duarte (2007) discussed the advantages and disadvantages of adaptive multimodal user interfaces:

Advantages of adaptive multimodal user interfaces

Flexibility: In comparison to a traditional user interface where users are stuck with a single modality or a single device, adaptive multimodal user interfaces provide the users with an option to interact with the system as they see fit. In a smart home setting, this accommodates a wide range of interaction possibilities supporting different user capabilities, preferences, and needs.

Stability and robustness: Due to multiple input sources, multimodal user interfaces improve the accuracy of services such as activity recognition. They also provide fallback options for users to interact with the system; making the user interactions more resilient to change, thus making them robust.

Efficiency: When the system is accepting user inputs or outputting system information to the user, the multimodal user interfaces provide a means to combine modalities or to select the most appropriate modality based on the context. Doing so improves the efficiency of the interaction when compared with single modal user interfaces.

Accommodating User Preferences: Adaptive multimodal user interface can provide user interfaces that are in line with the user's preferences. Depending on the user's preference and the context, the user interface layer can be adapted which will result in a better user experience.

Disadvantages of adaptive multimodal user interfaces

Hunting problem: When users interact with user interfaces, they tend to create a mental model of how the interaction happens. These mental models tend to get disrupted with adaptive user interfaces. Therefore, users may struggle to create a consistent mental model when interacting with adaptive user interfaces.

Loss of control: Another drawback is the feeling of losing control when interacting via adaptive multimodal user interfaces. Since adaptations can happen automatically and it is harder to predict how and when some adaptations may occur, users tend to have a feeling of losing control of the interaction.

Reliability: In line with the previous disadvantage, a user may feel that adaptive multimodal user interfaces lack reliability. This problem is worsened when users are not aware of the context change which trigged the adaptation or if the users are quite new to the system.

Privacy: Another drawback is the possible privacy violations that could happen due to adaptive multimodal user interfaces. Other users could access/overhear the personal information of another user, or they can be disturbed due to the shared nature of the multimodal user interface.

When developing a framework to generate privacy-aware adaptive user interfaces, it is vital to understand the positives and negatives of generated user interfaces to leverage the positives and mitigate the negatives.

Adaptive multimodal user interfaces will cater for individual user's needs and preferences to support the generation of user interfaces that are usable and privacy protective. In addition, these adaptations may also improve the efficiency of the interaction, as users could achieve their tasks via multiple means. On the other hand, the framework should try to mitigate the negative aspects of adaptive multimodal user interfaces. For example, providing explanations for adaptions and reminding before an adaptation would improve the user's trust with the smart home system.

2.2.1.3 Fundamentals of Adaptive User Interface Frameworks

This section presents some of the fundamentals of adaptive user interface frameworks which need to be understood before reviewing the literature in the following section.

MAPE-K Loop (Kephart and Chess, 2003) is a commonly used reference framework for developing self-adaptive systems. It consists of five main components (Figure 2.5) where MAPE (*Monitor, Analyze, Plan, Execute*) components construct the control loop and the K (*Knowledge*) component is shared among the control loop elements. *Monitor* refers to the automated mechanisms of continuous context information collection required by the system. *Analyze* refers to the evaluation of context to determine if something has changed. *Plan* refers to strategizing the necessary actions to address context change. *Execute* is the step of enacting the planned strategy. Knowledge represents the stored information regarding the system that is required by the control loop components. MAPE-K loop helps to lay the foundation for an adaptive user interface framework by providing the necessary components required for the adaptation of user interfaces.

Different frameworks have implemented the control loop components to fit their approach but almost all the frameworks have utilised MAPE-K loop in one form or the other.

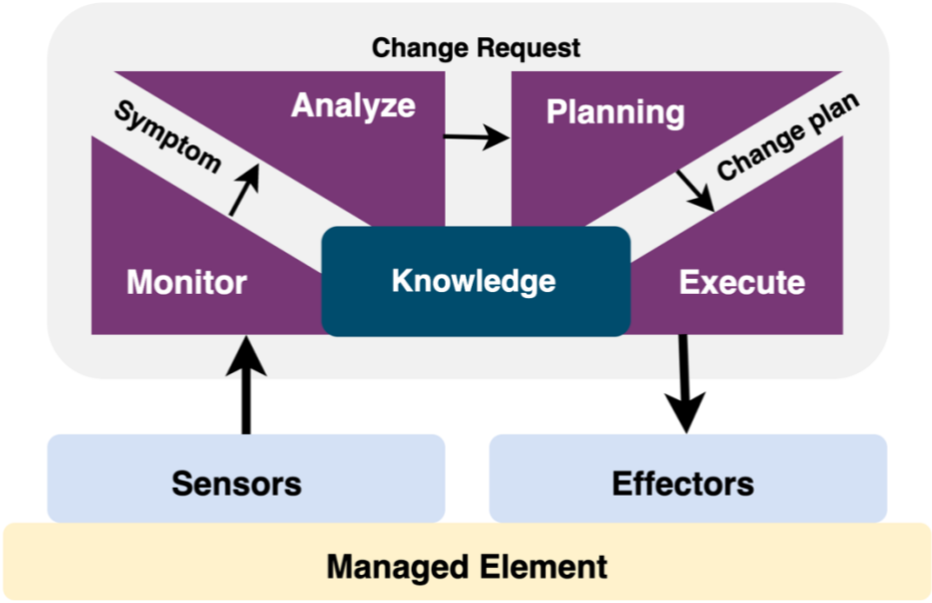

Figure 2.5: MAPE-K Loop (Kephart and Chess, 2003)

MVC (Model-View-Controller) architecture (Reenskaug, 1979) is an architecture pattern that supports the development of interactive systems. Even though it was originally developed for GUI based systems, it has now been adopted to multimodal systems such as smart homes with minor adjustments. The architecture consists of three main components: *Model, View and Controller*. *Model* refers to an abstract representation of data objects in the system. In a smart home setting, this could be a smart home user or a user interface. In the original document, *View* referred to the visual representation of a *Model* wherein a smart home setting it could refer to multimodal user interfaces or other smart home components which would be operated by the architecture. *Controller* sits in between the user and the system accommodating the user interaction which will manipulate *Model* layer and the *View* Layer components according to the user's requests. MVC architecture can be used to develop smart home user interface frameworks as it provides an adequate base architecture to construct extensible and maintainable framework as it provides a clear separation of concerns between different layers of the system.

The Cameleon framework (Calvary, Coutaz and Thevenin, 2001) is a reference multimodal user interface framework for ubiquitous computing. The framework presented domain models, task models, the context of use in the framework (Figure 2.6). User interfaces were divided into three main parts as abstract UI, concrete UI, and final UI. Based on domain models and task models, interaction designers were able to define an abstract UI. The abstract UI was defined as platform independent interactions which helped the designers to define modalities of the interaction. Then the abstract UI can be mapped to a concrete UI which were platform dependent interactions. In the last step, the final UI was used to define the device dependent interaction components.

The intention was not to provide an engineering framework; hence it didn't provide user models, multimodal fission, multimodal fusion, and user interface adaptation mechanisms. It was to act as a reference framework for the development of model-driven user interface generation. Therefore, the Cameleon reference framework has been used by many smart home user interface frameworks which adopted a model-driven architecture.

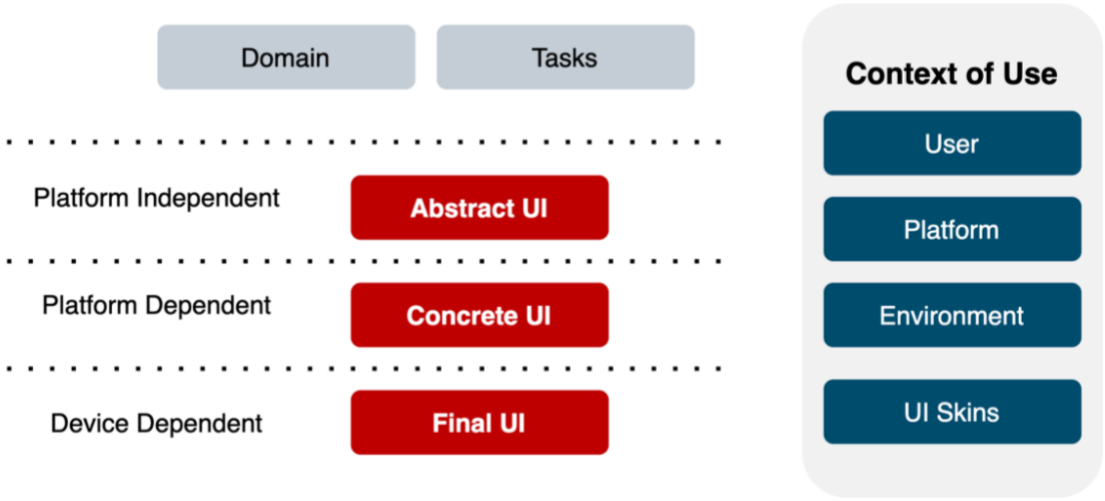

Figure 2.6: Cameleon Reference Framework (Calvary, Coutaz and Thevenin, 2001)

The MAPE-K loop, MVC architecture and the Cameleon framework provided the foundation for the development of most of the adaptive user interface frameworks. These can be used in different aspects of the framework and most of the recent research regarding adaptive user interface frameworks have directly or indirectly adopted these frameworks/architectures when developing their frameworks. The following section presents the review of the adaptive user interface frameworks.

2.2.2 Adaptive User Interface Frameworks

Adaptive user interface frameworks provide an engineering approach for building dependable, robust, and extensible smart home user interfaces. This section reviews the literature regarding the adaptive user interface frameworks, where it analyses the state of the art to identify the research gap. The review is supported by the criteria developed based on the functional requirements of a framework that can generate privacy-aware smart home user interfaces. These requirements were elicited from the example interpersonal privacy violating scenarios presented in Chapter 1. The criteria anchored the review by providing a benchmark to evaluate the level of support provided by each framework for generating adaptive user interfaces. The following section presents and justifies the criteria and Table 2.1 explains the various categories of each criterion.

2.2.2.1 Criteria

Multimodal support: This refers to the support provided by the framework for generating multimodal user interfaces. Smart home user interfaces are multimodal in nature and the framework should be able to represent these different modalities.

Fission and fusion modelling: Fission refers to the framework's ability to split the output stream into multiple modalities or devices and fusion refers to the ability to accept input from multiple modalities or devices for a given interaction. Smart home user interfaces are multimodal and distributed in nature. When adapting to protect privacy, the framework should have the means to switch the broadcast of information between modalities (or devices) and accept inputs from different modalities (or devices).

Engineering framework: This assesses whether an approach provides an engineering framework to develop the user interface layer. It is relevant because an engineering framework helps to implement dependable, robust, and extensible user interfaces and support effective run-time user interface adaptations.

User modelling: This evaluates the support provided by the framework for user modelling. The framework should support the modelling of user's preferences (privacy and user interface) and capabilities to drive effective and usable adaptations. Therefore, generating user interface adaptations based on accurate user models ensures that the adaptations are usable, privacy preserving user interfaces that are preferred by the users.

Adaptability: This evaluates the support for user interface adaptations provided by the framework. The framework needs to accommodate both feature adaptations (i.e., adapting the modality in use) and modality adaptation (i.e., switching to a different modality) to generate privacy-aware user interface adaptations.

Context modelling: This evaluates the level of support provided by the framework to support the context apart from the user models. The framework needs to understand the smart home context to decide when and how to drive adaptations. These models should represent the entities related to the smart home: smart home layout, smart home users (beyond personal preferences and capabilities), smart home devices and other factors defining the smart home.

Support / Criteria	No support (○)	Partial support (◗)	Full support (●)
Multimodal support	Multimodality is not supported	Supports only one type of modality (input or output) or limited support for both modalities.	Fully supports both types of modalities
Fission and fusion modelling	Fission and fusion not supported	Supports one aspect (fission or fusion) or limited support for fission and fusion	Fully supports fission and fusion both
Engineering framework	No engineering framework provided	Provides Minimal information on how to engineer the user interface layer.	Comprehensive engineering framework with worked examples.
User modelling	No support for user modelling	Provide either privacy preference modelling or capability and user preference modelling.	Comprehensive user model with capability and user preference modelling (both privacy and user interface)
Adaptability	No support for user interface adaptations	Supports one type of adaptation or limited support for both variations of adaptations.	Supports modality adaptation and feature adaptations.
Context modelling	No support for context modelling	Partial support for context modelling.	A comprehensive set of models for smart home layout, user tracking, device tracking, and other types of environment tracking.

Table 2.1: User Interface Framework Evaluation Criteria

2.2.2.2 Review

Apart from the criteria mentioned in Table 2.1, the review also looked at how authors have evaluated their frameworks and the level of coverage they provided regarding the scenarios they used to evaluate the framework.

Dynamo-AID (Clerckx, Luyten and Coninx, 2004) (Appendix B: §10.2.1) is a model-based runtime architecture for user interface development that focused on building context sensitive user

interfaces based on task models. The framework provides WIMP-style user interface support, a run-time architecture, task model-based user interface adaptations and limited context modelling support. It does not address fission, fusion, and user modelling. Dynamo-AID provided one of the first examples of adaptive interaction modelling using concurrent task trees (CTT) (Paternò, Mancini and Meniconi, 1997) in the ubiquitous computing space but due to the coupling between the UI and task models, it restricted the scalability of the adaptations. Even though Dynamo-AID was not sufficient to be directly used for the purpose of generating privacy-aware adaptive user interfaces, it provided inspiration to use CTT to develop adaptive user interfaces.

The MASP (Multi-Access-Service-Platform) framework (Blumendorf, 2009) (Appendix B: §10.2.2) adopts a model-driven solution to develop and handle the runtime management of smart environment user interfaces. Overall, MASP provides a comprehensive context model which represented the features of different user interfaces, smart home layout and smart home users (beyond personal preference and capabilities). It provides multimodal support, fission, fusion, and an engineering framework to develop the user interface layer. MASP supports feature adaptation of the user interface layer but didn't present a mechanism for modality adaptation. The framework also provides limited support for user modelling, but it did not cover dimensions such as user's privacy preference, user interface preferences and user capabilities. MASP's user models consist of the necessary information needed to support simultaneous multiple users, but no evaluation was conducted to test this capability. In conclusion, MASP is a good enough framework that provides the foundation needed to develop a framework to generate privacy-aware user interface adaptations.

AALuis (Mayer *et al.*, 2013) (Appendix B: §10.2.3) is a middleware that provides a personalised interface for users with different abilities (especially for older adults). The authors discussed user context models, device context models, service context models and environmental context models, but these models were not provided. When developing the context models of AALuis, the authors have considered the requirements of different stakeholders, but they have not integrated user's privacy preferences into the user context models. Overall, AALuis does not provide sufficient details and coverage to support the development of privacy-aware adaptive user interfaces but similar to Dynamo-AID (Clerckx, Luyten and Coninx, 2004) it provided inspiration to use CTT to develop adaptive user interfaces.

AALFI (McNaull *et al.*, 2014) (Appendix B: §10.2.4) focuses on an adaptive multimodal user interface for ambient assisted living during the night time. It only supports visual and auditory modalities, and it does not support fission and fusion. They provide implementation details of the framework and the processes used to generate adaptive user interfaces. The framework provides comprehensive context models and partial user models. Context models can model the status of the environment and user models capture user's user interface preferences and user capabilities. Both

these models support the feature adaptation of the modality, but the framework provides no support for modality switching at run-time. Since the context model is limited by the scope of this framework (only focussing on GUI and voice), their extensibility to smart homes with multimodal user interfaces is limited. Another drawback of the AALFI is that the user modelling feature does not support privacy preference modelling. Therefore, AALFI is not extensible enough to engineer a privacy-aware smart home user interface layer but provided valuable dimensions needed for adaptive user interface generation such as context modelling and user preference modelling.

The Cedar architecture (Akiki, 2014) (Appendix B: §10.2.5) is a reference architecture for developing adaptive model-driven enterprise application user interfaces. Due to the scope of this work, it only supports adaptations related to desktop-based GUIs. Therefore, there is no discussion on multimodality, fission, fusion, or context modelling. But the framework provides a comprehensive engineering framework with detailed models and architecture diagrams. The architecture supports user interface adaptations via reducing the features and optimising the layout of the GUI, but there is no modality switching as the focus is on GUI. Apart from that, the framework also does not provide means to model user's privacy preferences. Even though the Cedar architecture is not supportive of smart home user interface generation directly, its use of an engineering framework with the integration of CTT (Paternò, Mancini and Meniconi, 1997) for task modelling and feature-based adaptations are quite valuable foundations for developing privacy-aware smart home user interface generation.

The GPII personalisation infrastructure (Loitsch *et al.*, 2017) (Appendix B: §10.2.6) presents a knowledge-based framework that guides the generation of different layers of multi-modal application to provide universal accessibility. The GPII framework supports multimodal user interfaces, but there is no support for fission or fusion. It also does not provide an engineering framework for generating user interfaces where it only provides a rule-based mechanism to adapt the user interfaces based on the user's capabilities and preferences. Apart from that, GPII presents a conflict resolution mechanism, but it is limited to the handling of application-level conflicts.

GPII provides limited context modelling support, and it did not support smart home layout modelling and user location tracking. The user modelling only supported user's capability modelling and limited preference modelling where it didn't support modelling user's privacy preferences. It also lacked support for multiple users since the focus has been on a single user who may move across environments. Another drawback is that the adaptive user interfaces have only been evaluated with experts, but not with real users. In conclusion, the GPII framework is not sufficient to develop privacy-aware user interface adaptations, but it highlighted the importance of modelling the user's capability and the usage of a rule-based reasoning engine to develop user interface adaptations.

MIODMIT (Cronel *et al.*, 2019) (Appendix B: §10.2.7) is a model-based generic architecture for smart environments supporting multimodal user interfaces which focused on software as well hardware aspects. It supports multimodal fission and fusion, but it does not support user modelling or context modelling. The authors do not provide enough information on how the user interface modelling can be implemented as the architecture discusses most of the components at a high level. Therefore, the MIODMIT architecture needs to be improved to meet the requirements of generating privacy-aware adaptive user interfaces.

AM4I (Almeida *et al.*, 2019) (Appendix B: §10.2.8) provides an architecture and a framework to design multimodal and multi-device smart home user interfaces. The architecture supports input and output modalities, fusion and fission, and models to handle context and users. The framework supports concrete deployment of the architecture to create interactions within the smart home. AM4I's user models provided basic support for privacy and user interface preference modelling where they mentioned the possibilities of interpersonal privacy violations that could happen at the user interface layer.

One of the drawbacks of the AM4I was the lack of support for multiple users in real-time. Furthermore, the context models and the user models need to be developed further. Improvement of the context models would allow the framework to handle the spatial layout of the smart home which is required for privacy violation detection. User modelling needs to be improved to provide more detailed user capabilities, privacy preferences and user interface preferences. These improvements are required for AM4I to handle all the possible interpersonal privacy violations.

Sapiens (Schipor, Vatavu and Wu, 2019) (Appendix B: §10.2.9) is an engineering framework for interactive smart home systems. The framework supported multimodal use interfaces, user modelling and context modelling. Context modelling included device and user tracking and other environmental information. User modelling supports basic representation, and it has provided spatial modelling for smart home entities, but it was only tested using a web-based prototype. Therefore, it needs to be tested with real-world applications. Did not capture users' privacy preferences nor user interface preferences. Furthermore, it does not provide details on user interface adaptations. Sapiens provided some valuable components needed to develop privacy-aware adaptive user interfaces, but it was not sufficient for a concrete implementation.

Table 2.2 summarises the analysis of the models against these criteria; each model is then discussed in turn. General descriptions and architecture diagrams for each model are provided in Appendix B (§10.2).

User interface framework	Multimodal support	Fission and fusion modelling	Engineering framework	User modelling	Adaptability	Context Modelling
DynaMo-AID (Clerckx, Luyten and Coninx, 2004)	◗	○	○	○	○	○
MASP (Blumendorf, 2009)	●	●	●	◗	◗	●
AALuis (Mayer *et al.*, 2013)	○	○	○	◗	◗	◗
AALFI (McNaull *et al.*, 2014)	◗	○	●	◗	◗	◗
CEDAR (Akiki, 2014)	○	○	●	◗	◗	○
GPII (Loitsch *et al.*, 2017)	●	○	◗	◗	◗	○
MIODMIT (Cronel *et al.*, 2019)	●	○	●	○	○	○
AM4I (Almeida *et al.*, 2019)	●	●	●	◗	○	◗
SAPIENS (Schipor, Vatavu and Wu, 2019)	●	○	◗	◗	○	◗

Table 2.2: Summary of the Evaluation of User Interface Frameworks

2.2.2.3 Discussion

A framework that can support the generation of privacy-aware adaptive user interfaces needs to support multimodality, fission, fusion, context modelling, and user modelling. It is also helpful for it to provide an engineering framework. The context models should be comprehensive enough to support different contexts within the smart homes and the user models should be able to represent different users' capabilities and preferences regarding user interfaces and privacy. This will enable the framework to generate effective and usable privacy-aware user interface adaptations.

As identified in this section, the existing user interface frameworks do not provide means to protect interpersonal privacy, but they cover different aspects required for generating privacy-aware adaptive user interfaces. Most of the frameworks support multimodal user interface generation; the exceptions are Dynamo-AID, CEDAR and AALuis. MASP and AM4I comprehensively cover fission and fusion of multimodal user interfaces, where other frameworks do not. It is helpful to have an engineering framework to support the generation of smart home user interfaces; MASP, CEDAR, MIODMIT and AM4I provided such engineering frameworks but CEDAR focuses only

on GUI and MIODMIT only provides limited information required for implementation. MASP and AM4I are quite comprehensive regarding their engineering frameworks but MASP is slightly better as it provides more details regarding the models and the framework's functionality.

For the adaptations to be effective they need to be based on the user requirements and context information. None of the frameworks provides a comprehensive user model required to create privacy-aware user interface adaptations. Some frameworks such as MASP, GPII, MIODMIT and AM4I provide some level of user modelling features, but they lack the ability to capture users' privacy preferences. MASP was the only framework to provide comprehensive context models including smart home layout modelling. This aspect is quite important to assess possible privacy violations and to drive the correct adaptation.

The other aspect is the support provided for the adaptations in each framework. Most of the frameworks provide some notion of adaptation but none of them modelled both feature adaptations and modality switching type of adaptations.

Considering the requirements criteria (Table 2.1), the MASP framework can be considered the most adequate framework to draw inspiration from for developing a framework that can support privacy-aware user interface adaptations. But the MASP framework lacked comprehensive user modelling capability which can model user's privacy preferences, capabilities, and user interface preferences. Therefore, the next section reviews the smart home user modelling literature to identify suitable models to fulfil the knowledge representation requirements.

2.2.3 Smart Home User Modelling

The term user modelling may have different meanings in different contexts, but this research will utilise W3C's definition (https://www.w3.org):

"User models are used to generate or adapt user interfaces at runtime, to address particular user needs and preferences. User models are also known as user profiles, personas, or archetypes. They can be used by designers and developers for personalisation purposes and to increase the usability and accessibility of products and services.".

In the context of smart homes, user modelling helps to provide personalised user interface adaptations which are both usable and effective. This requires adequate representation of knowledge regarding the user and the smart home context where this section focuses on the modelling of the user. To further understand user modelling, the rest of this section explores the six categories of user models related to ubiquitous computing displays summarised by Kuflik et al. (2012).

Feature-Based and Content-Based User Modelling: This refers to user models that have a set of feature value-pairs (Brusilovsky, 1996). A model may have any number of feature-value pairs that can represent user preferences, capabilities and other factors that may characterise the user. Content-based modelling, which is a variation of feature-based modelling develops the model based on the type of content that the user consumes (Hanani, Shapira and Shoval, 2001). In the space of smart homes, feature-based user modelling may represent user's privacy preferences, user interface preferences and capabilities as value-pairs where at run-time the model can be used by the framework to understand user characteristics. The content-based modelling aspect will allow the learning of the user's preference depending on the content they use via the smart home.

Case-based user modelling: This approach captures information with regard to a specific case/scenario and model the user's behaviour depending on that information (Aamodt and Plaza, 1994). These models learn depending on the user's experience and will help automate actions for similar cases in the future. Regarding interpersonal privacy violation cases, this modelling technique would capture the user's behaviour with regard to different privacy cases and use that information in the future to automate the user interaction.

Collaborative User Modelling: This approach is based on the assumption that users who have similar preferences will continue to have similar preferences in the future (Goldberg *et al.*, 1992). In a smart home setting, this approach may help to populate the user preference information of a user whose current preferences are not modelled. This method will help to understand the unknown user's preferences by collaboratively evaluating the available preference information of the other users.

Demographic User Modelling: Commonly used in marketing, this method categorises the users on their demography and identify certain preferences related to that category. Then it will apply the identified user preferences with the demography cluster, which will be used to understand users in the future. This can be used in a smart home scenario where a child's preferences can belong to a certain category and an adult's preferences can belong to another category. Therefore, it will help to model users in a high-level manner. Furthermore, this idea is closely related to modelling user preferences based on the role of a user where it would model role-based user information to define role-based access control rules.

Knowledge-based User Modelling: This type of modelling uses the help of experts to model the users depending on the product or the service that they are going to use. These kinds of mechanisms can only be used if there is an already existing body of knowledge or experts in that domain. In a smart home scenario, this would mean getting the help of experts on privacy or smart homes to support the modelling of users.

Hybrid User Modelling: As the word suggests, in this model multiple methods are combined to get the best type of model while eliminating the trade-offs of each user modelling mechanism. In a smart home scenario, it can be beneficial to have a hybrid user model as that would create a more comprehensive model with fewer limitations. But this could mean more time is spent on combining user models

Considering Kuflik et al.'s (2012) six categories, I decided to utilise a hybrid user modelling approach, because none of the methods individually are able to fulfil the requirement of user modelling related interpersonal privacy violations. The user model for privacy-aware smart home interfaces needs to represent granular information regarding user's preference and capabilities to generate accurate adaptations. This information also had to be easily understood by the humans and the system (machine). Therefore, this requirement was better fulfilled by feature-based model where user information can be represented in a structured manner. Apart from that interpersonal privacy violating scenarios are quite nuanced in nature and had to be considered case by case. Therefore, utilising a case-based modelling technique helped to capture this nuanced user information.

Evaluating the knowledge representation requirements based on the example scenarios, I decided to focus on three main types of user model features. These were user's user interface preference, user's capabilities, and user's privacy preferences. In the literature, the user interface preferences and capabilities were provided in aggregation with a single user model where privacy preference modelling was not part of these models. Therefore, the rest of this section will first review the user's user interface preference modelling and capability modelling (§2.2.3.1) and then will review the privacy modelling techniques (§2.2.3.2).

2.2.3.1 User Interface Preference and User Capability Modelling

Adequate representation of user's user interface preferences and the capabilities are needed by the framework to generate usable user interface adaptations. To critically evaluate the literature to identify a suitable model, I developed a set of evaluation criteria. These criteria were based on the user's user interface preference and the capabilities that emerged from the example scenarios and the functional requirements of the proposed framework. The section below presents and justifies these criteria and Table 2.3 provides a summary of the criteria and the scores that were used for the evaluation.

2.2.3.1.1 Criteria

Human Readability: This criterion evaluated the readability of the model by a human. Human readability is a useful feature at the early stage of framework development but as the framework evolves this would have less significant importance. This is because the modelling will be

abstracted to a high-level input mechanism where a general user can define their personal preferences and capabilities.

Machine Readability: This criterion evaluated if the user model can be read easily consumed by the framework. This is quite important for easier integration with the rest of the framework components and to algorithmically reason with the user model knowledge.

User Interface Feature Representation: This evaluated if the user model can represent detailed user interface preferences. This is needed when generating a user interface adaptation that is preferred by the user.

User Capability Representation: This refers to the model's ability to represent the user's different capabilities. These could be the user's physical capabilities (motor, speech, vision, and hearing) and the user's cognitive capabilities. This supports the generation of user interface adaptations that is usable by the user.

Implementation Details: This evaluated if the model provided implementation details in a way that can be easily integrated to existing software systems.

Support / Criteria	Minimal or no support (○)	Partial support (◗)	Full support (●)
Human readability	Low readability	Average readability	High readability
Machine readability	Inability to parse through machines	-	Ability to parse through machines
User Interface Feature Representation	Not provided	Partial support	Comprehensive support
User Capability Representation	Not provided	Partial support	Comprehensive support
Implementation Details	Not provided	Partial support	Comprehensive support

Table 2.3: User Interface Preference and User Capability Modelling Evaluation Criteria

2.2.3.1.2 Review

The rest of this section provides the analysis of the user modelling techniques based on the criteria provided in Table 2.3.

A **Persona-based user model** was developed by Casas et al. (2008) to represent the preferences and capabilities of older adults and disabled people. The model was human-readable, but it was not machine-readable. The authors have partially provided means to represent user features such as cognition level, sensorial and physical disabilities. But the model is not comprehensive enough to cover different variations of user capabilities and it did not represent user's preferences regarding user interfaces. Even though the model lacks some key features, it highlighted the importance of providing means to define granular level details of the user capability features and user's cognition abilities regarding the system. In addition, the model also did not provide comprehensive details regarding the implementation. Overall, this was not an adequate model for the requirements of a privacy-aware smart home interface framework.

An **Ontology-based user model** was provided by Skillen et al. (2014) to personalise on-demand services in pervasive environments. The model was human-readable and machine-readable where it represented user interface preferences and the capabilities (physical and cognitive) of the user. The user interface preferences modelling allowed a user to define preference regarding a modality or a feature of a modality and it allowed the pairing of specific tasks when defining these preferences. One of the drawbacks of this model was that it didn't provide means to define devices as a preference or to order multiple preferences. It also didn't provide enough granularity to define modality features details where it only provided three high-level choices. These are important features when selecting an appropriate user interface adaptation with the available smart home devices. Therefore, the model needs to be adjusted to fit the knowledge representation requirements. The authors also provided implementation details including a software architecture a rule engine making it easier to integrate into existing systems.

VUMS (Virtual User Modelling and Simulation Standardisation) cluster (Kaklanis et al., 2016) aggregated user models in the ubiquitous computing space to develop a comprehensive and standard user model. VUMS cluster provided human-readable and machine-readable (VUMS exchange format) user models which represented user interface preferences and user capabilities (physical abilities, perceptual abilities, cognitive abilities, and motor abilities) with high granularity, but it did not provide mechanisms for how to define device preferences and to sort the order of preferences. VUMS cluster also defined converters to map models which were written using VUMS exchange language to project-specific models. This provided easier integration to existing implementations.

Table 2.4 provides a summary of the analysis and the rest presents the user models that were considered.

User Model	Human readability	Machine readability	User Interface Feature Representation	User Capability Representation	Implementation Details
Persona based user model (Casas et al., 2008)	●	○	○	◗	◗
Ontology based user model (Skillen et al., 2014)	●	●	◗	●	●
VUMS cluster (Kaklanis et al., 2016)	●	●	◗	●	●

Table 2.4: Summary of the Evaluation of User Modelling Techniques

2.2.3.1.3 Discussion

VUMS cluster (Kaklanis et al., 2016) and the ontology-based user model (Skillen *et al.*, 2014) provided adequate support for representing smart home user's user interface preferences and capabilities, but they required modification to provide necessary granularity level regarding user model features and required a mechanism to prioritise user interface preferences to ensure effective run-time execution. Apart from upgrading the existing features of the model to fit the knowledge representation requirements, all three of the models lacked the capability to model user's privacy preferences. This was justifiable as none of the application of the models required a representation of privacy preferences. But in this research, modelling privacy preferences was critical for detecting privacy violations and generating privacy-aware user interfaces. Therefore, the following section looks at different privacy preference authoring languages to identify a suitable mechanism for modelling user's privacy preferences.

2.2.3.2 Privacy Preference Authoring Languages

A critical part of user modelling is representing the user's privacy preferences. Accurate representation of privacy preferences helps the user interface framework to evaluate privacy violations at run-time and to generate privacy-preserving user interface adaptations.

Generally, privacy authoring languages are being used to define a user's privacy preferences so a reasoning engine can use these rules to evaluate the privacy status of a given context. Privacy preferences in the example scenarios and the functional requirements of the framework helped to generate the evaluation criteria for the privacy authoring languages. These criteria supported the critical evaluation of the languages to identify a suitable language for the privacy preference representation requirements of the proposed framework. The section below presents and justifies

these criteria and Table 2.5 provides a summary of the criteria with different levels of the evaluation.

2.2.3.2.1 Criteria

Human readability: This evaluates the ease of readability of a privacy rule by a human. This is important in the initial versions of the framework where users can easily define their privacy preferences. But this would have a minor impact as the framework develops because the privacy authoring would be abstracted to a high-level interface allowing a general smart home user to easily define their privacy preferences.

Machine readability: This refers to the privacy rule's ease of understanding for a reasoning engine. It is important for the privacy rule to be easily understood by the framework's reasoning component so it can evaluate the privacy status of the smart home for a given context.

Applicability: This evaluates if the language has been used in the domain of smart homes. This would provide an early indication of the suitability of the language for modelling smart home user's privacy preferences.

Implementation: This checked if there were example implementations of the language, ideally in the smart home domain. An implementation or a framework that can support implementations may reduce the time taken to integrate the privacy rule modelling feature into the proposed user interface framework.

Access-control: This criterion evaluated if the language had the means to support access control. Since the interpersonal privacy can be modelled as an access control problem to sensitive information or the user's bodily sensors, the privacy authoring language should possess access control features.

Conflict resolution: This evaluated the conflict-resolution features of the language. As smart homes are shared by multiple users with varying privacy preferences, conflicts are meant to arise. Therefore, the language should have the capability to handle these types of conflicts.

2.2.3.2.2 Review

The rest of this section provides the analysis of the privacy authoring language based on the criteria provided in Table 2.5. A general description of selected languages and worked examples are provided in Appendix B (§10.2).

Support / Criteria	Minimal or no support (○)	Partial support (◗)	Full support (●)
Human readability	Low readability	Average readability	High readability
Machine readability	Inability to parse	-	Ability to parse
Applicability	Inability to apply	Partially ability to apply	Full ability to apply
Implementation	No implementation details	Partial implementation details	Full implementation details
Access control	Not provided	Partially provided	Comprehensive access control provided
Conflict resolution	Not provided	Partially provided	Comprehensive conflict resolution mechanism provided

Table 2.5: Privacy Authoring Language Evaluation Criteria

P3P (Reagle and Cranor, 1999) (Appendix B: §10.2.10) was created by the W3C to facilitate data requests and privacy practices of service providers with intention of creating transparent data processing of web services. P3P proposals are machine-readable and partially human-readable at it uses XML and RDF based syntax to write the privacy proposals. P3P provides implementation details but it is not applicable in a smart home setting as the purpose of P3P was to support web-based interactions. P3P provides partial support for access control but it is not flexible enough to manage mismatches in the policies of the user and the service provider. P3P was one of the first privacy policy authoring languages which inspired many of the other languages that followed.

Ponder (Damianou *et al.*, 2001) (Appendix B: §10.2.11) is a policy language created for access control in the management and security of complex distributed systems. Ponder is human-readable as well as machine-readable. It provides a comprehensive role-based access control mechanism with four types of access control policies: authorisation policies, delegation policies, information filtering policies and refrain policies. These four controls provide flexibility when defining smart home user's privacy preferences by writing access enabling and access restricting policies. It also provides a mechanism that supports conflict resolution among different policies. The authors have provided implementation details of Ponder with worked examples making it easier to integrate to an existing system. From a technical standpoint, Ponder is one of the languages which qualified as suitable for specifying the privacy preferences of smart home users.

Rei (Kagal, 2002) (Appendix B: §10.2.12) is a general-purpose policy language that uses first-order logic; created to make policy authoring simple and universally applicable. Rei is human-readable as well as machine readable and supports access control. Rei allows writing policies to allow or restrict access to resources and it allows defining new constraints making it quite flexible when defining privacy preferences of smart home users. Furthermore, it provides conflict resolution by prioritising certain rules over others and setting precedence for certain modalities over others, but this requires further improvement as there can be scenarios where the rule-setter has not defined priority or precedence before the run-time. Rei also provides detailed implementation and a policy engine that uses Prolog (https://www.swi-prolog.org/) and RDFS (https://www.w3.org/TR/rdf-schema/) to evaluate policies. The Rei policy engine is quite robust as it enforces the rule engine to output a result (negative or positive) avoiding scenarios without a decision. Rei's ease of use, flexibility and extensibility made it is one of the most preferred choices for modelling user privacy preferences required for the framework.

XACML (Extensible Access Control Mark-up Language) (OASIS, 2013) (Appendix B: §10.2.13) is an attribute-based access control (ABAC) policy language where its main goal was to have a shared terminology and interoperability between access control implementations (in this section, I would be using XACML to refer to XACML 3.0 unless specified otherwise). XACML also can be used to implement role-based access control protocols as a specialised case of ABAC. XACML is machine-readable and to a certain extent, it is human readable. Since XACML can represent RBAC policies, XACML can be used for smart home privacy preference modelling with minor changes. XPACML (Bekara, Mustapha and Laurent, 2010) is an example of XACML used in authoring privacy policies. XACML also provides the option to combine rules using the "rule combining algorithm" and the option to combine policies using the "policy combining algorithms". These algorithms are quite useful when it is needed to aggregate rules or policies as well as to resolve conflicts between rules or policies. XACML provides detailed model specification, distributed architecture, and implementation details. One of the drawbacks of XACML is the complexity of the language as it was developed for large complex systems with changing policies. Apart from the complexity, XACML is a good candidate for modelling privacy preference modelling within the smart home domain.

Other privacy preference authoring languages

The rest of this section briefly looks at some other privacy authoring languages which are quite valuable in the privacy authoring domain but do not necessarily fit the requirements of a privacy-aware smart home interface framework.

E-P3P (Ashley *et al.*, 2002) supported the authoring of enterprises' internal privacy policies regarding collected user data. It uses XML based syntax that is machine-readable and partially human readable. It mimics an access control mechanism and provides the infrastructure to evaluate

the privacy policies against user request and implementation details. It also provides the flexibility to define new constraints allowing the language to be scalable. On the other hand, it does not provide a conflict resolution mechanism and it is not directly applicable in a smart home setting.

EPAL (Ashley *et al.*, 2003) is an IBM project which provides automated information flow control between enterprise IT applications and systems. EPAL uses an XML-based syntax, hence it is machine-readable and partially human-readable. It provides a comprehensive access control policy for data elements which can be written as positive rules (to allow) or as negative rules (to restrict). These policies use a hierarchical data model to define data categories, user categories, the purpose of the usage, action sets that can be enacted upon the collected data, conditions, and obligations. Apart from that, EPAL provides partial support for conflict resolution between rules but needs further improvements to fully manage different types of run-time policy conflicts. It provides detailed syntax guidelines and example implementation, but it is not directly applicable in the smart home domain since the focus has been on data management between complex enterprise systems.

XPref (Agrawal *et al.*, 2005) is a privacy preference authoring language developed to be used with P3P using and it uses Xpath expressions to write the policies. XPref addressed the drawbacks of its predecessor APPEL (W3C, 2002) by simplifying the rule authoring, allowing users to write preferences that they would accept, and reducing the erroneous nature of the policies. The XPref language is partially human readable, machine-readable and provides implementation details but it does not provide access control and it does not provide a conflict resolution mechanism. XPref focuses on web-based interaction in conjunction with P3P. Therefore, it cannot be directly applied to define privacy preferences within the smart home.

SecPAL (Dillaway, 2006) is a Microsoft project which focuses on policy authoring for complex distributed systems where it uses predicate based logic. It is machine-readable but contrary to their claim it is harder to read by a general user. It discusses conflict resolution to a certain extent but needed more detailed examples to further understand its capabilities. SecPAL provides worked examples of the policies but does not provide enough information regarding real-life integrations as its geared toward providing a more abstract policy framework. SecPAL has been extended to be used as a privacy preference authoring tool by SecPAL4P (Becker, Malkis and Bussard, 2009) but it is not been used in the smart home domain. Overall, SecPAL is a comprehensive policy authoring language, which technically qualifies to define privacy preferences of the smart home users, but it is more suitable for complex distributed systems.

The Air Policy language (Kagal, Hanson and Weitzner, 2008) is an MIT project which was developed to improve trust between the users and the system. It provides an explanation at reasoning-time using a method named *dependency tracking* which helps the users to understand the reasoning behind the system output regarding a policy evaluation. Air policy uses Turtle

(https://www.w3.org/TR/turtle/) to represent policies, which is a more human-readable version of RDF (https://www.w3.org/TR/rdf-schema/) and it is machine-readable. It allows access control, but it does not provide a mechanism for conflict resolution. Apart from that AIR provides an ontology and a reasoner for evaluating policies. The Air policy language is not used in the smart home space, but it is one of the first languages that highlighted the need for explaining the results of policy evaluations of a system. This motivates the need of incorporating explanations with privacy-aware user interface adaptations.

Jeeves (Yang, Yessenov and Solar-Lezama, 2012) focuses on writing privacy policies for managing information flows. Jeeves is said to be program independent where the authors have used Scala to implement examples of the policy. Symbolic representation of Jeeves makes it harder to be understood by a general user, but it is easier for a machine to read. Jeeves does not provide a conflict resolution mechanism and the real-world applicability and scalability have not been evaluated. Therefore, Jeeves is not suitable for the requirement of authoring privacy preference languages, but it motivates the need for separation of privacy preference reasoning from the core functionality of a system.

P2U (purpose-to use) (Iyilade and Vassileva, 2014) was inspired by P3P, where it focuses on authoring privacy policies for secondary usage of user data collected via web services. P2U uses XML based syntax which is machine-readable and partially human readable. A P2U policy consists of the purpose of data sharing, data retention time, and if the data can be sold. P2U provides a certain level of flexibility for users to negotiate policy details and the needs of the users. P2U is not applicable to be used within the smart home space and it has limited capability to handle policy conflicts.

Table 2.6 gives a summary of the analysis of the languages against these criteria.

2.2.3.2.3 Discussion

The languages evaluated above serve different purposes and have distinct features. For example, languages such as P3P, XPref and P2U addressed privacy policy authoring on the web, therefore, they were not considered to be suitable for smart homes. Languages such as Ponder, Rei, SecPAL and XACML focused on providing a general-purpose policy language. Out of these Ponder, SecPAL and XACML were more suitable for complex and distributed systems where Rei is more suitable for a simpler but extensible system. In addition, policy languages such as E-P3P and EPAL focus on supporting privacy policies within organisations and AIR focuses on improving the trust between the system and the user by providing explanations. For the requirement of defining privacy preferences of smart home users, languages such as Ponder, Rei, SecPAL XACML filled the functional requirement.

Out of these four languages, I decided to use Rei because it is simpler, much more human-readable compared to the other languages, machine-readable, supports easier integration to an existing framework with its Prolog implementation and the framework and provides an intuitive conflict resolution mechanism.

Language	Human readability	Machine readability	Applicability	Access Control	Implementation	Conflict resolution
P3P (Reagle and Cranor, 1999)	◗	●	○	○	○	○
Ponder (Damianou *et al.*, 2001)	●	●	●	●	●	●
E-P3P (Ashley *et al.*, 2002)	◗	●	○	●	●	○
Rei (Kagal, 2002)	●	●	●	●	●	●
XACML (Anderson *et al.*, 2003)	◗	●	●	●	●	●
EPAL (Ashley *et al.*, 2003)	◗	●	○	●	●	◗
XPref (Agrawal *et al.*, 2005)	◗	●	○	○	●	○
SecPAL (Dillaway, 2006)	◗	●	●	○	◗	◗
Air Policy (Kagal, Hanson and Weitzner, 2008)	●	●	○	○	●	○
Jeeves (Yang, Yessenov and Solar-Lezama, 2012)	○	●	○	○	●	○
P2U (Iyilade and Vassileva, 2014)	◗	●	○	○	◗	◗

Table 2.6: Summary of the Privacy Authoring Language Evaluation

2.3 Summary

This chapter reviewed the literature regarding privacy for smart home users. It highlighted that a majority of the existing research has focused on privacy violations that happen *outside* the smart home while limited research has been done on privacy violations that happen *within* the smart home. Further exploration highlighted how the shared nature of smart home devices caused privacy violations between smart home users. I have named this type of privacy as *interpersonal cyber-physical privacy* (§2.1.3.4) (for brevity: *interpersonal privacy)*. Since *interpersonal privacy* violations happen at the user interface layer, I hypothesise that *interpersonal privacy* can be

protected by adapting the user interface layer. This motivated the review of smart home user interface literature.

A review of the smart home user interfaces showed that it is a common practice in the field to use engineering frameworks to develop the user interface layer. It highlights those existing frameworks provided minimal or no support for *interpersonal privacy* protection, even though *interpersonal privacy* violations happen at the user interface layer. To address this gap, this research will develop an engineering framework that can generate privacy-aware adaptive user interfaces.

Based on the literature review and the example scenarios, I identified the core features required by a framework to generate privacy-aware adaptive user interfaces. After this step, I used MAPE-K loop (Kephart and Chess, 2003) as a reference framework to guide my literature review in identifying the required components for the framework. The MAPE (*monitor, analyse, plan, execute*) part of the adaptive system was explored by the review conduct earlier in this chapter as most of the adaptive frameworks used a similar base architecture. The K (*knowledge*) part of the adaptive system motivated the identification of suitable models to represent the knowledge required to characterise interpersonal privacy violating scenarios. Based on the criteria created, I reviewed the literature of 1) user interface preference models and 2) privacy preference models where I identified suitable models for knowledge representation requirements. I picked the MASP (Blumendorf, 2009) framework as a foundation for user interface framework, VUMS cluster (Kaklanis et al., 2016) as a foundation for user modelling and Rei for privacy preference modelling (Kagal, 2002).

The next chapter will formally establish the main research question, research sub-questions and the hypotheses to answer the research gaps identified in this chapter. It will also present and justify the research methods chosen to address the research questions.

3. Research Design

3.1 Introduction

The literature review presented in the previous chapter highlighted the current limits on the understanding of how to engineer systems that support the management of interpersonal privacy among smart home users. In particular, it identified a need for research regarding interpersonal privacy violations that arise when co-occupants share smart home devices and highlighted that interpersonal privacy violations happen at the user interface layer. The literature review also showed that the existing smart home user interface engineering frameworks provide minimal support for interpersonal privacy protection. The personal and contextual nature of individual privacy requirements means that it is not possible to design a static solution that can prevent potential privacy violations. Therefore, this research proposes an approach based on adapting the user interface layer to protect interpersonal privacy.

These considerations motivated the main research question:
How can smart home user interfaces be engineered to adapt their configuration and behaviour to preserve privacy between users in multi occupancy contexts?

This chapter describes how this overarching question was decomposed into a sequence of three research sub-questions that shaped the research.

1) **RQ1** (evaluation of the requirements modelling techniques): *How can we characterise the smart home environment adequately to drive privacy-aware user interface adaptations?*
2) **RQ2** (architecture and algorithm testing): *What is an appropriate software architecture for a privacy-aware adaptive smart home interface framework?*
3) **RQ3** (user experience evaluation): *What is the user experience of privacy-aware adaptive user interfaces?*

The research sub-questions collectively helped to answer the overarching research question. As the first step, the smart home system needs to understand the user's privacy preferences, user interface preferences, and the smart home context to generate effective privacy-aware user interface adaptations. Therefore, **RQ1** helped to identify and evaluate suitable models to represent these knowledge representation requirements of the adaptive system. As the second step, the smart home should be able to utilise the modelled knowledge from **RQ1**, and accurately detect possible privacy violations and generate appropriate user interface adaptations. This required the development and

systematic evaluation of a software architecture and a set of algorithms that can detect different types of privacy violations and execute user interfaces adaptations for different smart home contexts. Therefore, **RQ2** helped in developing and evaluating the adequacy of the architecture and the algorithms. Finally, the user experience of generated adaptive user interfaces needed to be evaluated, as privacy and the experience of user interfaces are specific to different users. Hence **RQ3** helped to evaluate the user experience of concrete implementations of privacy-aware user interfaces when applied in different interpersonal privacy violation scenarios. Furthermore, to support answering RQ1 and RQ2, and to understand the rich context needed to model interpersonal privacy violating scenarios, a set of example scenarios were developed.

After introducing the example scenarios, each sub-question is introduced in turn in the subsequent sections below. Each of these sections discusses the evidence that is required to address the relevant research sub-question, identifies, and justifies the method used to gather that evidence, and describes the tools, analysis techniques applied in the service of those methods. The overall structure of the research is summarised in Figure 3.1. The methodology sections are followed by a discussion of the reliability and validity of the research.

3.2 Example Scenarios

To explore the rich interpersonal privacy violating scenarios in depth, it was required to develop hypothetical scenarios that captured different dimensions of such scenarios. This was done by drawing examples from the literature and from the personas developed from the STRETCH project user interviews. STRETCH (Socio-Technical Resilience for Enhancing Targeted Community Healthcare) (https://stretch.dalmatianrex.co.uk/) was a research project focused on helping older adults live independently in their smart homes with the help of their 'circle of support'.

3.2.1 Background

Sally is a 76-year-old woman who lives alone in her own smart home. She has a circle of support (§Table 3.1) which is comprised of her adult son Zack and a caregiver Yasmin. Zack visits his mother regularly and sometimes he decides to stay with her for longer periods.

Name	**Role/Relationship with respect to Sally**
Yasmin	Caregiver
Zack	Son

Table 3.1: Sally's Circle of Support

Sally and Zack have their own privacy preferences (§Table 3.2). For example, Sally does not share her health details with anyone other than her caregiver as she feels that other smart home users such as Zack would become annoyed with her if her health is not optimal. Sally is also an avid meditator, and she has an expectation of not being disturbed when meditating. To avoid such situations, she has set appropriate privacy rules using the PASHI framework.

Zack sometimes stays with his mother for longer periods. Therefore, Zack also has set privacy rules using the PASHI framework. One of Zack's personal habits is that he likes to watch cartoons on Netflix, but he is embarrassed to let anyone know his viewing history. Sometimes Sally takes video calls to her relatives to which Zack will get invited to participate if he walks within the camera's view. Zack does not like to be disturbed during the weekend and has configured his privacy preferences to avoid being seen on Sally's calls.

Zack and Yasmin have specified their user interface preferences, as shown in Table 3.3 Yasmin has input modality and output modality preferences for the activity of accessing health data. Zack specifies device preferences where his most preferred user interface is the smart speaker, and when it is not available, he would prefer to use the Bluetooth headset to listen to music.

Name	Privacy preference(s)
Sally	Health data will only be shared with her caregiver.
	Does not want to get disturbed while meditating.
Zack	Does not share his preference to watch cartoons with anyone.
	Does not want to get disturbed by people outside the smart home on weekends.
Yasmin	-

Table 3.2: Privacy Preferences of the Smart Home Users

User	Task	User-interface preference(s)
Yasmin	Access Health Data	<u>Input Modality Preferences</u> 1. Voice without any masking features. 2. Text input with font size 12, font type Arial and font colour black. <u>Output Modality Preferences</u> 1. Voice with a female voice and 150 words per minute speed. 2. Visual with 80% brightness and resolution of 1920*1200 pixels. 3. Visual with 80% brightness and resolution of 220*170 pixels.
Zack	Listen to music	<u>Device Preferences</u> 1. Smart speaker 2. Bluetooth headset

3.2.2 Scenario 1: Health Information

One day Yasmin tries to access Sally's health data to treat her. Just as she is about to access Sally's blood glucose levels, Zack enters the room. The smart speaker pauses its broadcast of the low glucose level on the smart speaker and directs that output to Yasmin's smartwatch to support Sally's privacy preference.

3.2.3 Scenario 2: Meditation

On a specific day, Zack tries to play music loudly via the smart speaker without knowing that Sally is meditating. The smart home identifies this possible privacy violation and enforces the smart speaker to automatically play the music at a low volume. Then the smart home provides options on Zack's mobile phone to play music and also provides the reason for the user interface adaptation. The four options are 1) play music in a low volume, 2) play music on the Bluetooth headset, 3) play music later 4) play music anyway. Zack picks the option to play music via the Bluetooth headset.

3.2.4 Scenario 3: Netflix

One day Zack tries to watch Netflix on the smart TV. He goes through the movie suggestions where Netflix shows cartoon suggestions based on his viewing preferences. Suddenly Zack's mother enters the room, and the smart home switches the personalised movie suggestions to more generic movie suggestions by removing the cartoon suggestions.

3.2.5 Scenario 4: Skype call

Zack's mother is on a call with her sister during a weekend. Zack is home and he is taking the day off. Without knowing that his mother is on a call with her sister, Zack walks across the camera view. The smart home identifies Zack's privacy preference to not be disturbed by video calls during the weekends from people outside the smart home and masks him from the camera input. Without this intervention, Zack might have been invited to join the call, which would have disturbed him.

3.3 Identification and Evaluation of Requirements Modelling Techniques

One of the key aspects of an adaptive system is the adequate knowledge representation of the environment and its users to drive adaptations (IBM, 2006). Similarly, privacy-aware adaptive user interface generation required to have adequate knowledge of the smart home and its users. Achieving an appropriate, actionable characterisation of the smart home requires attention both to the requirements for such adaptation and to the problem in context. These include both the smart home environment and the users. Therefore, the research approach addressing **RQ1** (*How can we characterise the smart home environment adequately to drive privacy-aware user interface adaptations?)* had two parts:

1) ***Analysis*** of the literature and the example scenarios to identify the key inputs required for the adaptation (knowledge requirements) and reviewing the literature to identify models that would capture those requirements adequately.
2) ***Evaluation*** of the identified knowledge requirements and models to assess whether they would capture enough of the rich smart home context to make resultant adaptations effective. This step required finding evidence that the identified requirements and models successfully captured the rich details of the scenarios or not. If not successful, evidence of what was lacking.

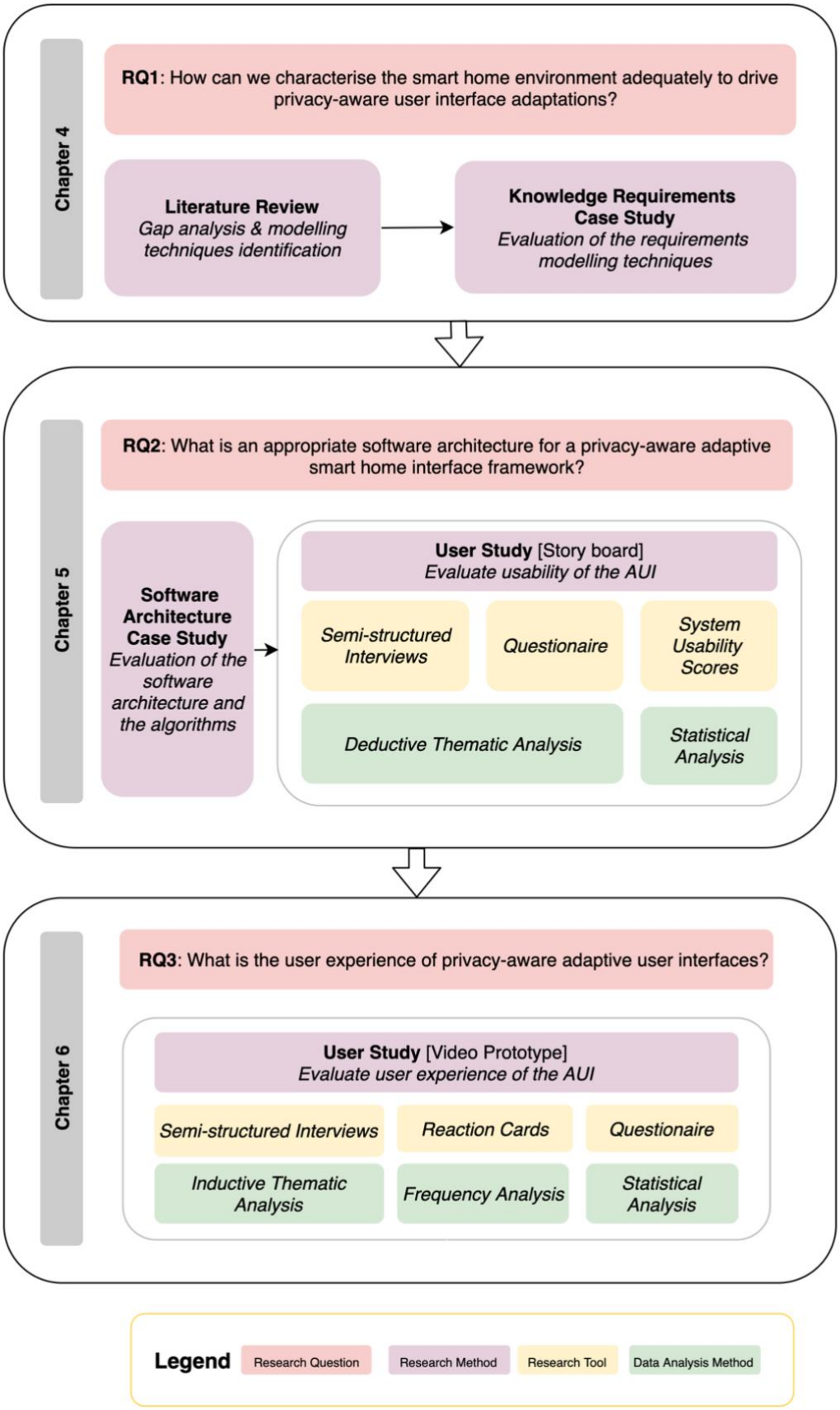

Figure 3.1: Research Methodology

3.3.1 Analysis: Model Identification

The example scenarios (§3.2) helped to highlight the core knowledge requirements needed to drive user interface adaptations. These knowledge requirements were:

1) user's privacy preferences,
2) user's user interface preferences,
3) features of the smart home user interface layer, and
4) the smart home context.

These knowledge requirements guided the literature review to identify appropriate models that could represent interpersonal privacy violation scenarios. It is common for researchers to use existing research and tools to develop certain aspects of their research. For example, Akiki (2014) took a similar approach which utilised existing models and frameworks to develop aspects of his adaptive user interface models. Using existing models with slight modifications instead of developing models 'from the ground up' helped to speed-up the research process and to improve the soundness of this research. After suitable models were identified from the literature, they were modified to better suit the example privacy-violating scenarios which were then evaluated for appropriateness. For example, VUMS cluster (Kaklanis et al., 2016) provided the means to capture user interface preferences as feature preferences (i.e., the preferred value for a given user interface modality). However, this was not sufficient for the requirement at hand. Therefore, this model was improved to integrate the following new features:

- smart home device preferences,
- prioritisation of preferences, and
- information related to contextual constraints in which the preferences are valid.

Similarly, other models were also adapted to meet the requirement of modelling the context of interpersonal privacy violation scenarios.

Identifying and addressing limitations

Sourcing models from the literature is inherently limited by the models that have been published. Three steps were taken to mitigate this:

1) The search criteria, based on the example scenarios to identify suitable models, helped to compare the capabilities among the existing models and identify the most suitable model for the knowledge representation requirement.
2) The selected models were then modified to better fit the knowledge representation requirements.
3) Finally, the selected models' applicability was evaluated with the support of a case study that embodied four distinct interpersonal privacy violating scenarios. This is reported next.

3.3.2 Evaluation of the Models: Knowledge Requirements Case Study

Addressing **RQ1** (*how can we characterise the smart home environment adequately to drive privacy-aware user interface adaptations?)* required evidence of whether the models sourced from the literature were able to capture the knowledge requirements in different contexts sufficiently and accurately – and in a way that the framework can consume. This required an evaluation approach that would give due attention to the fit between the models and different rich contexts; and reveal any gaps in the models. Therefore, this was evaluated using a constructed case study that embodied four different example scenarios. The example scenarios were chosen to represent key interpersonal privacy violations within a smart home context which were based on the literature review and the inspirations drawn from the STRETCH project. The scenarios were representative of two different types of interpersonal privacy violations (information interpersonal privacy and physical interpersonal privacy), and both input and output user interface modalities.

Broadly, a case study is an in-depth study of a specific instance, usually within a real-world context. According to Rogers, Sharp and Preece (2011), case studies can be used for four main reasons:
1) to *explore* new problems or scenarios,
2) to *explain* certain models that were created to understand certain situations,
3) to *describe* a scenario in detail, and
4) to *demonstrate* the applicability of a new tool.

In software engineering research, case studies are used as a method of inquiry addressing real contexts. For example, using a case study approach to understand the motivation of software engineers in a research and development organisation (França, de Araújo and da Silva, 2013), or as in this case –to provide a basis for systematic analysis of a framework. It is important to highlight the distinction between a constructed case study as used in this evaluation and a traditional case study that is used to observe specific instances in real-world contexts. This was also discussed by Easterbrook et al. (2008), who stated that case studies based on worked examples are an appropriate research method in software engineering to conduct systematic evaluations of frameworks; he also highlighted the confusion it may cause to researchers who use case studies in a traditional sense of contextual inquiry. A similar method (constructed case study approach) has been used by previous research in the space of adaptive user interfaces to demonstrate the capabilities of the knowledge representation models. For example, Blumendorf (2009) and Akiki (2014) used case studies to demonstrate the applicability of their adaptive user interface models.

The constructed case study was designed to include multiple scenarios to provide variation across the dimensions of privacy preferences, user interface preferences, type of privacy violated, device

capabilities and context information. The use of a case study was intended to evaluate the flexibility and the applicability of the models with an appropriate level of scenario coverage and correctness needed for the framework (i.e., the fourth of Rogers, Sharp and Preece's objectives). However, such variations are nuanced and hence are difficult to evaluate systematically in detail, and so pragmatically the method aspires to provide a representative, rather than comprehensive, coverage of possible scenarios.

The evaluation used Unified Modelling Language (UML) (Booch, 2005) to present meta-models, allowing standardisation and ease of future use. These models were then evaluated in terms of the case study; each model was used to represent the knowledge requirements (users' user interface preferences and privacy preferences) of the four example scenarios. Finally, the evaluation used concurrent task trees (Paternò, Mancini and Meniconi, 1997) to model the interactions of the four scenarios in a way that allows run-time adaptations. This allowed a principled evaluation of the user interface models for suitability in this context and to identify any gaps.

Identifying and addressing limitations:

In this context, the case study is primarily an analytical tool, and so any limitations in the case study may result in limitations in the evaluation. The four example scenarios used for the analysis were artificially constructed by a single researcher and may therefore be susceptible to researcher biases and may be limited in generalisability to real-world contexts.

To minimise researcher bias during the case development, the cases were developed carefully to be representative of the rich smart home context, situated in the literature and the user requirements of the STRETCH project. The cases were validated by senior researchers for representativeness and accuracy. The same validation was carried out for the worked examples to ensure accuracy.

As discussed previously, this case study is arguably representative, rather than comprehensive, providing sufficient evidence to compare models and assess which are sufficient to characterise smart home context for the purpose of privacy-aware user interface adaptations (or, more accurately, to assess which are insufficient). Therefore, after evaluating the appropriateness of the models for knowledge representation, they were used to support the privacy-aware user interface adaptions. This process was carried out by the software architecture and the algorithms developed under **RQ2** which will be discussed next.

3.4 Evaluation of the Software Architecture and the Algorithms

Based on the functional requirements elicited from the literature review and example scenario analysis, a software architecture and a set of algorithms were developed that can generate privacy-aware adaptive user interfaces. The next step was to evaluate the proposed architecture and the algorithms, i.e., to address **RQ2** (*"What is an appropriate software architecture for a privacy-aware adaptive smart home interface framework?*). The assessment was addressed from two perspectives: satisfaction of requirements evaluation and usability evaluation, which are discussed in the sections that follow.

3.4.1 Satisfaction of Requirements: Software Architecture Case Study

The evaluation of the ability of the proposed architecture and algorithms to generate privacy-aware user interface adaptations led to the evaluation of the two core processes supported by the proposed architecture:

a) interpersonal privacy-violation detection, and
b) user interface adaptation generation to address those detected violations.

The evaluation of requirements satisfaction required evidence of whether the proposed architecture and algorithms supported the aforementioned core processes successfully, or, if not, evidence of what was lacking. This required a method that can assess the architecture and the algorithms' capabilities in depth. Therefore, similar to the approach for **RQ1**, a constructed case study was used due to the nuance and rich nature of interpersonal privacy violation scenarios.

Although the case study permitted in-depth analysis of capabilities, it did not demonstrate the applicability of the model for every possible scenario; rather it provided sufficient evidence of the ability of the architecture and the algorithms to represent privacy-aware adaptive user interface generation. A case study approach has been used by other research which looked to evaluate software architecture's ability to generate adaptive user interfaces. For example, Blumendorf (2009) used a case study to evaluate the MASP framework's software architecture, and Schaub (2014) used a case study to evaluate his dynamic privacy adaptation system.

Analysis of the case study included standardised representation to support comparison and algorithmic analysis. Unified Modelling Language (UML) (Booch, 2005) was used to represent the core processes. The use of UML provided the required standardisation and ease of future use. The case study demonstrated the applicability of the software architecture for each of the core processes

by representing their behaviour via activity diagrams. The algorithmic analysis using the case study also demonstrated efficacy, efficiency, and the scalability of each algorithm via algorithmic analysis, which was critical for adapting the user interface layer at run-time. Algorithmic analysis also investigated how well the algorithms performed when the number of smart home entities increased. Further details of the methodology are provided in Chapter 5.

Identifying and addressing limitations:
Similar to the previous case study (§3.3.2), the same potential limitations and biases were addressed using a similar approach. One of the additions in this case study was the algorithmic analysis, which introduced a standard evaluation within the case study to assess the scalability of the privacy detection process and the user interface adaptation process, which together demonstrated a certain level of external validity. To further evaluate the adequacy of the framework, the next step presents the usability evaluation conducted on the generated user interface adaptations.

3.4.2 Usability Evaluation: Storyboard Study

Generally, adaptive user interfaces tend to receive mixed reactions with regard to their usability. Duarte (2007) highlighted that adaptive user interfaces might have negative user responses due to users having inconsistent mental models. However, Duarte also suggested that adaptive user interfaces could have high usability due to personalisation and its task-oriented nature. Therefore, it was critical to evaluate how users perceived the usability of different adaptive user interfaces generated by the proposed framework as part of evaluating the adequacy of the framework.

This required user responses regarding the usability of different adaptive user interfaces when applied in mitigating different interpersonal privacy violating scenarios. To generate the necessary evaluation of the usability of different adaptive user interfaces generated by the proposed framework, a storyboard-based usability study (Appendix A: §10.1.1 & §10.1.2) was conducted. The study evaluated three variations of privacy-aware user interface adaptations applied to two variations of interpersonal privacy violations.

Storyboards were selected as the stimuli as they provided means to gather user responses quickly; at the same time, they presented sufficient conceptual details for users to provide further feedback to improve the framework. Even though storyboards were far from a concrete implementation, they provided answers which are consistent with real prototype-based user studies (Rogers, Sharp and Preece, 2011); hence a storyboard-based study was sufficient and suitable to generate accurate user responses to evaluate the usability.

During the study, both qualitative and quantitative data were collected as means of improving the richness and accuracy of the evaluation (Figure 3.1). The system usability scale (SUS) (Appendix A: §10.1.5) was used to gather quantitative data regarding usability; this permitted a quantitative comparison of the different adaptive user interface configurations using descriptive statistical analysis. Using system usability scales alongside statistical analysis is common in HCI research to compare different variations of user interfaces. A similar approach has been used to compare novel text input variations for smart TVs (Choi and Li, 2016). Qualitative data was collected via semi-structured interviews (Appendix A: §10.1.3) and questionaries. During the study, the participants were encouraged to "think aloud" (Lewis, 1982), to allow further insight into their reasoning for SUS ratings and questionnaire answers.

Interview transcripts and questionnaire answers were analysed using deductive thematic analysis (Fereday and Muir-Cochrane, 2016). Nielsen's heuristics (2005) were used as the base themes for the analysis because it was a commonly used approach for usability evaluation in product design. The use of deductive thematic analysis (rather than inductive analysis) helped to evaluate adaptive user interfaces against the standard usability heuristics. In-depth details of this method are provided in Chapter 5.

Identifying and addressing limitations:

The usability study was developed and executed with attention to possible biases and limitations. Similar to previous steps (§3.3.2, §3.4.1), example scenario development was susceptible to researcher biases and had limitations regarding external validity. Therefore, they were developed paying attention to the literature and the STRETCH project to ensure that they are sufficiently representative of the different variations of interpersonal privacy violations, the adaptive user interface variations, and the smart home contexts.

Another limitation was the potential effect of the abstract nature of the storyboards on the internal validity of the study by admitting different interpretations by different users. This limitation was an acceptable compromise at this stage of the research, as the storyboards were chosen with the intent to elicit appropriate user responses to evaluate the usability of adaptive user interfaces – and at the same time to prompt participants to provide further feedback on how to improve the adaptive user interfaces and to identify more interpersonal privacy violating scenarios from their daily lives. To further address possible biases and limitations, multiple steps were taken. As some of these steps are shared with the user experience evaluation study (§3.5), they will be discussed together later in this chapter (§3.6).

3.5 Evaluation of the User Experience: Video-Prototype Study

Findings of the storyboard study helped to investigate whether the proposed architecture and the algorithms managed to generate usable and effective adaptations; how users perceived the usability of different variations of adaptive user interfaces; and what to prototype. But the storyboard study was more conceptual and only investigated a limited number of scenarios. Therefore, more evidence regarding the user experience of multiple situated implementations of adaptive user interfaces was needed to fully understand how users perceived adaptive user interfaces and the applicability of the framework to different scenarios. Furthermore, these implementations needed to be representative of adaptive user interface variations, different user interface modalities and interpersonal privacy variations.

Answering **RQ3 (***what is the user experience of privacy-aware adaptive user interfaces?*) required evidence regarding the user experience of concrete implementations of different privacy-aware user interface adaptations. This required a research method that could generate rich user responses to different implementations of adaptive user interfaces. Therefore, a lab-based user study was planned – however, during this time the COVID-19 pandemic started, and the face-to-face lab-based study had to be cancelled. Considering both the requirement of generating rich user responses to concrete implementations and the impact of COVID-19 restrictions, I decided to use a video-prototype based user experience evaluation study.

Video prototypes are a type of prototypes used to evaluate interactive systems using a video recording of the interaction or part of the interaction (Mackay, 1988). Video prototypes are richer than storyboards in terms of the level of detail of the interaction but poorer than lab-based implementations. Video prototypes allow the researcher to demonstrate a comprehensive outlook of an interactive system in a quick and cheap manner compared to lab-based implementation, and a video prototype based user study provides user responses that are consistent with a lab-based user study (Bajracharya *et al.*, 2013). Apart from that, this method allowed the evaluation of more scenarios covering multiple interaction modalities and privacy violation types more rapidly compared to a lab-based user study and allowed recruiting a high number of participants due to its remote-friendliness. Even though the video prototype study was not planned at the beginning of the research, it was found to have the advantage of providing enough evidence to evaluate the external validity of the research findings, as multiple modalities, adaptation variants and interpersonal privacy variants could be tested with a higher number of participants. Therefore, when the COVID-19 pandemic struck, video prototypes were used for evaluating the user experience, as an alternate tool to a lab-based implementation of the adaptive user interface.

The video prototype study used the findings from the previous storyboard study to decide which variations of adaptive user interfaces to use in which variation of interpersonal privacy violations. When compared to the storyboard study, the video prototype study explored more types of user interface modalities, scenarios, and adaptive user interface variants, as it was more situated. Therefore, it provided an in-depth understanding of the user experience of concrete implementations of adaptive user interfaces when used in appropriate scenarios. The study also provided evidence to evaluate whether the proposed framework can support multiple modalities, user interface variations and scenarios providing external validity.

Similar to the previous study, this was also conducted as a mixed-method study in order to improve the accuracy of the findings via data triangulation. A card sorting technique (Microsoft product reaction cards) (Appendix A: §10.1.4) was used to capture user reactions to the adaptive user interfaces which was then followed by a questionnaire to further understand participant perception of adaptive user interfaces. Participants were also instructed to use the "think aloud" protocol (Lewis, 1982) when they were selecting reaction cards and answering questionnaires. This was done to further understand the reasoning behind their selections and answers. Furthermore, participants were also interviewed to understand their reasoning and were prompted to define types of user interface adaptations that they might not have liked. At the end of the study, a semi-structured interview (Appendix A: §10.1.3) was conducted to understand the overall perception of AUI and the user experience of AUI.

In the data analysis step, inductive thematic analysis (Fereday and Muir-Cochrane, 2016) was used to evaluate the qualitative data with the support of McCarthy and Wright's framework (2004). This allowed us to capture aspects of user experiences that might not have initially been hypothesised as it helped to evaluate user experience from multiple lenses. Frequency graphs were used to visualise reaction card picks and statistical analysis to understand quantitative answers to the questionnaire. As initially planned, frequency graph results and statical analysis triangulated the findings from the interview data. Further details of the methodology and the findings of the video prototype study are presented in Chapter 6.

Identification and addressing limitations:

Even though the video prototype study aimed to address some of the limitations of the storyboard study, it inevitably had its own limitations and potential biases.

Potential biases regarding example scenario development were addressed in a similar manner to the previous studies (§3.3.2, §3.4.1 and §3.4.2). The development of more rich and representative example cases was aided by the findings of the previous study, as participants commented on how to improve the adaptive user interfaces and where to use them appropriately. This study attempted

to improve generalisability (external validity) compared to the other three studies (§3.3.2, §3.4.1 and §3.4.2) by covering multiple variations of user interface adaptations, multiple modalities, different user preferences, and different smart home contexts. The number of participants was also higher (N=23) than the storyboard study (N=15), in an attempt to minimise random errors that may have arisen with a lower number of participants.

Biases that may arise due to the study methodology, execution and analysis were addressed in a similar manner to the previous user study (§3.4.2). One of the distinct and critical limitations regarding this study was the inability of the participants to interact physically with the adaptive user interfaces. This may have reduced the internal validity but taking a mixed-method approach helped to mitigate this through the triangulation of data.

3.6 Reliability and Validity

To evaluate the design of the research, it is important to consider the reliability and validity of the methods chosen. Reliability of the measures underpins the credibility of the findings where the validity of the measures underpins the generalisability. Reliability refers to the consistency of a measure and hence the repeatability of the findings; validity refers to the accuracy of a measure, and hence the likelihood that the findings are true. Attention was paid throughout the research to promote the reliability and validity of the research – and to identify and mitigate potential limitations and bias.

Key steps included:

- **Following good practices:** The research adopted several practices intended to expose and mitigate potential bias. These included:
    - Independent evaluation of the research design and protocol by senior researchers and by the Human Research Ethics Committee.
    - Pilot studies were conducted to ensure smooth and appropriate data collection. Then the collected data was evaluated to check if they were capable and adequate to answer the research questions.
    - Questionnaires used in the user studies were developed to be more open-ended prompting descriptive answers.
    - User studies were designed to avoid user fatigue by limiting the study duration to be less than an hour.
    - The study conditions were methodically ordered and allocated to address the learning effect to improve the validity of the findings.
    - Learnt how to conduct effective HCI related interviews and followed them during the study.

- Conducted the usability study in a quiet and comfortable meeting room and the user experience study in the comfort of the participant's homes to remove possible external disturbances.
- The user studies were conducted by a single experimenter to minimise inconsistencies in the study procedure and the biases that may arise due to multiple researchers conducting the same study.
- "Think-aloud" by participants was used to better understand participants' responses.
- The senior researchers evaluated the codes used to analyse the qualitative data and the generated themes to minimise possible researcher biases.
- Multiple data sources made it possible to cross-validate for the consistency of each pool of data collected, to assess the consistency of research findings from different data sources, and to provide opportunities to identify assumptions or potential biases.
- Used data triangulation along with statistical analysis to improve the internal validity of the findings.

- **Use of standard methods and tools:** Where appropriate, the research used standard methods whose reliability has been established in comparable contexts. For example:
  - The usability study used SUS (Appendix A: §10.1.5) as a means of quantifying the usability of different AUI variations.
  - In both the studies, open-ended questionnaires were used where they were developed to minimise bias and to maximise the opportunity to understand the phenomena.
  - The user experience evaluation study used structured questionnaires in conjunction with a Likert scale. The phrasing of the questions alternated between the negative and positive type of questions to prompt the users to actively think while answering the questions.
  - In both the studies, semi-structured interviews (Appendix A: §10.1.3) were conducted as a method of in-depth inquiry while following the best practices of user interviews.
  - Both the studies utilised card sorting tools (specifically Microsoft Reaction cards) (Appendix A: §10.1.4) which is a standard tool for quickly capturing user feedback in HCI research.
  - Standard methods were used for data analysis in both the user studies. The usability evaluation study used deductive thematic analysis in conjunction with Nielsen's heuristics (2005) and statistical analysis of the SUS scores; the user experience evaluation study used inductive thematic analysis in conjunction with McCarthy and Wright's User Experience framework (2004).

- **Selection of rich and representative scenarios:** Example scenarios were chosen carefully to represent key elements of privacy (and privacy violations) in the smart home context. These example scenarios were used for eliciting requirements, for evaluating the applicability of the models and the framework, and for evaluating the usability and the user experience of the adaptive user interfaces. The example scenarios chosen represented different privacy variations, user interface variations, privacy and user interface preferences, and different smart home contexts. This helped to improve the internal as well as external validity of the research findings.

Nevertheless, inevitably, the work has its limitations.

- **Applicability in real life:** Even though the scenarios generated were rich and representative of the different aspects of interpersonal privacy violating scenarios, they were artificially constructed. Hence, these limited the applicability of the findings in real life. This was minimised to a certain extent in the user studies as participants were asked their view of the suitability of the scenarios chosen and the applicability of the AUI for those scenarios. Nevertheless, further studies should be conducted to better understand the applicability of the AUI in real life contexts.

- **Generalisability:** Exhaustively covering all the interpersonal privacy violating scenarios and the variations of the AUI within a smart home is impractical due to the nuanced and rich nature of the context. Thus, the research didn't look to provide 100% generalisable findings but looked to provide adequate representation of the different privacy variations and the AUI variations. This means the scenarios chosen only provides a certain degree of generalisability. Generalisability was addressed to a certain degree in the second case study (§3.4.1) where algorithmic analysis was conducted to evaluate how the framework can be applied to other scenarios beyond the ones that were discussed. Apart from that, the user experience study tested out an increased number of different scenarios compared to prior studies. User experience study provided a greater range of variations in key dimensions of privacy violations, interaction modalities, smart home context, and user preferences. Hence, this study provided the most reliable evidence regarding AUIs applicability in managing interpersonal privacy.

3.7 Summary

This chapter has provided an overview of the research design, articulating the key research questions, and motivating the design decisions for the studies. As summarised in Figure 3.1, the chapter explained the relationships between the phases of the research and highlights how the

research design contrasted analytic work to assess the technical approach, and user studies to understand the proposals in the context of use. The next chapter presents and justifies the models selected for knowledge representation. The studies are reported in detail in Chapters 5 and 6.

4. Modelling Privacy-aware Smart Home User Interfaces

4.1 Introduction

The protection of interpersonal privacy that is required when using shared smart home devices has not been properly addressed in the literature (*Research Gap 1*). Since interpersonal privacy violations happen at the user interface layer, interpersonal privacy can be protected by adapting the user interface layer of the smart home. This notion of adapting the user interface layer motivated the review of the smart home user interface framework literature. This identified a gap in the smart home user interface framework literature, showing that there is a lack of support for interpersonal privacy protection in smart home user interface frameworks (*Research Gap 2*). To address both the aforementioned research gaps, I formulated **RQ0**: *"How can smart home user interfaces be engineered to adapt their configuration and behaviour to preserve privacy between users in multi occupancy contexts?"*

Addressing interpersonal privacy violations in smart homes requires a solution that can adapt to the context-specific privacy requirements and interface capabilities of the environment. To ensure such a solution is robust and capable of being deployed in different smart home contexts, it is important that it be developed by following a systematic engineering approach. Therefore, I decided to develop an engineering framework to generate privacy-aware adaptive user interfaces, building on the MAPE-K architecture pattern (Kephart and Chess, 2003) for adaptive systems design, MVC architecture pattern (Reenskaug, 1979) for interactive system design and the Cameleon reference framework (Calvary, Coutaz and Thevenin, 2001) for smart environment user interface design. This mirrors the approaches taken by Blumendorf (2009) and Akiki et al. (2015) who have also developed engineering frameworks to guide adaptive user interface generation in their respective research.

According to the MAPE-K loop (Kephart and Chess, 2003), knowledge representation is critical for the four functions of an adaptive system (i.e., monitor, analyse, plan and execute). The literature review and the examination of example scenarios identified three knowledge requirements for supporting privacy-aware smart home user interface adaptations: (1) user interface preferences to support usability and positive user experience; (2) privacy preferences to ensure users' privacy is

protected; and (3) user interface information to determine the optimal user interface configuration that can satisfy both privacy and interface preferences of the user.

This research gap is highlighted in **RQ1**: *How can we characterise the smart home environment adequately to drive privacy-aware user interface adaptations?*

The literature review identified suitable modelling mechanisms based on the knowledge representation requirements of the privacy-aware smart home interface framework (PASHI). This chapter describes how the modelling techniques can be adapted to represent the knowledge required to support the adaptive user interface capabilities of the PASHI framework. The capabilities of this knowledge representation are demonstrated through a case study.

To support the case study, the four scenarios presented in §3.2 will be used. These scenarios represent two variations of adaptations (switching the modality and adapting the features of a modality) and two variations of privacy violations (physical privacy violations and information privacy violations). These four scenarios will be used throughout this chapter as examples to model the knowledge required to support privacy-aware smart home user interface adaptations. First, the user interface preference model and it is applicability will be presented. Then the privacy preference model and its application will be presented. Finally, the smart home user interface model will be presented.

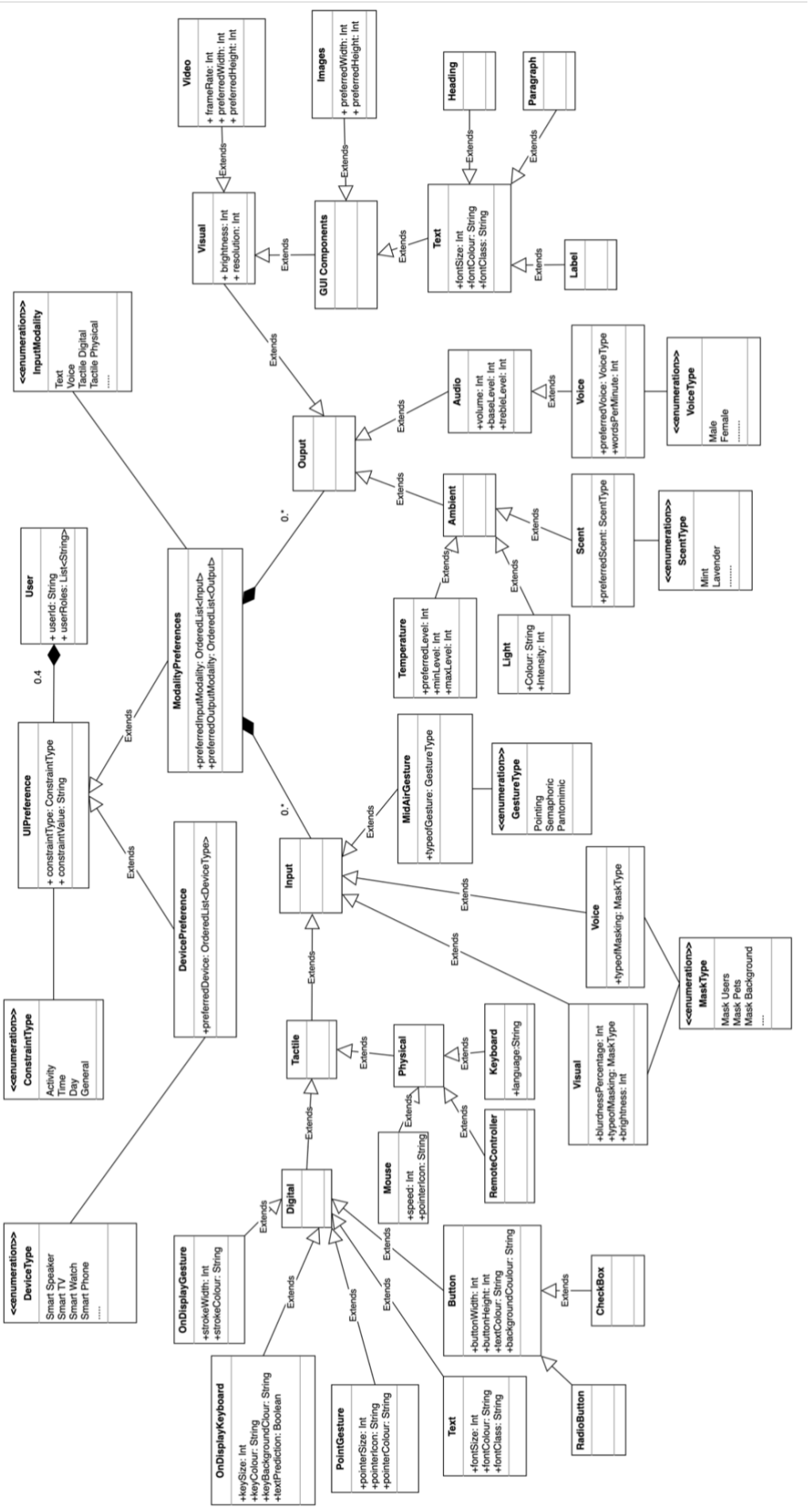

Figure 4.1: User Interface Preference Model

4.2 User Interface Preference Modelling

User interface preference modelling is one of the three components of the required knowledge representation of the PASHI framework. Modelling a user interface preference captures each user's partiality towards certain smart home devices or modality features. This knowledge enables the PASHI framework to generate user interface adaptations that are usable and liked by smart home users.

User interface modelling can be based on a preferred set of smart home devices or based on a preferred set of modality features. In Scenario 1 (§3.2.2), Yasmin has a list of user interface preferences (Table 3.3) based on the modality features when accessing health data. These preferences are divided into input modality and output modalities. Under each type of modality, Yasmin has an ordered list of modality features that she likes to use. Similarly, in Scenario 2 (§3.2.3), Zack has a list of smart home device preferences when listening to music. Zack likes to use the Bluetooth headset if the smart speaker is not available. Furthermore, the user interface preference model should allow users to define if these preferences apply all the time or if they would apply under certain constraints such as the current activity of the user, or a particular time and day.

Motivated by these knowledge representation requirements and inspired by research work such as MASP (Blumendorf, 2009) and VUMS cluster (Kaklanis et al., 2016), I developed the user preference model shown in Figure 4.1. This model supports the representation of the two variations of user interface preferences discussed above. Users can define their preferences for certain smart home devices or certain modality features. Each of these options has its strengths and weaknesses. Defining preferences based on the modality gives more flexibility regarding expressing user interface preference compared to the smart home device-based preferences. On the other hand, smart home device-based preferences allow users to quickly define their user interface preferences. Apart from that, this model enables the user to define when the user interface preference is applicable. The validity of the user interface preference can be constrained by the *activity* of the user, the *day* or the *time*. The user is also given the facility to apply the user preference for all the interactions by selecting the *general* constraint. The remainder of this section will show the applicability of the user interface preference model with some worked examples.

User preferences based on modality features

Yasmin's user interface preference (Table 3.3) is a modality-based preference that is constrained by the activity of *accessing health data*. Using the user interface preference model, Yasmin's user interface preferences can be represented as shown in Listing 4.1. Yasmin's preferences for input and output modalities are captured by ordered lists (*PreferredInputModality* and

prefferredOutputModality). Listing 4.1 only shows the model values which apply to this instance. The full implementation would contain a longer JSON object with empty values as Yasmin has not defined preferences for other types of modalities.

```
{
“ConstraintType”: “Activity”,
“ConstraintValue”: “Accessing Health Data”,
“ModalityPreference”:
      {
            “preferredInputModality”: [
            {
                  “Voice”: {
                        “typeOfMasking”: “None” }},
            {
                  “Text”: {
                        “fontSize”: 12,
                        “fontType”: “Arial”,
                        “fontColour”: “Black” }}
            ],
            “preferredOutputModality”: [
            {
                  “Voice”: {
                        “preferredVoice”: “Female”,
                        “wordsPerMinute”: 150 }},
            {
                  “Visual”: {
                        “brightness”: “80%”,
                        “resolution”: “1920*1200Px” }},
            {
                  “Visual”: {
                        “brightness”: “80%”,
                        “resolution”: “220*176Px” }}
            ]
}
}
```

Listing 4.1: JSON Representation of Yasmin’s UI Preference

User interface preferences based on smart home devices

Similar to Yasmin, Zack also has a user interface preference constrained by an activity (Table 3.3). In contrast to Yasmin’s modality-based user interface preference, Zack has a list of smart home devices that he likes to use. Zack prefers to use a Bluetooth speaker whenever the smart speaker is not available to listen to music. This is shown in Listing 4.2, in which his preference of smart home devices is represented by an ordered list named *preferredDevices.*

```
{
“ConstraintType”: “Activity”,
“ConstraintValue”: “Listening to Music”,
```

```
“DevicePreference”:
     {
          “preferredDevices”: [“Smart Speaker”,
                               “Bluetooth Headset”]
     }
}
```

Listing 4.2: JSON Representation Zack’s UI Preference

The user interface preference model shown in Figure 4.1 provides a flexible and efficient way to capture the smart home user’s interface preferences. This section showed how the user interface modelling being used by the PASHI framework provides a means to model both modality-based preferences (as illustrated in Listing 4.1) and smart home device-based preferences (as illustrated in Listing 4.2). It is important to note that the two instances provided, do not cover all types of user interfaces preferences accommodated by the model (Figure 4.1). Furthermore, the model can define a number of constraints required for user interface preference modelling and can be further extended to integrate novel features if the requirement arises. The next section discusses the privacy preference modelling aspect of the PASHI framework.

4.3 Privacy Preference Modelling

Another category of knowledge representation requirement for the PASHI framework is privacy preference modelling. Privacy preference modelling is required for the system to understand the user’s privacy requirements and consequently to adapt the user interface layer to preserve the user’s privacy. This requirement motivated the modelling of the user’s privacy preferences as part of the knowledge representation of the PASHI framework.

There are multiple components in modelling user privacy preferences. In Scenario 1 (§3.2.2**Error! Reference source not found.**), Sally’s privacy preference is to not share her health information with anyone other than her caregiver. Hence, this scenario highlights the need to model private information types when defining privacy preferences (information privacy) and the need to define role-based access control to private information. In Scenario 2 (§3.2.3**Error! Reference source not found.**), Sally’s privacy preference is to not be disturbed while she is meditating. This scenario motivates the need to model the current activity of Sally as a constraint and to control access to Sally’s auditory, visual, and tactile senses (physical privacy). In Scenario 4 (§3.2.5), Zack’s privacy preference is to not be disturbed by people outside his household during the weekends. This scenario highlights the need to have time-based constraints when modelling privacy preferences. Therefore, the privacy preference model should be able to define different types of privacy violations (information privacy and physical privacy) and to define access control rules based on constraints such as time, day, role, and activity.

PASHI adopts an approach inspired by the role-based access control (RBAC) (Ferraiolo, Kuhn and Chandramouli, 2003) mechanism for modelling privacy preference rules. RBAC allows the definition of rules on the roles rather than individuals. This provides flexibility over defining rules as well as changing rules when there are multiple people within a smart home. PASHI does not strictly adopt all the features provided by RBAC, such as hierarchical roles, as the roles within the smart home are typically flat in nature. On the other hand, the approach does allow adding multiple roles and grouping certain smart home users when writing privacy rules.

Whenever possible, roles are assigned to each smart home user depending on the relationships each has with each other. A smart home user's privacy is modelled as objects where access needs to be controlled. As mentioned in the literature review, the focus is on the physical privacy and information privacy aspect under IPCP-privacy. A smart home user's physical privacy can be protected by controlling access to the smart home users' senses where they can be accessed via different smart home devices. Therefore, defining privacy rules to control access to a user's senses would allow the user to control their physical privacy. Similarly, smart home users can protect their information privacy by controlling access to their different types of personal information. Both these types of privacy are considered to be the objects of access control.

Figure 4.2 shows how relationships are modelled among Yasmin (caregiver), Sally (care receiver and mother) and Zack (son).

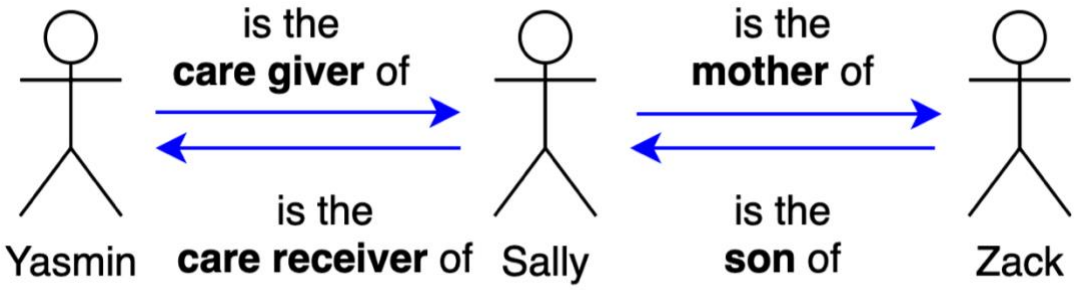

Figure 4.2: Relationship Mapping

Figure 4.3, represents each smart home user's privacy preferences, clearly separating the different aspects of a rule such as *agent, condition, effect, object* and the *owner* or the role. *Agent* refers to the entities which try to access a smart home user's personal information or senses. Personal information and senses are named as objects over which access must be controlled. *Condition* indicates the context in which the rules are applicable where effect denotes the rule's outcome when it is true.

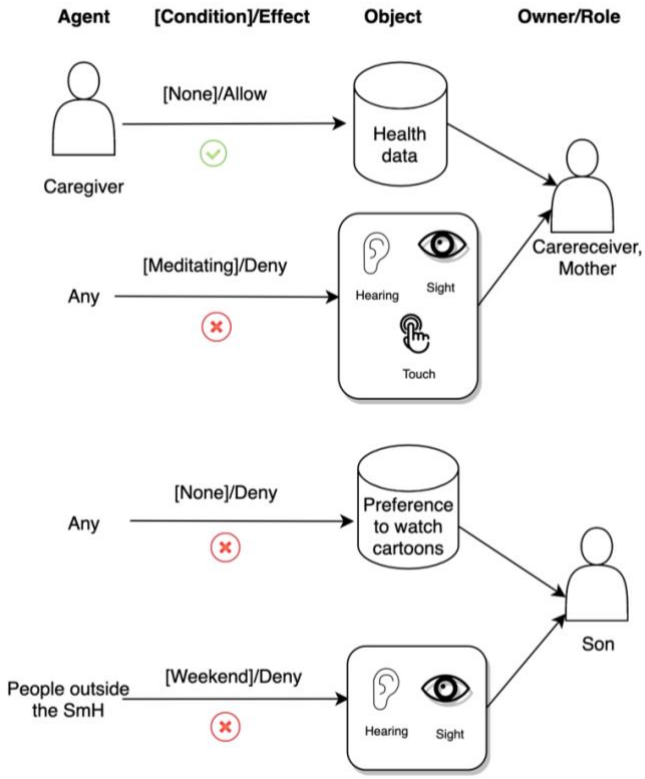

Figure 4.3: Privacy Rule Mapping Based on Roles

The following section discusses how privacy rules are represented in a machine and human-readable manner.

4.3.1 Privacy Preference Rules

PASHI adopts the Rei policy model (Kagal, 2002) to generate its own privacy preference rule model as depicted in Figure 4.4. The user class represents the user's capabilities, UI preferences, role, and privacy preferences. In contrast to the expanded version of the UI preference modelling provided in Figure 4.1, this section focuses on the privacy rule aspect of the user modelling. The user could have a rule set with an arbitrary number of rules. Modelled on Rei's policy rule, a PASHI privacy rule consists of all the aspects required to define a privacy rule. It represents personal information types and the user's senses as target objects of the rule, where its access can be regulated depending on the rule. Further, it defines different constraints required to specify the validity of a privacy rule to a particular context such as time, day, location, and activity as enumerations. The type of a privacy rule is also defined using enumeration, where the rule setter can make it a positive (allow) rule or a negative (deny) rule.

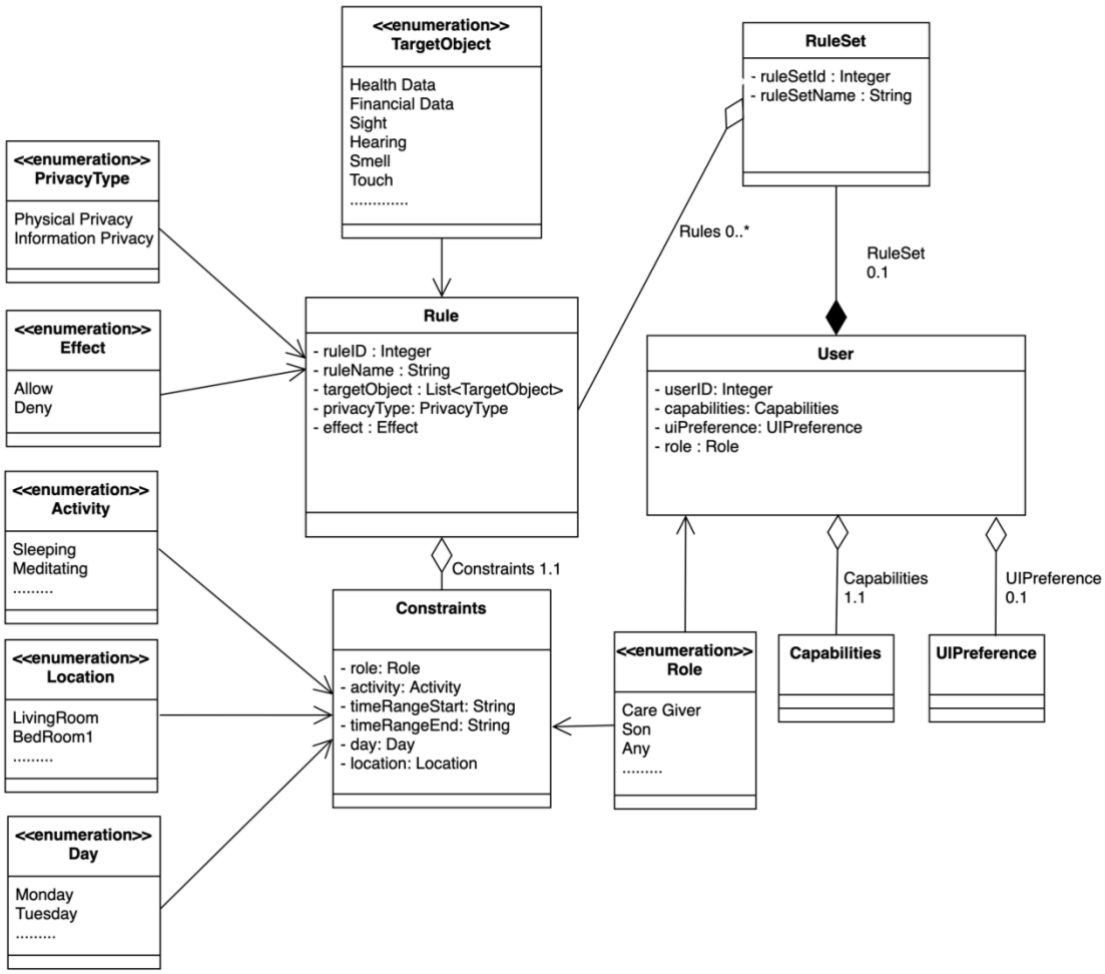

Figure 4.4: Privacy Preference Rule Model

```
{
“userID”: 1,
“ruleName”: “Accessing Health Data”,
“ruleID”: 1,
“effect”: “Allow”,
“privacyType”: “Information Privacy”,
“targetObject”: “Health Data”,
“constraints”:
      {
      “role”: “Care Giver”,
      “activity”: null,
      “timeRangeStart”: null,
      “timeRangeEnd”: null,
      “location”: null,
      “day”: null
      }
}
```

Listing 4.3: JSON Representation of Sally’s Privacy Rule Regarding Her Health Information

As described in Scenario 1 (§3.2.2), one of Sally’s privacy preferences is to keep her health information to herself, only sharing it with her caregiver. The PASHI framework would model Sally’s privacy rule regarding her health information as shown in Listing 4.3. Sally has defined the

rule to her health data by allowing only a person with the role of caregiver can access that information. The PASHI framework will then convert this model to the Rei policy language's original format, which can be parsed and evaluated using a Prolog engine. Listing 4.4 shows the converted Rei policy of the privacy rule which would be saved in the Prolog knowledge base. At run-time, the privacy rule engine would check the role of the person who is trying to access the information as well as the type of information that is been accessed. If both of those conditions are met, the caregiver can access Sally's health data.

```
Has(P, right(Accessing Health Data, X , [role(Sally , Care Giver, P),
data(Sally, Health, X)], [assert(access(X))]))
```

Listing 4.4: Sally's Privacy Rule for her Health Data

Sally's second privacy preference is regarding physical privacy, and it can be stated in this manner: *"Sally does not like to get disturbed while she is meditating"*. She has defined this rule as the second rule in her rule set (Listing 4.4) and has defined restrictions on access to her three senses: sight, touch, and hearing. Furthermore, she has defined an activity-constraint (while meditating) for this rule to be valid. This privacy rule model will then be converted into a Rei rule (Listing 4.6). At run time, the Prolog engine would check if any smart home device could impact Sally's three senses and if her current activity is meditation. If both of those conditions are met, the privacy rule is applied.

```
{
"userID": 1,
"ruleName": "Disturbance During Meditation",
"ruleID": 2,
"effect": "Deny",
"privacyType": "Physical Privacy",
"targetObject": ["Sight", "Touch", "Hearing"],
"constraints":
      {
      "role": "Any",
      "activity": "Meditation",
      "timeRangeStart": null,
      "timeRangeEnd": null,
      "location": null,
      "day": null
      }
}
```

Listing 4.5: JSON Representation of Sally' Privacy Rule for Meditation

```
Has(P, prohibition(Disturbance During Meditation, Y, [role(P, Any),
or(sense(Sally, Vision, Y), sense(Sally, Touch, Y),  sense(Sally,
Hearing, Y)), activity(Sally, Meditation)], [assert(access(Y))]))
```

Listing 4.6: Rei Rule for Meditation Scenario

Similar to Sally, Zack also has two privacy preferences (Table 3.2**Error! Reference source not found.**). The first privacy preference is to protect his personal preference to watch cartoons from being disclosed to anyone else. This can be represented as shown in Listing 4.7 where Zack has restricted access to his Netflix suggestions regarding cartoons to anyone. This model is then converted to a Rei policy as shown in Listing 4.8. At run time, the Prolog engine would check if the data accessed is Zack's Netflix suggestions for cartoons and apply this privacy rule.

```
{
"userID": 2,
"ruleName": "Restricting Access to Cartoon Preference",
"ruleID": 1,
"effect": "Deny",
"privacyType": "Information Privacy",
"targetObject": "Netflix Suggestions for Cartoons",
"constraints":
      {
      "role": "Any",
      "activity": null,
      "timeRangeStart": null,
      "timeRangeEnd": null,
      "location": null,
      "day": null
      }
}
```

Listing 4.7: JSON Representation Zack's Netflix Privacy Rule

```
Has(P, prohibition(Restricting Access to Cartoon Preference, Y, [role(P,
Any), data(Zack, Netflix Suggestions for Cartoons, Y)],
[assert(access(Y))]))
```

Listing 4.8: Rei Rule for the Netflix Scenario

Zack's second privacy preference is the need to be not disturbed via sight and hearing senses by people outside the smart home on weekends. Listing 4.9 shows how this rule can be modelled. Zack's need for safeguarding his sight and hearing is represented in the target object. Zack has also defined the two constraints regarding the role of the people and the days that this rule will be valid. Listing 4.10 shows how this rule would be converted to a Rei policy. At run-time, the privacy rule engine would check for the role of the person who is trying to access Zack's hearing and sight senses and the current day. If the constraints are being met, the rule will be applied.

```
{
“userID”: 2,
“ruleName”: “Disturbance During the Weekend”,
“ruleID”: 2,
“effect”: “Deny”,
“privacyType”: “Physical Privacy”,
“targetObject”: [“Sight”, “Hearing”],
“constraints”:
      {
      “role”: “People outside the Smart Home”,
      “activity”: null,
      “timeRangeStart”: null,
      “timeRangeEnd”: null,
      “location”: null,
      “day”: [“Saturday”, “Sunday”],
      }
}
```

Listing 4.9: Zack’s Privacy Rule During the Weekend JSON Representation

```
Has(P, prohibition(Disturbance During the Weekend, Y, [role(P, People
outside the Smart Home), [or(sense(Zack, vision, Y), sense(Zack,
auditory, Y)), or(day(current_day, Saturday), day(current_day,
Sunday))], [assert(access(Y))]))
```

Listing 4.10: Rei Rule for Zack’s Privacy Rule for the Weekend

This section discussed the model used to represent user’s privacy preferences. The applicability and the generalisability of the model were shown with the help of the four examples. This section demonstrated the model’s ability to represent both information privacy rules and physical privacy rules. It also accommodated rules constrained by the role of the agent that can violate the privacy, activity of the main user, time, day, and location of the main user. The next section presents the user interface modelling techniques utilised to represent the smart home user interface layer.

4.4 User Interface Modelling

The third knowledge representation requirement of the PASHI framework is to model the smart home user interface layer for a given interaction. This is required by the framework to understand the available modalities or devices to achieve a certain task, and the privacy violating nature of each user interface choice. The user interface model will provide the required information to the PASHI framework to adapt the user interface layer to be privacy-preserving and usable. The user interface model needs to have multiple capabilities to support the PASHI framework’s knowledge requirements fully. The section below highlights some of these capabilities, motivated by the four examples presented in Section 2 of this chapter.

Scenario 1 (§3.2.2**Error! Reference source not found.**): In the example, Yasmin first accesses Sally's health information via the smart speaker (audio output modality). When Zack enters, the smart home switches the broadcast of information to Yasmin's smartwatch (visual output modality). Therefore, Scenario 1 highlighted: 1) the need to represent an interaction task via multiple modalities or multiple devices, and 2) the need to map task-level components to suitable modalities and devices.

Scenario 2 (§3.2.3**Error! Reference source not found.**): In the example, Zack was provided with four options to play music. These options were smart home devices and different feature variations of those devices with varying privacy impact. Hence, Scenario 2 motivated: 1) the need to represent multiple user interface options to complete a single task, and 2) the need to incorporate multiple modalities and variations of these modalities when providing options.

Scenario 3 (§3.2.4**Error! Reference source not found.**): In this scenario, Zack's Netflix feed was adapted from a generic feed to a privacy-protected version. This motivated the need to represent multiple variations of a single output modality that can have varying privacy protection levels.

Scenario 4 (§3.2.5**Error! Reference source not found.**): In this scenario, Sally's camera input was adapted from a generic stream to a privacy-protected version. This motivated the need to represent multiple variations of a single input modality that can have varying privacy protection levels. Scenario 4 also highlights the need to model concurrent interaction tasks where one modality can have privacy protection.

The PASHI framework models the UI layer of smart homes by incorporating the requirements motivated from the examples above and the seminal works from the literature such as concurrent task trees (CTT) (Paternò, Mancini and Meniconi, 1997) and the Cameleon reference framework (Calvary, Coutaz and Thevenin, 2001). Concurrent task trees modelled the tasks as well as the possible alternative paths to complete the goal of the user. The Cameleon reference framework helped to map the task models to concrete user interface (CUI), concrete user interfaces to abstract user interfaces (AUI) and lastly abstract user interfaces to final user interfaces (FUI) at design time.

Figure 4.5 demonstrates the commonly used icons and arrows adopted in the user interface model. Three commonly used icons are abstract task, application task, and interaction task. *Abstract task* represents high-level tasks that can be decomposed into more concrete interaction components (application task and interaction task) later. *Application task* represents output generated from the framework, and the *interaction task* represents interaction points where the user's input is needed to continue the task. The modelling notation also uses three types of arrows: *enabling tasks* that lead to the next task, *concurrent tasks* which run independently from each other, and *choice* which gives the user the option to pick the path of the interaction.

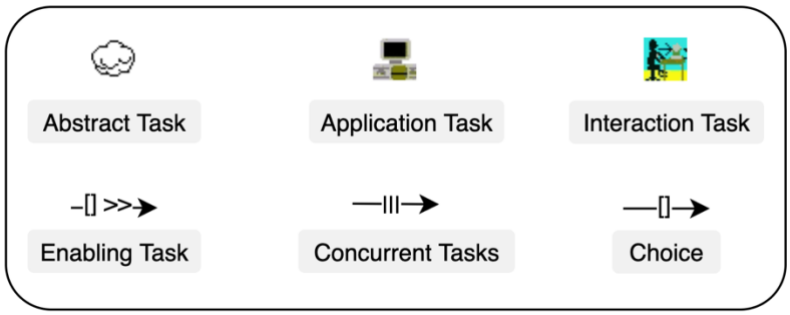

Figure 4.5: Concurrent Task Tree Legend

The user interface model consists of four layers:

1) task model layer,
2) abstract user interface layer,
3) concrete user interface layer and
4) the final user interface layer.

The Task model layer represents the highest level of abstraction. The task model is independent of user interface components and is used to define the interaction at the task level. Task model layer elements have a one-to-one mapping with the abstract user interface layer elements. Based on the task model layer, the abstract user interface layer defines abstract user interface components independent of a specific modality. The abstract user interface layer is followed up by the concrete user interface layer. The concrete user interface layer extends the abstract user interface components to have concrete modalities. There can be multiple modalities for a single abstract user interface component. The concrete user interface layer's components map to the final user interface layer. The final user interface layer consists of smart home devices and their feature variations which can accommodate the concrete user interface components. There can be multiple smart home devices for a single element mapped from the concrete user interface layers. Representing the user interface layer like this helps the framework invoke run-time adaptations to protect the smart home users' privacy.

In Scenario 1 (§3.2.2), Yasmin accessed Sally's health information via a smart speaker and then switched to a smartwatch when Zack entered. At run-time, the user interface layer should support the switch from the smart speaker to the smartwatch. Figure 4.6 shows how to model this interaction so it can support run-time adaptation. The task model layer represents three steps of the interaction, including steps to present information to the user and to receive information from the user. Then these components are mapped to abstract user interface components. After that, abstract user interface components are instantiated into modality-dependent components in the concrete user interface layer. For example, the abstract user interface associated with receiving the user's input query is mapped to a text input modality and an audio input modality. Similarly, output interaction is mapped to a graphical output modality and audio output modality. In the final user interface layer, these modality components are mapped to real smart home devices. For example,

audio output can be mapped to a smart speaker or a Bluetooth headset. Similarly, the graphical user interface component can be mapped to a smart TV, smartwatch, or smart phone. At run time, the PASHI framework will use this knowledge to decide the most appropriate device to deliver the information – considering the privacy risk as well as the usability.

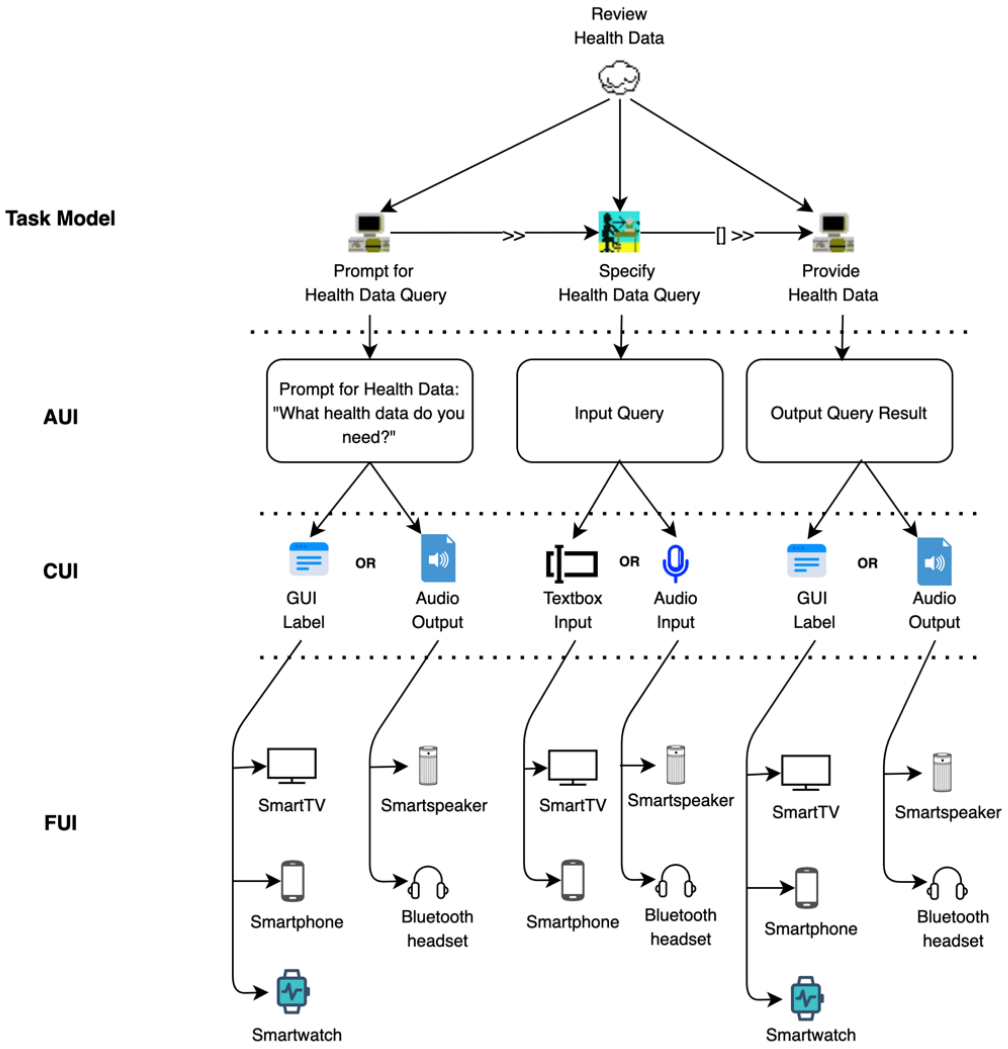

Figure 4.6: User Interface Modelling for the Health Information Scenario

In Scenario 2 (§**Error! Reference source not found.**), Zack tries to play music while his mother is meditating. The smart home then presents four options to play music. Figure 4.7 represents the user interface model required for representing this interaction. The different layers serve the same purposes as described above for Scenario 1's user interface model. However, in contrast to Scenario 1, this example provides choices for the user to select the device to play music rather than adapting automatically. This is defined at the task model level, where the sub-task of *playing music with options* provides the user options to select the preferred user interface adaptation. All the leaf nodes of the task model (i.e., the Final UI elements) are then mapped to abstract user interface components. The user can be presented with choices via multiple modalities (graphical user interface and audio), and the user can select their choices via multiple modalities (touch and audio). Since the task is to listen to music, the final sub-task of playing music will only be presented using

the audio modality. At the final user interface layer, the user is provided with four options to play music.

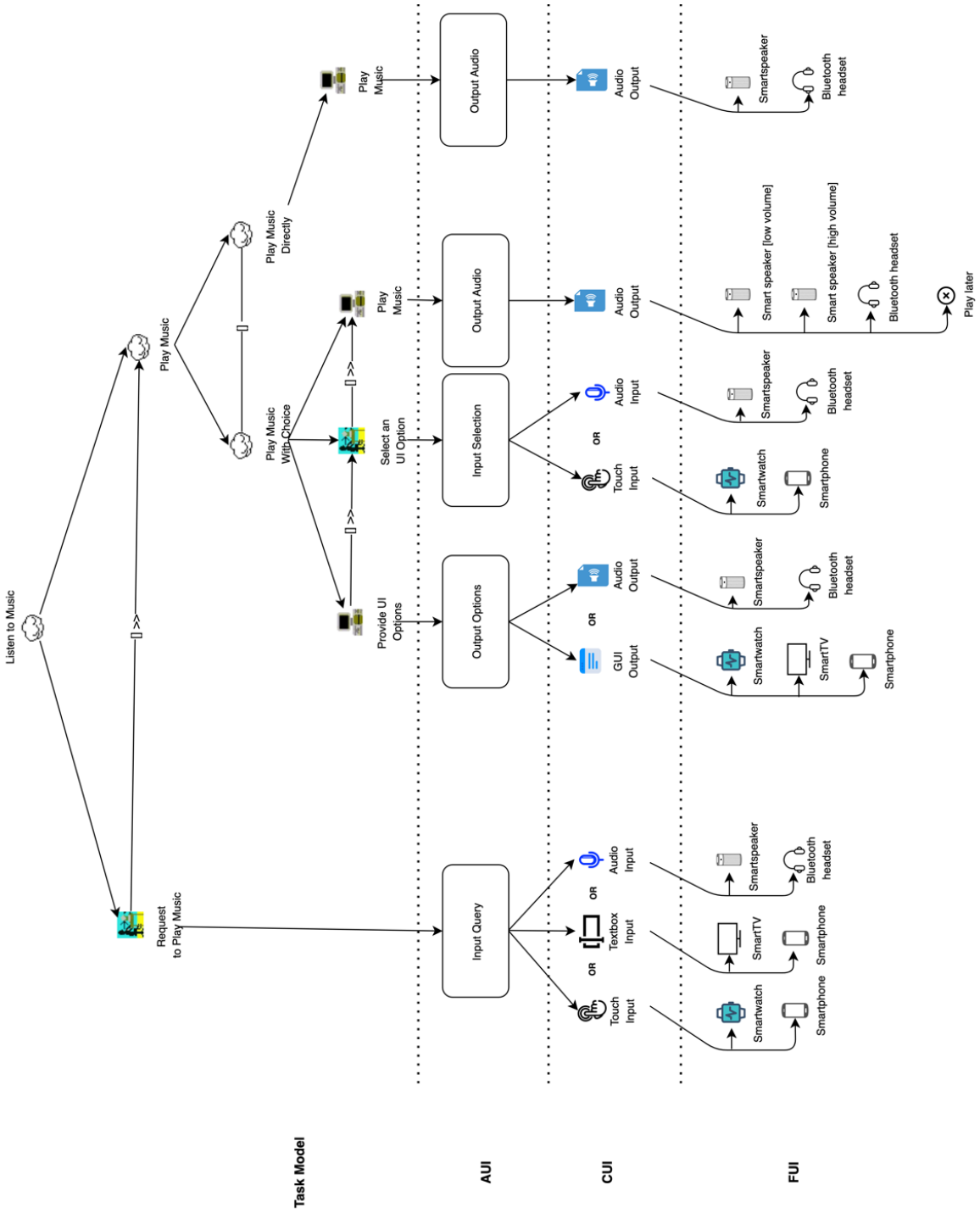

Figure 4.7: User Interface Modelling for the Meditation Scenario

This includes feature adaptations of the smart speakers with varying volume levels, device choices between the smart speaker and the Bluetooth headset, and the option to terminate the task. At run-time, the PASHI framework has the flexibility to provide choices to the user and adapt the user interface layer according to the user's choices.

In Scenario 3 (§**Error! Reference source not found.**), Zack's Netflix feed switched from a generic version to a privacy-protected version as his mother entered the room. This differs from Scenario 1, as the adaptation happens in the same modality (graphical user interface of the smart TV), and it differs from Scenario 2, as Zack is not given a choice to pick the adaptation at run-time. This functionality is shown at the task model layer. The task of showing Netflix is forked (Figure 4.8), where one of the options provides the generic Netflix feed, and the other option provides the privacy-protected Netflix feed. Modelling the interaction in this manner means that the PASHI framework can adapt quickly to the privacy-protected version of the Netflix feed.

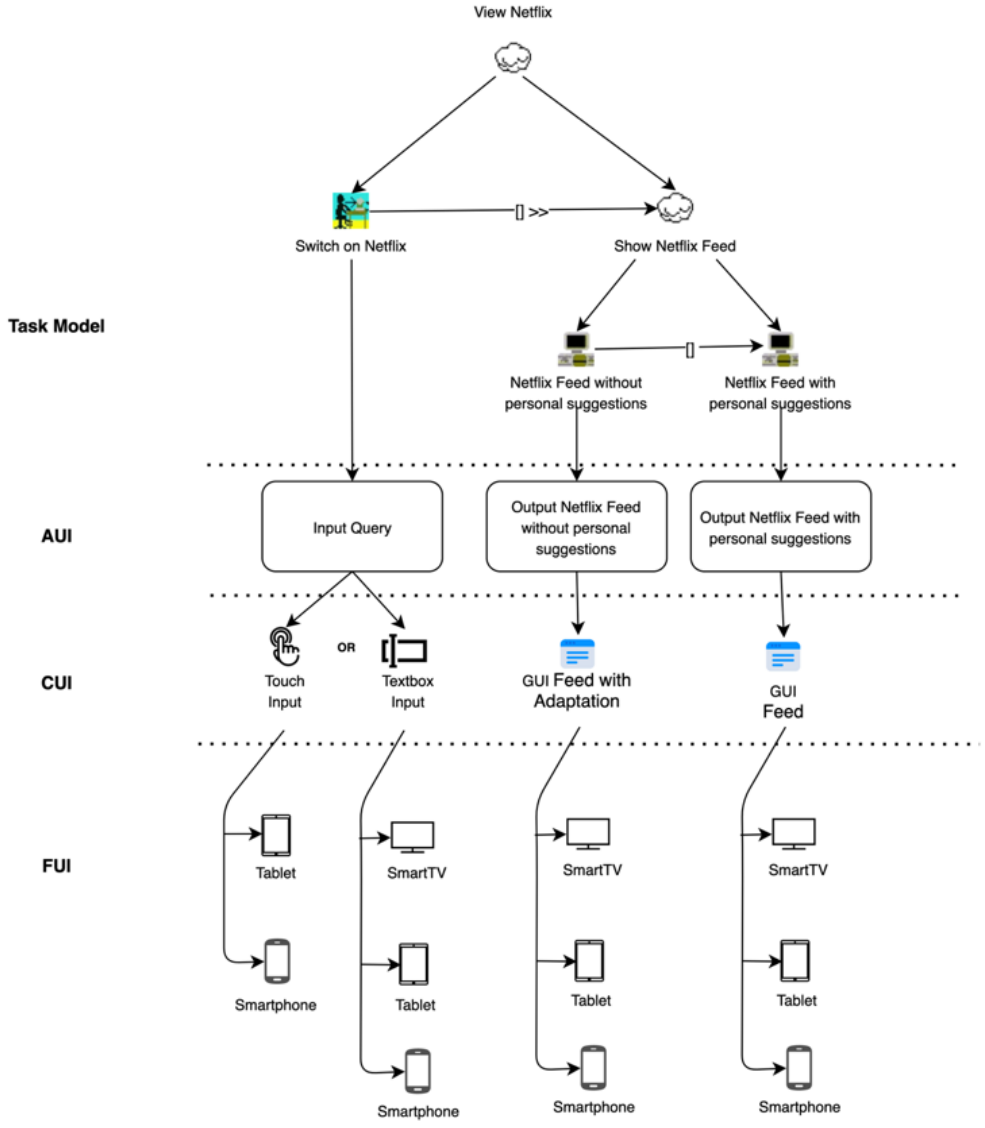

Figure 4.8: User Interface Modelling for the Netflix Scenario

In Scenario 4 (§**Error! Reference source not found.**), Sally's camera input feed is adapted from a generic version to a privacy-protected version to safeguard Zack's privacy. Scenario 4 is like Scenario 3 regarding switching to a privacy-protected version of the same modality. At the same time, it differs, as the video conference call consists of two concurrent interactions, and the feature adaptation happens at the input modality. Figure 4.9 shows how the video conference call is constructed of two concurrent input and output interaction tasks. Also, the input camera feed can be modelled to have either a generic feed or a privacy-protected feed. Both camera-input versions are

mapped to the abstract user interface components, modality-dependent concrete user interface components, and device-dependent final user interface elements. Modelling the user interaction for Scenario 4 enables the PASHI framework to adapt the camera feed and protect privacy at run-time.

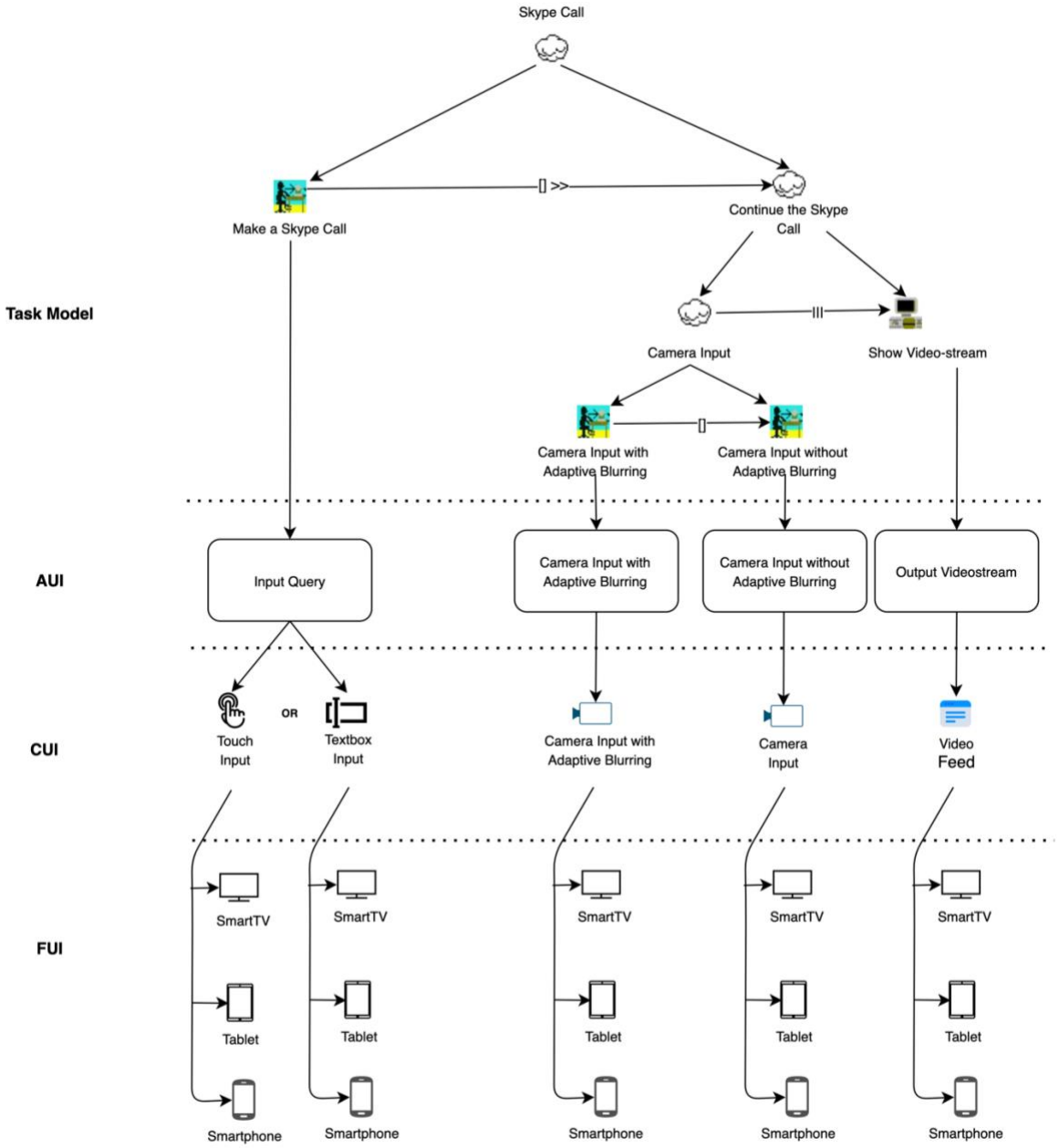

Figure 4.9: User Interface Modelling for the Skype Call Scenario

This section highlighted the features required by the user interface model to support the PASHI framework's knowledge representation. This was presented via four distinct smart home interpersonal privacy violation examples, demonstrating the user interface model's ability to:

1) represent user interface components with multiple abstraction levels from the task level to the device level;
2) map multiple modalities and devices that can achieve a single interaction task;
3) map variations of the same modality and device that can achieve a single interaction task;
4) represent concurrent interaction tasks with support for adapting either of the tasks; and

5) provide choices to the user to select adaptations.

4.5 Discussion

The existing smart home adaptive user interface frameworks such as MASP (Blumendorf, 2009), GPII (Loitsch *et al.*, 2017), and MIODMIT (Cronel *et al.*, 2019) do not support interpersonal privacy violation detection and protection, because, although they capture generic knowledge of the smart home required for user interface adaptations, they do not capture knowledge required to detect interpersonal privacy violations. Knowledge representation is a critical step for the functionality of adaptive systems (IBM, 2006); hence it is pertinent for generating privacy-aware smart home user interfaces. This research gap motivated **RQ1**: *How can we characterize the smart home environment adequately to drive privacy-aware user interface adaptations?*

The literature review (§2) and the analysis of the example scenarios (§**Error! Reference source not found.**) generated criteria for the knowledge representation needs of the PASHI framework to generate adaptive user interfaces. Then, this chapter presented and justified the three modelling approaches used to fulfil these knowledge representation requirements. Furthermore, the applicability, generalisability, and extensibility of these three models were also discussed via a case study based on four different privacy-violating scenarios relating to interpersonal privacy in smart homes. This section presents a summary of the findings and discusses them.

4.5.1 Summary of Findings

Characteristics identified to model the knowledge representation of interpersonal privacy violations were appropriate and sufficient. The following characteristics were identified for the knowledge representation:

- user's privacy preferences,
- user's user interface preferences,
- features of the smart home user interface layer, and
- the smart home context.

The case study demonstrated that these characteristics were sufficient to model the knowledge requirements for managing interpersonal privacy for a range of interpersonal privacy-violating scenarios within a smart home. The characteristics were then used to identify the required models.

The knowledge representation models in the PASHI framework are adequate for capturing the rich context of the interpersonal privacy-violating scenarios. The case study demonstrated this by using the models to represent the knowledge related to four selected interpersonal privacy-violating scenarios. These scenarios were representative of the different interpersonal privacy

violations (both information privacy and physical privacy), user's privacy preferences, user's user interface preferences, smart home user interfaces, and contexts.

- *The user interfaces preference mode*: §4.2 showed the model's ability to capture different user interface preferences of the user, including preferences for smart home devices and modalities. Furthermore, the model proved to be flexible enough to capture multiple constraints associated with these preferences such as the current activity of the user, time, and the day.
- *The privacy preference model*: §4.3 showed the model's ability to capture users' different interpersonal privacy preferences (information privacy and physical privacy). The model also demonstrated the ability to incorporate context information regarding privacy preference such as user roles, time, day, current activity, and location.
- *The user interface model*: §4.4 demonstrated the model's ability to represent different modalities and features of smart home user interfaces that can impact interpersonal privacy. In addition to that, the model provided the required level of abstraction from the interaction level to the device level allowing flexible user interface adaptations. The model also accommodated multiple modalities and feature variations of the same modality when representing interaction steps and concurrent interaction tasks.

Different features of the models provide the dimensions used to derive example scenarios. Different variations of privacy preference rules (e.g.: based on the privacy type or the constraint type), different variations of the user interface preferences (e.g.: modality preferences or smart home device preferences), and variations of adaptive user interfaces (e.g.: automatic adaptations or choice-based adaptations) helped to generate example cases to be used in the two user studies discussed later in this thesis (§5.5 and §6).

4.5.2 Discussion

The knowledge representation models adequately characterized interpersonal privacy-violation scenarios to fill a research gap in the smart home user interface framework literature and the user modelling literature.

As discussed earlier (§2.2.2), existing user interface frameworks did not fully support the knowledge representation required for modelling interpersonal privacy violations. MASP, GPII, MIODMIT, and AM4I provided partial user modelling support but they were not sufficient for the requirement. For example, none of these frameworks had interpersonal privacy preference models, and comprehensive user interfaces preference modelling. In contrast, most of the frameworks provided some level of user interface modelling required for modelling interpersonal privacy violation scenarios. For example, out of the framework analysed in the literature (§2.2.2), the

MASP framework covered the greatest number of knowledge representation requirements. It included a detailed user interface model, smart home context, and layout information but in the user interface model, MASP did not provide the flexibility to define multiple paths for a specific task allowing modality switching. This concurrent task-based user interface modelling was presented in both Dynamo-AID and CEDAR architecture, but they had other drawbacks such as Dynamo-AID not supporting user modelling and CEDAR was not supporting multimodal user interfaces. PASHI framework models bridged this gap in the literature and provided the more comprehensive knowledge representation models required for capturing the information of interpersonal privacy violation scenarios. However, the case study focussed on evaluating whether the models were sufficient, rather than if they were complete. Therefore, further research should be conducted to investigate the completeness of the models and extend them as needed. Apart from that, the models individually improved the existing knowledge representation models with certain limitations.

As discussed previously (§2.2.3), the VUMS cluster (Kaklanis et al., 2016) and the ontology-based user model (Skillen *et al.*, 2014) provided sufficient support for modelling user capability and user interfaces preferences, but they lacked support for prioritising user inter preferences and they did not provide the required flexibility to define smart home device preferences and feature preferences. In addition, none of the user models provided support for interpersonal privacy preferences. These gaps were addressed by the PASHI framework's knowledge representation models. Furthermore, individual models can be discussed as follows:

Privacy preference model: Modelling interpersonal privacy using a role-based access control mechanism allowed the successful definition of both types of privacy preferences (information and physical privacy) with greater expressivity. Even though the *privacy preference model* directly extended the Rei policy language (Kagal, 2002), Rei was not previously evaluated for its applicability with interpersonal privacy preference modelling. The case study demonstrated Rei's applicability in different contexts. However, the model's ability to handle conflicting privacy preferences was not evaluated with the selected scenarios even though the model provided limited conflict resolution support. Therefore, further inquiry is required to understand different types of interpersonal privacy conflicts, the applicability of the privacy preference model to represent and resolve those conflicting politics.

User interface preference model: Modelling both device and modality preferences added an extra dimension to the existing user interface preference modelling literature. VUMS cluster being one of the most comprehensive provides a detailed user interface preference model, but it lacks support for adding device preferences as in the PASHI-models. Furthermore, VUMS cluster was not tested with interpersonal privacy-violating scenarios which required the representation of different user interface features that impact interpersonal privacy and the context of which the preference can be

applied. The PASHI-models addressed this gap by incorporating the required additional information (e.g.: smart home context information). However, the model was not evaluated for extendibility but sufficiency. Therefore, further inquiry should be done to understand the extendibility and the generalisability of the model to present user interface preferences. Furthermore, the model does not capture preferences for direct human-to-human interactions. To support this, the user interface preference model would need to capture users' preferences for direct interaction with humans. This requires further analysis as well.

User interface model: The model successfully represents the privacy-aware adaptive user interface layer where it used methods from the literature while filling a gap in the existing smart home user interface model literature. Using CTT (Paternò, Mancini and Meniconi, 1997) and Cameleon framework (Calvary, Coutaz and Thevenin, 2001) to represent adaptive user interfaces was done in CEDAR but it was in the domain of enterprise software (GUI). In comparison with existing user interface models of MASP, GPII, and MIODMIT, PASHI-models provided the flexibility to do modality (or smart home device) switching based adaptation. However, the user interface model was not evaluated for completeness but sufficiency. Therefore, the model requires further evaluation regarding its ability represent other smart home contexts (completeness).

Apart from the model's individual drawbacks, the current version of the two preference models (privacy and user interface) does not account for evolving user preferences with time. Generally, with time and experience, user preferences tend to change. Therefore, the models should be able to evolve with the user.

Another aspect that can be improved is the policy authoring (in this case user preference authoring) features. At the moment policies are set by an engineer/researcher who would set up the smart home. This is a limitation of the framework as the smart home users lack control over their preference setting. Works of Reeder et al. (2008) presented a grid-based visualisation tool for defining security policies that outperformed the standard list-based rule setting. A similar approach can be extended and used in this context. Therefore, this motivates the development and the evaluation of a suitable preference authoring tool set for users to set their privacy preferences and user interface preferences.

Thinking beyond the problem at hand, these models can also be used independently with other adaptive user interface frameworks with minimal changes. This will allow the respective framework to understand the required context of interpersonal violating scenarios and in-directly act as a mechanism to source novel interpersonal privacy-violating scenarios and their representative knowledge.

4.6 Summary

This chapter addressed the **RQ1** (*How can we characterize the smart home environment adequately to drive privacy-aware user interface adaptations*) via a case study. The case study enabled the identification of knowledge representation requirements for privacy-aware smart home interfaces. The three models that were produced (user interface preference, privacy preference, and user interface) found to be adequate for modelling the rich context of interpersonal privacy violation scenarios used in the evaluation studies reported in Chapter 5 & 6. In addition, certain limitations of the case study and the models were identified, and to address them, the following recommendations can be made:

Model improvements:

- The user interface preferences model should be extensible enough to integrate novel preferences (e.g., direct human-to-human interaction) and be descriptive and flexible enough to define the detailed user interface feature preferences.
- The privacy preference model should provide more support for handling privacy preference conflicts.
- Both the user preference models should be improved to capture changing user preferences.

Further evaluations:

- Develop interpersonal privacy violating taxonomy to help the studies that look to evaluate the completeness of the models.
- Conduct studies to evaluate the completeness of the knowledge representation models in capturing the rich context of interpersonal privacy violating scenarios.
- Inquire into different interpersonal privacy preference conflicts and conduct studies to evaluate the applicability of the PASHI framework's privacy preference model in handling the identified conflicts.
- Conduct studies to evaluate the ease of integration of the models into other types of adaptive user interface frameworks or to frameworks that require understanding the contexts of interpersonal privacy violations in a cyber-physical environment.

5. Privacy-aware Smart Home Interface Framework

5.1 Introduction

The previous chapter presented and evaluated the modelling techniques used to capture the required knowledge for generating adaptive user interfaces. These modelling techniques managed to represent users' privacy preferences, user interface preferences, and the smart home user interface layer. The next step of generating privacy-aware adaptive user interfaces is to integrate the modelled knowledge into an adaptive framework. The framework will utilise the modelled knowledge to drive user interface adaptations. Therefore, this chapter presents and evaluates the privacy-aware smart home interface (PASHI) framework's software architecture and its functionality. In doing so, this chapter will address **RQ2**: *"What is an appropriate software architecture for a privacy-aware adaptive smart home interface framework?"*

This chapter will first introduce the PASHI framework's software architecture by discussing its layers and components. Then it will discuss the framework's functionality by evaluating the core processes: 1) privacy violation detection process, and 2) user interface adaptation process. In the evaluation, the underlying algorithm of each process will be presented and analysed with the support of an example scenario. Finally, the chapter will report on a user study conducted to evaluate the usability of adaptive user interfaces. The health scenario from Chapter 3 (§3.2.2**Error! Reference source not found.**) will be used as an illustration in §5.3 and §5.4.

5.2 PASHI Software Architecture

Architecture-based frameworks help to build self-adaptive systems. Kramer and Magee (2007) argued that architecture-based frameworks provide the right level of abstraction and generality to manage the problems faced by self-adaptive systems. They also argued that an architecture-based solution would provide means to use existing work, to scale when necessary and to integrate with other work (modelling techniques, analysis, adaptation, etc). Support for this argument is strengthened by exploring the works of Blumendorf (2009), Akiki et al. (2015) and Cronel et al. (2019), in which the researchers have used an architectural-based framework to build adaptive user interfaces in smart environments. Therefore, I have also used an architectural-based framework to build adaptive user interfaces to preserve interpersonal privacy in a smart home.

The PASHI framework draws from three software architecture patterns: 1) the MVC architecture (Reenskaug, 1979), 2) MAPE-K loop (Kephart and Chess, 2003), and 3) the Cameleon reference framework (Calvary, Coutaz and Thevenin, 2001). MVC pattern's core concepts such as separation of concerns helped in defining the PASHI framework to be modular. Apart from that, the MVC pattern acted as the general architecture of the PASHI framework which laid the foundation to integrate other architecture patterns and components easily. The MAPE-K loop infused adaptive capabilities into the framework by defining the necessary components. As discussed in Chapter 4, the Cameleon reference framework provided the basis to define the smart home user interface layer which can be adapted easily at different abstraction levels. Mirroring the MVC architecture, the PASHI framework software architecture (see Figure 5.1) consists of three main layers: the View layer, the Control layer, and the Model layer. The following section will discuss these layers and their components.

5.2.1 View Layer

Originally the MVC pattern's view layer was developed to be used with graphical user interfaces. To apply MVC within the smart home domain, the PASHI framework has extended the view layer from a GUI representation to a multimodal user interface representation. As shown in Figure 5.1, the view layer consists of the physical devices in the smart home. These could be smart home UIs such as smart speakers, smartwatches, smart TVs, etc., or smart home sensors such as cameras, microphones, ambient sensors, and so on. It is also important to note that smart home sensors can be integrated into commonly used smart home UIs such as smart speakers.

Based on the Cameleon reference model for interfaces described in Chapter 4, the view layer represents the final user interfaces of the smart home system. Final user interfaces model the actual user interfaces within the smart home. Each device will have a specific implementation to handle the PASHI framework's server-side output and to send user input back to the PASHI framework's server. At the server-side, the user interface controller (Figure 5.1) will coordinate the communication between the users and the PASHI-server. In parallel to this functionality, the sensor layer of the smart home captures the smart home's context information and sends it back to the PASHI server. On the server-side, the sensor-controller handles these data streams and communicates that to the *Context Manager*.

The next section discusses the controller layer of the PASHI framework.

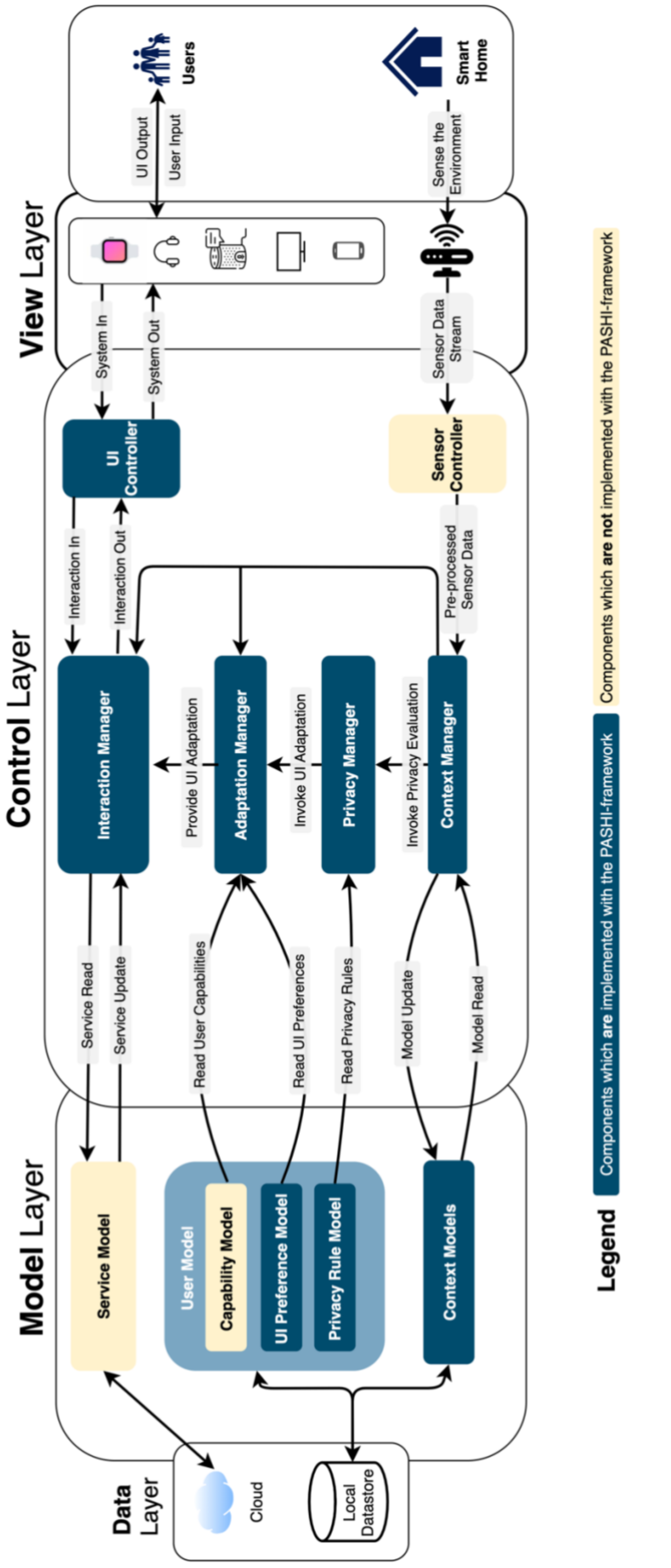

Figure 5.1: PASHI framework

5.2.2 Control Layer

The control layer of the PASHI framework handles its logic. It incorporates the MAPE-K adaptive control loop (Kephart and Chess, 2003), where M stands for Monitor, A stands for *Analyse*, P stands for *Plan*, E stands for *Execute* and K stands for *Knowledge*. The MAPE parts are in the control layer. The *Knowledge* aspect is represented in the model layer, which was discussed in detail in Chapter 4 and will be briefly discussed in the Model layer (§5.2.3). MAPE components are mapped to the PASHI framework as follows:

- ***M**onitor*: represented by the *Sensor Controller* and the *Context Manager*.
- ***A**nalyse*: represented by the *Privacy Manager*.
- ***P**lan*: represented by the *Adaptation Manager*.
- ***E**xecute*: represented by the *Interaction Manager* and the *User Interface Controller*.

These components will be discussed in detail in this section.

The *Context Manager* is responsible for keeping an up-to-date status of the context of the smart home. The *Context Manager* uses context models from the model layer and keeps them populated using the information received via the *Sensor Controller* (note that the current research does not explore the details of sensor controllers as it is outside the scope of interpersonal privacy management). Whenever there is a context change, the *Context manager* will update the *Privacy Manager* to check for any privacy violations. The architecture uses the observer-observable design pattern for this functionality to occur where the *Privacy Manager* acts as an observer of the context models. Whenever there is a context model update, the *Privacy Manager* is invoked. This is similar to moving to the *Analyse* stage of the MAPE-K loop.

The *Privacy Manager* handles the task of privacy violation detection. Whenever the *Context Manager* triggers the *Privacy Manager*, it will evaluate the privacy status of smart home users. First, the *Privacy Manager* will use the updated information from the *Context Manager* to construct privacy queries. These queries will be evaluated against the knowledge base of the PASHI framework. The knowledge base was created by saving each smart home user's privacy preferences. Privacy preferences were written using the Rei policy language (Kagal, 2002) where Prolog (https://www.swi-prolog.org/) was used as an implementation language. Therefore, when there is a context change, the *Privacy Manager* will create and evaluate privacy queries using the Prolog engine. If there is a privacy violation, the *Privacy Manager* will invoke the *Adaptation Manager*, moving to the *Plan* stage of the MAPE-K loop. The *Adaptation Manager* generates the appropriate adaptation to preserve the privacy of the smart home users. Whenever there is a privacy violation, the *Adaptation Manager* gets invoked. When this happens, the *Adaptation Manager* evaluates the best possible adaptation using the user interface adaptation algorithm (Listing 5.2). This algorithm outputs the best user interface adaptation which preserves the privacy of the smart home user while maintaining usability as much as possible. Then the user interface adaptation

details are sent to the *Interaction Manager*. This is analogous to invoking the *Execute* stage of the MAPE-K loop.

The *Interaction Manager* and the *UI Controller* manipulate the user interface layer depending on the information received from the other components of the framework. The *Interaction Manager* can receive user input and provide the required services to the user as well as present information to the smart home user. When there is a privacy violation, the *Interaction Manager* receives information from the *Adaptation Manager*. Then the *Interaction Manager* adapts the UI layer. This is executed by the *Interaction Manager* passing the information required for the adaptation to the *UI Controller*. Then the *UI Controller* converts the UI model information and sends that to the appropriate UI as JSON objects. The client devices will have a method implemented to receive these JSON objects and to present the UI to the smart home user.

5.2.3 Model Layer

This section discusses the model layer of the PASHI framework. Chapter 4 already discussed the user model components: the *UI Preference Model* and *Privacy Rule Model*. However, the *Service Model* is not discussed as it was not within the scope of the research and the *Capability Model* as the examples are not representative of different capabilities of users. But the UI adaptation algorithm (Listing 5.2) does support the user's capabilities, hence the user capabilities can be easily incorporated into the PASHI framework when the need arises.

The *Context Model* represents and holds the context of the smart home with the individual user details off-loaded to the user model. The user models are part of the context model, but Figure 17 shows them separately for ease of explanation. The *Context model* captures the context information such as the smart home layout, position of the users, activities of the users, location of the smart home devices, temperature, time, day, etc. This information will be updated with the input received by the *Context Manager*, keeping the context model up to date. Detailed discussion of the model layer components was provided in Chapter 4.

This section discussed the PASHI framework's software architecture and explained how the software architecture was structured and how each component and layer communicated.

5.3 Privacy Violation Detection

This section discusses the process of privacy violation detection and the algorithm that is used to detect privacy violations.

5.3.1 Privacy Violation Detection Process

The PASHI framework needs to have the ability to detect potential privacy violations. This feature is required to invoke UI adaptation at the right time. As discussed in the previous section, the PASHI framework uses a Prolog-based privacy rule engine to evaluate privacy violations, whose rule structure was based on the Rei policy language (Kagal, 2002). Figure 5.2 demonstrates the activity diagram of the privacy violation detection process.

In the health scenario example, the main user (Sally) tries to access her blood glucose details via the smart speaker. This request is transferred through to the UI controller (this component is not shown in the activity diagram, hence refer to Figure 5.1) where it will process the user intent and pass to the *Interaction Manager*. The *Interaction Manager* will then process the request by forwarding the information required by the user. In parallel, another co-occupant (Zack) enters the room. This context change will be captured by the sensors (this component is not shown in the activity diagram, hence refer to Figure 5.1) which will then be sent to the *Context Manager* via the sensor controller. The *Context Manager* will use this information to update the models, and the change in context (co-occupant entering the room) will invoke the *Privacy Manager*.

The Privacy Manager is responsible for detecting privacy violations. *The Privacy Manager* will feed the context information from the *Context Manager* to the privacy risk evaluator algorithm (Listing 5.1) to evaluate the privacy status within the smart home. The results of this are sent back to the *Interaction Manager* to be used when generating the output. The Privacy Manager detects a privacy violation as the co-occupant (Zack) is not allowed to listen to the blood glucose levels (health data) of the main user (Sally). This detected privacy violation invokes the *Adaptation Manager* which calculates the best adaptation and sends the information to the Interaction Manager (the process of the Adaptation Manager will be discussed in section §5.4).

The Interaction Manager incorporates the required information and sends that to the main user (Sally). *The Interaction Manager* receives the results of the privacy risk evaluation from the Privacy Manager, the user's requested information (blood glucose data) from the service manager (this component is not shown in the activity diagram, hence refer to Figure 5.1) and the UI adaptation evaluation from the *Adaptation Manager. The Interaction Manager* creates an output with the received information and sends it to the appropriate user interface as a JSON object.

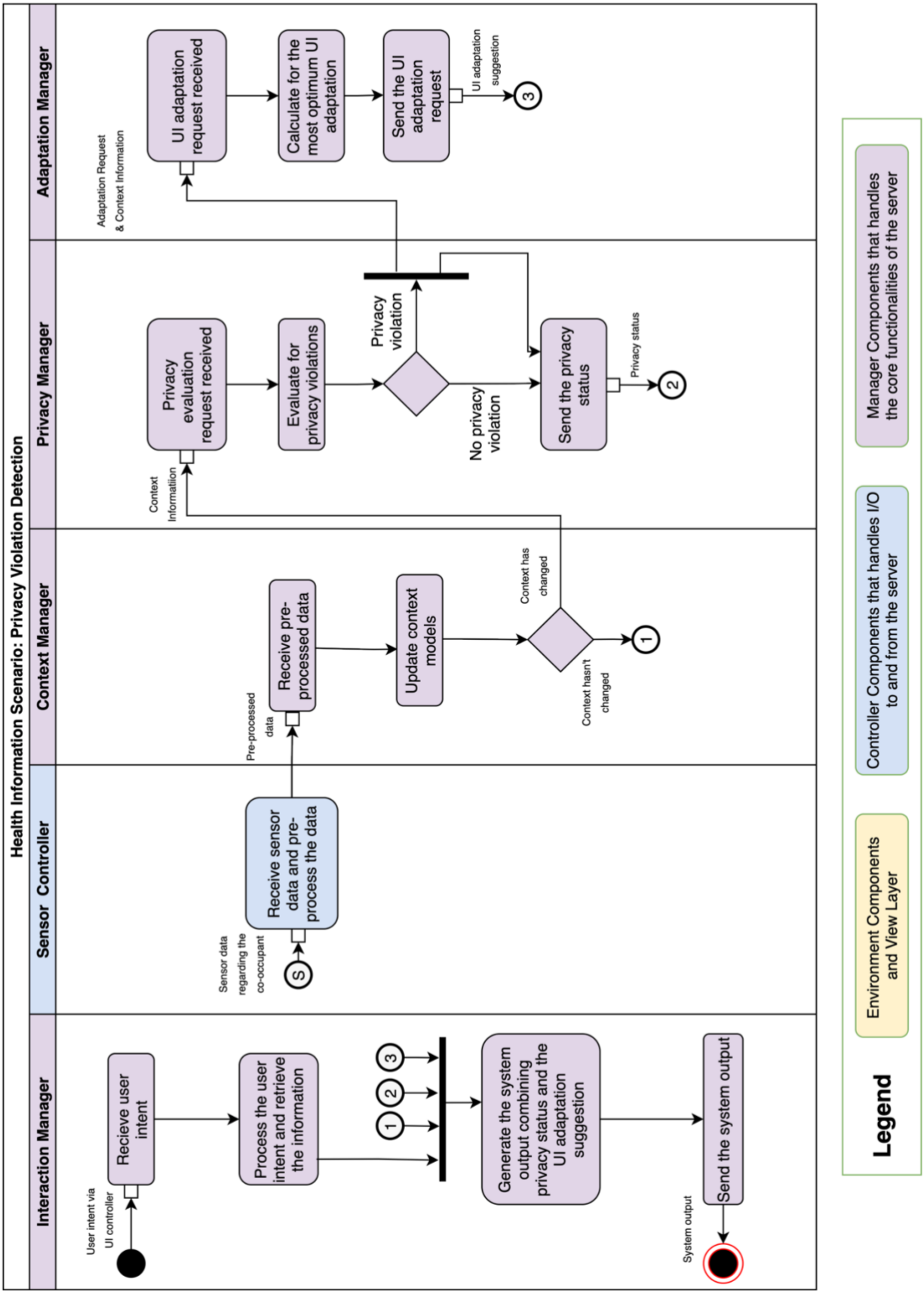

Figure 5.2: Activity Diagram for the Privacy Violation Detection Process

5.3.2 Privacy Violation Detection Algorithm

The Privacy Manager evaluates the privacy status of the smart home using the privacy risk evaluator algorithm. This algorithm incorporates context information and evaluates against the privacy rule knowledge base. Whenever there is a privacy violation, it will send that status to the Privacy Manager where it will call the Adaptation Manager.

In the example scenario, there are four smart home devices within the room: a shared smart speaker, a shared smart TV, Yasmin's smartwatch and Yasmin's smart phone where Yasmin is the caregiver. The smart speaker and the smart TV are shared among three of the smart home users while the smartwatch and the smart phone are personal to Yasmin.

The algorithm will create a temporary list (*ui_list)* of user interfaces that are either activated or about to get activated. Next, the algorithm will check with each user interface in the *ui_list* to check who is the range of each user interface. Then the algorithm will check for each person in the range of a specific user interface if the activation of that user interface would violate the privacy of any of the smart home users. This is done in two steps where the algorithm checks 1) if there is an information privacy violation with the information being output or 2) a physical privacy violation with the smart home device disturbing a smart home user who wants to be in solitude. These calculations are cached in the *privacy_risk_cache* dictionary with a unique key generated concatenating *ui_id and the user_id.* These cached dictionary entries will be used later to improve the efficiency of UI adaptation algorithm (Listing 5.2)

Device	Users in the range	Information privacy violation	Physical privacy violation
Smart speaker	**Sally, Yasmin & Zack**	**True**	**False**
Smart TV	**Sally, Yasmin & Zack**	**True**	**False**
Yasmin's smart phone	**Yasmin**	**False**	**False**
Yasmin's smartwatch	**Yasmin**	**False**	**False**

Table 5.1: Privacy Risk Evaluation for the User Interfaces

Table 5.1shows the status of each user interface. The smart speaker is currently activated where the other three user interfaces can be activated. The smart speaker has Zack in range, which causes an information privacy violation as he is not authorised to listen to Sally's health information. The same analysis goes for the smart TV, but it is not yet been used by any of the users. The smart speaker broadcasting the health information of Sally while Zack is in the room creates a privacy

violation and the algorithm will pass this finding back to the Privacy Manager to invoke the Adaptation Manager.

```
Privacy_risk_evaluator(active_uis, tentative_uis, privacy_risk_cache)
//Empty the privacy_risk_cache dictionary
  privacy_risk_cache.clear()

  //Combine active user interfaces and the user interfaces which has a
possibility to get activated
  ui_list <- active_uis.union(tentative_uis)
  //initialising the variables
  temp_data_id <- 0
  temp_ui_id <- 0
  privacy_violation <- False

  //loop through the user interface list
  FOR EACH ui_id in ui_list
    data_id = get_broadcast(ui_id)
    in_range_user_list = get_ui_range_list(ui_id)
    FOR EACH user_id in in_range_user_list
      if privacy_violation
        BREAK
      for rule_owner_id in in_range_user_list
        //skipping the same user id to reduce calculations
        if user_id == rule_owner_id
          CONTINUE
        location_id <- get_location(rule_owner_id)
        action_id <- get_action(rule_owner_id)
        //checking for privacy violations

        IF (is_physical_privacy_risk (user_id, ui_id, location_id,
action_id, rule_owner_id)) OR (is_information_privacy_risk (user_id,
data_id, location_id, action_id, rule_owner_id))
          privacy_violation <- True
          privacy_risk_cache[ui_id + user_id] <- True
        ELSE
          privacy_risk_cache[ui_id + user_id] <- False

  RETURN privacy_violation
```

Listing 5.1: Privacy Risk Evaluator Algorithm

The running time of the algorithm is established to be polynomial: O (*l* * *m* * *m*), where *l* = list of user interfaces that are activated or can be activated and *m* = number of people in the range of a user interface. *m* is repeated as the algorithm uses the same list to identify the rule owner as well as the person who is trying to access the information or the bodily sense of the main user. Even though the time complexity is polynomial, the values of *l* and *m* would not exceed 100 since the number of people in the smart home and the number of smart home devices are smaller in size.

The PASHI framework can detect interpersonal privacy violations at run-time for the given scenario and for other scenarios of that nature. This section described the privacy violation detection process and evaluated the algorithms used to detect privacy violations. If there is a risk of privacy violation, the Privacy Manager will invoke the Adaptation Manager. This process will be discussed in the next section.

5.4 User Interface Adaptation

This section discusses the process of the user interface adaptation and the algorithm that is used to generate an optimum user interface adaptation.

5.4.1 User Interface Adaptation Process

The core functionality of the PASHI framework is the privacy-aware user interface adaptation. This aspect of the PASHI framework fills the research gap in the smart home UI frameworks; it helps to protect the interpersonal privacy of the smart home users by adapting the UI layer. As I have discussed in Chapter 4, the PASHI framework uses the Cameleon framework's user interface modelling steps to model the UI layer of the smart home. Those design-time models help the Adaptation Manager to pick the most appropriate adaptation at run-time. The algorithm that picks this adaptation is discussed in the next sub-section (§5.4.2)

As shown in Figure 5.3, the caregiver (Yasmin) inputs a query to access the main user Sally's blood glucose level via the *smart speaker* where it is part of the *view layer* (Figure 5.1). The *smart speaker* will then pass the user's query to the *UI controller*, in which the user input would be processed. The processed user input will then be managed by the *Interaction Manager* which would process the user request. While this process carries on, a co-occupant (Zack) enters the room which triggers an UI adaptation request to the Adaptation Manager. Details of how the entering of co-occupant (Zack) triggered the UI adaptation were discussed in the previous section (§5.3).

The Adaptation Manager is responsible for calculating the optimum adaptation. When the request is received the Adaptation Manager will use the adaptation algorithm (§5.4.2) together with available context information to pick the ideal UI adaptation for the scenario. This suggestion

would then be sent to the *Interaction Manager* which will then incorporate that into the system output. The *Interaction Manager* would also incorporate the results from the *Privacy Manager* which is used to make the user aware of the possible privacy violations that were avoided. In this scenario, the PASHI framework has picked the smartwatch to deliver the information. Hence, the *UI controller* would send that information to the caregiver's (Yasmin's) smartwatch.

5.4.2 UI Adaptation Algorithm

The *Adaptation Manager* evaluates the available user interfaces in the smart home and calculates the best UI adaptation for a given scenario. This UI adaptation prioritises the following factors when selecting an adaptation in the same order that they are mentioned:

1) privacy protection
2) reachability to the main user
3) meeting user capabilities
4) meeting user's UI preference
5) maintaining the usability of the interaction.

The *Adaptation Manager* uses the UI adaptation algorithm (Listing 5.2) to identify the most suitable adaptation to the UI layer. I will extend the same example from the previous section to analyse this algorithm as well.

In Table 5.2, I have shown the user interface preference and usability ratings for each smart home device from the viewpoint of Yasmin. Yasmin's most preferred smart home device is the smart speaker and the second is the smartwatch. Yasmin rates the smart speaker to have a rating of 10 for usability where the smartwatch has a rating of 6.

Smart home device / **Value**	**Smart Speaker**	**Smart TV**	**Smart Phone**	**Smartwatch**
Preference order	1st	4th	3rd	2nd
Usability values	10	8	4	6

Table 5.2: Smart Home Device Ratings from Yasmin's Point of View

The algorithm will populate the score matrix (Table 5.3) and use that to pick the most appropriate UI adaptation. The order of the scoring happens in the most optimum way to improve the running time of the algorithm. The algorithm first checks if there is a privacy violation in each UI adaptation and then checks if each UI adaptation can transmit the information to the main user. After that, the algorithm will check if the UI adaptation's modality matches the main user's capability. The first three features have been represented as binary values and failing to meet any of

them would remove that specific UI adaptation from the possible list of adaptations. Scoring is then followed by the user's UI preference rating and the UI's usability ratings. These values are represented in Table 5.2.

Finally, all the feature scores are multiplied together where each UI adaptation choice will get a score on suitability. Finally, the *score_matrix* will be returned to the *Adaptation Manager*. The *Adaptation Manager* will send a sorted version of the *score_matrix* to the *Interaction Manager* to adapt the UI layer.

The Interaction Manager is responsible for sending the output to the user or handling the input from the user. Depending on the type of adaptation (choice-based adaptive user interface (CAUI) or automatic adaptive user interface (AAUI)), *the Interaction Manager* constructs the output message. If it is CAUI, the *Interaction Manager* presents the choices as per the sorted order of the *score_matrix*. If it is AAUI, the *Interaction Manager* will pick the UI adaptation with the highest score and use that to interact with the user. In this scenario, the *Interaction Manager* uses the UI adaptation with the highest score (*smartwatch (GUI)* option) in the *score_matrix* to output the information. In my studies, I have pre-defined the type of adaptation to increase the user response to a wider range of scenarios. But when the PASHI framework is deployed, it can be part of the UI preference model where users can pick the type of adaptation depending on the context.

Finally, the *Interaction Manager* will incorporate the information from the service model, results from the *Privacy Manager* and the sorted *score_matrix* to drive the UI adaptation. The final result on the user device would have the information requested by the main user and an explanation of the possible privacy risk that was avoided as a means of giving the reason for the adaptation.

Smart home device / **[Index]/[Feature]**	**Smart Speaker [Audio]**	**Smart TV [GUI]**	**Smart Phone [GUI]**	**Smartwatch [GUI]**
[0]/[PRIVACY_RISK]	**0**	**0**	**1**	**1**
[1]/[IN_RANGE]	0	0	**1**	**1**
[3]/[CAPABILITY]	0	0	**1**	**1**
[3]/[PREFERENCE]	0	0	**1/3**	**½**
[4]/[USABILITY]	0	0	**4**	**6**
[5]/[TOTAL]	0	0	**1**	**3**
[6]/[UI_ID]	**1**	**2**	**4**	**4**

Table 5.3: Score Matrix

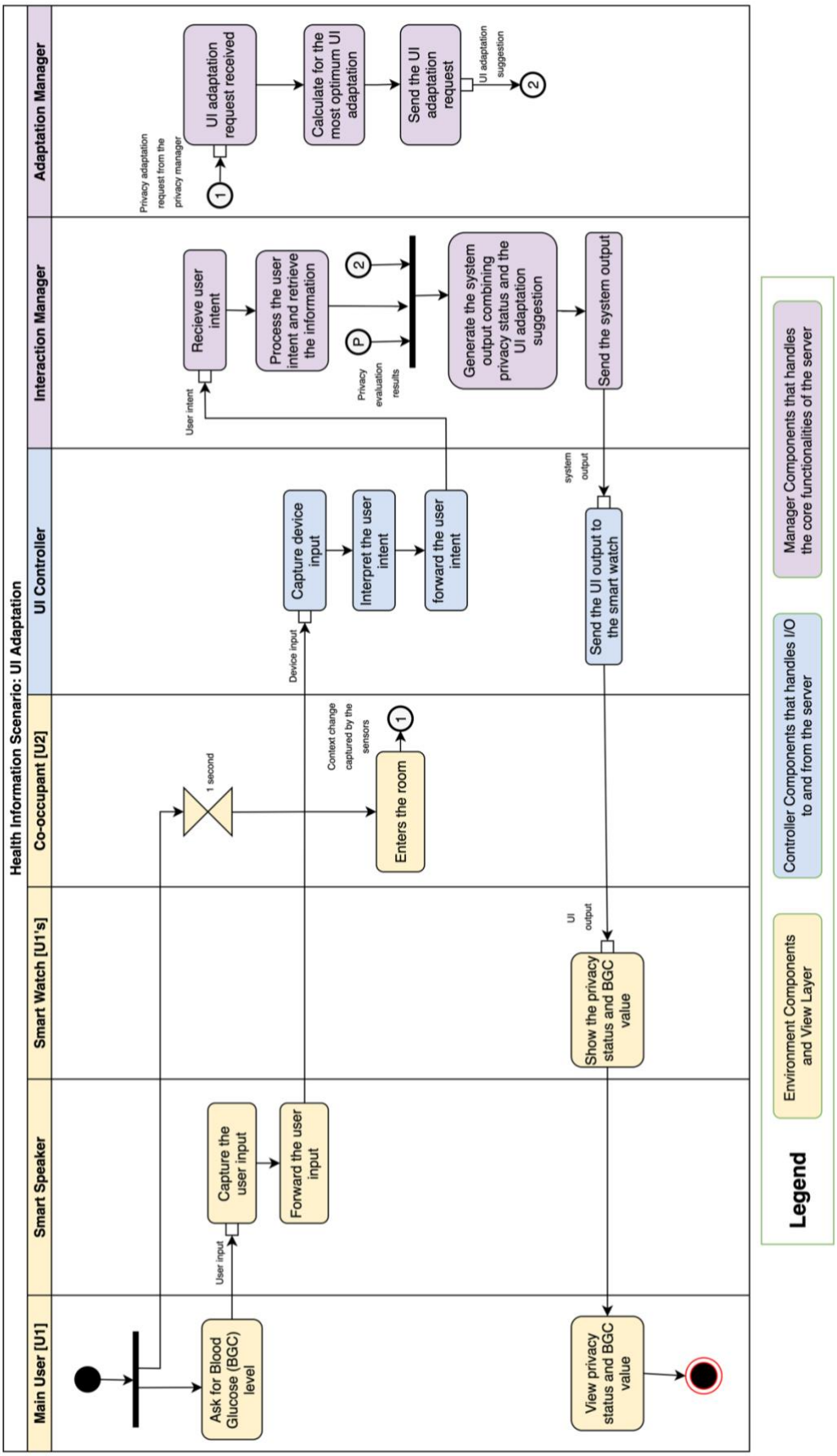

Figure 5.3: Activity Diagram for the UI Adaptation Process

```
Generate_UI_Adaptation (ui_list, user_id)
  COUNTER <- 0
  FEATURES <- 7 //Defines the number of rows in the matrix
  PRIVACY_PROTECTED <- 0 //Index of the row for privacy risk evaluation
  IN_RANGE <- 1 // Index of the row for in range score
  CAPABILITY <- 2 // Index of the row for user capability score
  PREFERENCE <- 3 // Index of the row for UI preference score
  USABILITY <- 4 // Index of the row for UI usability score
  TOTAL <- 5 // Index of the row for total score
  UI_ID <- 6 // Index of the row for UI ID
  score_matrix[length(ui_list)][FEATURES] <- 0//Adding individual scores
  FOR EACH uiid in ui_list
    if (NOT(privacy_risk_cache[ui_id + user_id]))
      score_matrix[PRIVACY_PROTECTED][COUNTER] <- 1
    else
      score_matrix[PRIVACY_PROTECTED][COUNTER] <- 0
      CONTINUE
    if (is_user_in_range(user_id, uiid))
      score_matrix[IN_RANGE][COUNTER] <- 1
    else
      score_matrix[IN_RANGE][COUNTER] <- 0
      CONTINUE
    if (capability_check(uiid, user_id))
      score_matrix[CAPABILITY][COUNTER] <- 1
    else
      score_matrix[CAPABILITY][COUNTER] <- 0
      CONTINUE
    score_matrix[PREFERENCE][COUNTER] <-
                    get_ui_preference_score(user_id, uiid)
    score_matrix[USABILITY][COUNTER] <-
                    get_usability_score(uiid)
    score_matrix[UIID][COUNTER] <- uiid
    COUNTER++

  //Calculating the scores
  FOR EACH uiid in ui_list
    score_matrix[TOTAL][uiid] <-
     (score_matrix[PRIVACY_PROTECTED][uiid]*
    score_matrix[IN_RANGE][uiid] * score_matrix[CAPABILITY][uiid] *
    score_matrix[PREFERENCE][uiid] * score_matrix[USABILITY][uiid])
  RETURN score_matrix
```

Listing 5.2: Adaptive-UI Generation Algorithm

The running time of the algorithm is established to be linear: O ($m + m + m$), where m = list of user interfaces that are available in the space. It is important to note that the *is_privacy_protected (uiid, user_id)* function call is of O (1) time complexity due to the earlier calculations made in the *Privacy Manager*.

This section presented the PASHI framework's user interface adaptation generation process. In doing so, the user interface adaptation algorithm (§5.4.2) was presented that would pick the most suitable adaptation based on the scoring criterion. The scoring criterion checks if the adaptation: 1) is privacy secure, 2) would reach the user, 3) is preferred by the user, 4) would match the user's capabilities, and 4) would improve or maintain the usability. Therefore, the PASHI framework's generated usable and appropriate privacy-aware user interface adaptations for the given scenario and for other scenarios of that nature.

The following section will present the usability study conducted to evaluate the adaptive user interfaces generated by the PASHI framework.

5.5 Usability Evaluation

Adaptive user interfaces (AUIs) have had mixed reactions in the past. An adaptive user interface's usability is negatively impacted by unclear mental models of the users, lack of control, unreliability and privacy concerns (Duarte, 2007). On the other hand, an adaptive user interface's usability is affected positively by flexibility, efficiency, stability, and the ability to meet user preferences. Due to this uncertainty regarding the usability of adaptive user interfaces, I was motivated to conduct a usability evaluation to understand the efficacy and usability of the AUI generated from the PASHI framework.

At this stage of the research, there were three main variations of adaptive user interfaces:

1) Automatic Adaptive User Interfaces (AAUI),
2) Choice-based Adaptive User Interfaces (CAUI), and
3) Non-Adaptive User Interfaces (NAUI).

With the AAUI, the user interface layer was automatically adapted if there was a possible privacy risk. In contrast to the AAUI, the CAUI provided the choices to the user to select the adaptation. The NAUI referred to the user interfaces without any type of adaptation. Apart from that, I was also exploring two variations of interpersonal privacy: 1) Information Privacy and 2) Physical Privacy. Therefore, I wanted to evaluate how users perceived these three types of user interface types when applied as a solution for the two varieties of interpersonal privacy violations.

The objective of this study was to determine whether adaptive user interfaces can preserve the interpersonal privacy of smart home users and whether adaptive user interfaces are more usable for the privacy preservation of smart homes users as opposed to non-adaptive user interfaces. I also wanted to investigate if the automatic adaptation of the user interface is preferred over choice-based user interface adaptation. The study was exploratory in nature and looked to gather insights for the user experience evaluation study (§6) which follows.

5.5.1 Methodology

This section presents the methodology used for the study where the Figure 5.4 provides an overview.

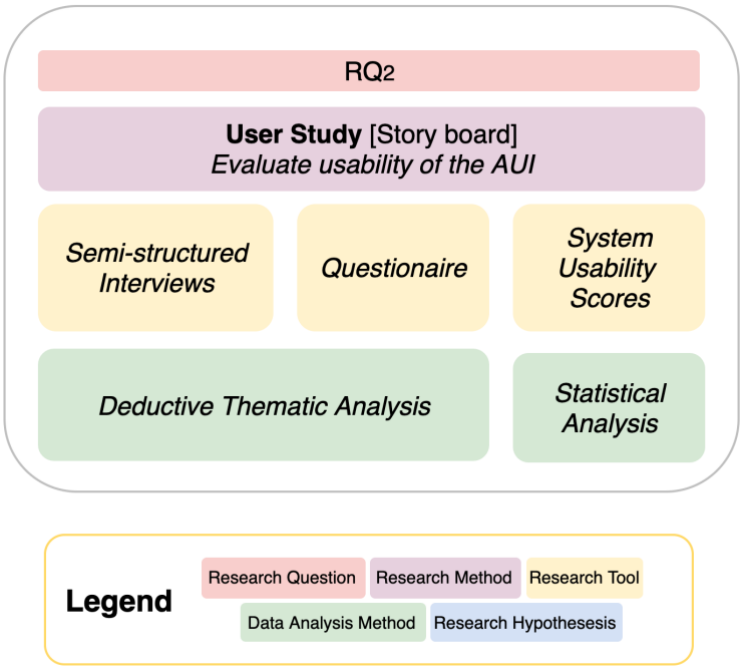

Figure 5.4: Methodology for Usability Evaluation Study

5.5.1.1 Ethics Approval

I obtained ethics approval from the Open University's Human Research Ethics Committee after providing the necessary documents (HREC/3417/Wijesundara). There were no health risks for the participants as the interview was done at a safe place (i.e., meeting room) without any health-hazardous tasks. The only participant identifying information was on the consent forms which were stored separately from the study data. The audio recordings of the post-study interview recordings of the study were stored with the participants' unique number on a secure password protected Open University server. The answers to the pre-study questionnaire and the post-study questionnaires were also stored online in a secure Open University Server. The participant consent has been acquired to keep the data (i.e., consent form answers, audio recordings, and questionnaire answers) for up to 5 years after the study. However, the data is scheduled to be deleted one year after thesis acceptance.

5.5.1.2 Participant identification and recruitment

Participants were recruited using word of mouth, posting on the Open University noticeboards, and snowball sampling. All the participants were adults with good conversational English skills where English did not have to be their first language. The study excluded any participants who were children, adults with cognitive impairments or any diminished capacity to consent.

5.5.1.3 Study preparation

Six storyboards were created using the tool: *storyboardthat* (https://www.storyboardthat.com/). The six storyboards were based on two base scenarios, where each base scenario generated three separate scenarios for each of the three user interface variations. The two base scenarios were previously described in Chapter 3 (§3.2.2**Error! Reference source not found.** & §**Error! Reference source not found.**) but are repeated below for ease of reference.

5.5.1.3.1 Background Information for the Scenarios

Sally is a 76-year-old woman who lives alone in her own smart home. She has a circle of support (Table 5.4) which is comprised of her adult son Zack and a caregiver Yasmin.

Name	Role/Relationship with respect to Sally
Yasmin	Caregiver
Zack	Son

Table 5.4: Sally's Circle of Support

Sally has a set of privacy preferences (Table 5.5). Sally does not share her personal health details with anyone other than her caregiver as she feels that other smart home users such as Zack would get annoyed with her if her health is not optimal. Sally is also an avid meditator, and she would not want to be disturbed while she is meditating. To avoid such situations, she has set privacy rules using the PASHI framework.

Name	Privacy preference(s)
Sally	Health data will only be shared with her caregiver. Does not want to get disturbed while meditating.

Table 5.5: Sally's Privacy Preferences

User	Task	User-interface preference(s)*
Yasmin	View health data	1. Smart speaker 2. Smart TV 3. Smart phone

Table 5.6:Yasmin's User Interface Preferences

Yasmin has a set of user interface preferences (Table 5.6). Yasmin prefers to use the smart speaker, smart TV, and smartwatch in that order to access Sally's health information. Note that in the previous example (§3.2**Error! Reference source not found.**), Yasmin's user interface preferences were provided as modality preference, wherein this case they were presented as smart home device preferences. Therefore, the two scenarios differ slightly.

5.5.1.3.2 Scenarios for the Storyboards

Table 5.7 shows the descriptions that were used to create the storyboards. The three user interface variations were:

i)*Automatic Adaptive User Interfaces (AAUI):* AAUI adapt the user interface automatically when there is a possible privacy violation.

ii) *Non-Adaptive User Interfaces (NAUI):* NAUI does not adapt the user interface when there is a possible privacy violation.

iii) *Choice-Based Adaptative User Interfaces (CAUI):* CAUI provides choices to the user to choose from when there is a possible privacy violation.

Figure 5.5 shows the storyboard of the meditation scenario in which the main user was provided choices from which to pick (CAUI version) when there is a possible privacy violation. Figure 5.6 shows the storyboard of the health information scenario in which the user interface was adapted automatically (AAUI version) when there is a possible privacy violation. The rest of the storyboards are provided in the Appendix (§10.3.1.3), and all the storyboards are available in a public dataset (Wijesundara, 2021b).

Base scenario	Base case description	AAUI description	NAUI description	CAUI description
Information leakage scenario with medical data	One day while Yasmin (caregiver) is taking vitals of Sally (care receiver) over the smart speaker in the living room, her son Zack enters the room. Sally's blood glucose levels	The smart home senses the arrival of Zack and pauses the broadcast of Sally's health data. The broadcast is then automatically switched to Yasmin's smart phone [video output].	There is no detection of Zack entering and the broadcast of Sally's blood glucose over the smart speaker continues and Zack hears Sally's sensitive information.	The smart home senses the arrival of Zack and pauses the broadcast of Sally's health data. The choice of switching the output devices used to broadcast information was given to Yasmin where she picks her smart phone screen to continue accessing

	have been increased.			Sally's blood glucose levels.
Disturbance scenario while meditating	One day while Sally (care receiver) is meditating in her room, her son Zack tries to play music on his smart speaker at a loud volume.	The smart home realises the privacy violation that is about to happen and restricts Zack from playing music loudly on his smart speaker. Music was automatically played in a lower volume, so it won't disturb his mother who was meditating.	The smart home is not aware of Sally's privacy preferences and lets Zack play his music loudly. Sally gets disturbed while meditating and gets upset with her son.	The smart home realises the privacy violation that is about to happen and gives an ordered set of options for Zack to change the output device for his music. Out of the list of choices, he picks up to reduce the volume of the smart speaker, so it won't disturb his mom in the other room.

Table 5.7: Storyboard Scenario Descriptions

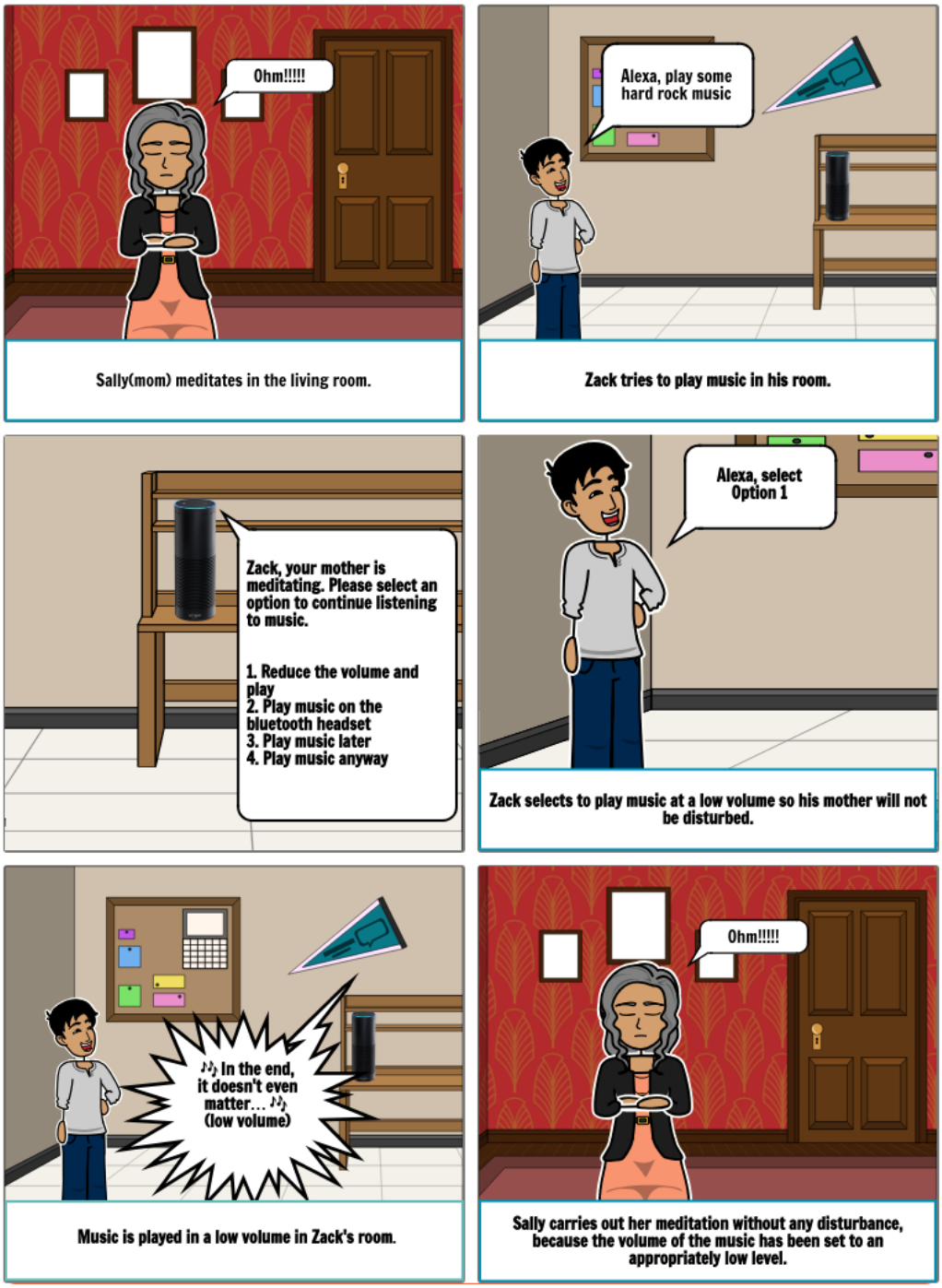

Figure 5.5: CAUI - Meditation Scenario

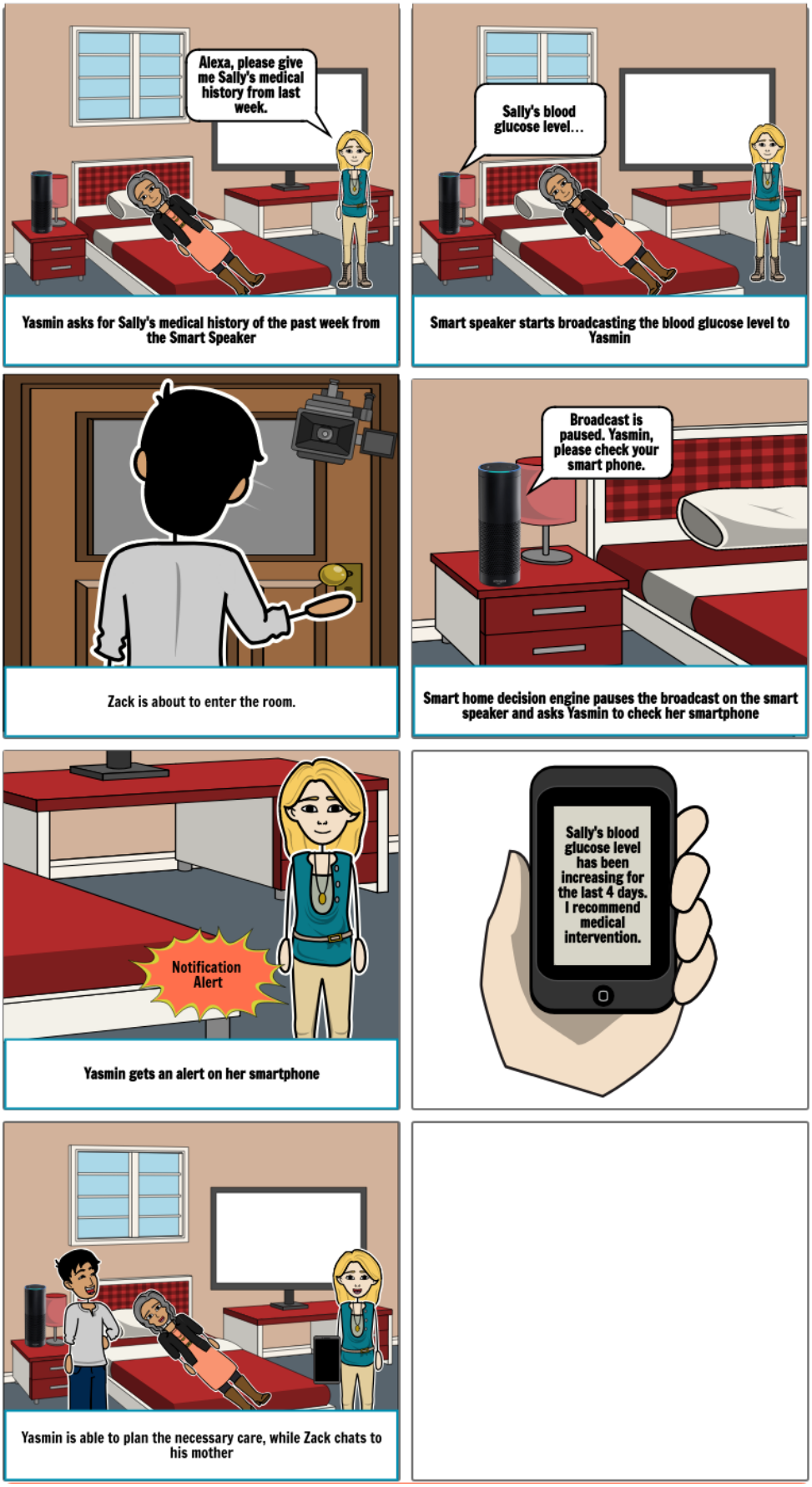

Figure 5.6: AAUI - Health Scenario

5.5.1.4 Study protocol

After receiving the participants' consent, I scheduled a session for each of them to come into the lab to complete the study. On the day of the study, I invited the participant to a meeting room where the participant was provided with a laptop with the online version of the study and an identical printed version of the study materials.

First, the participants were given the description of the experiment to understand the task they would be doing. Then they were presented with the printed version of the consent form to sign. After that, the participants were asked to fill in the pre-study questionnaire. Then they were asked to read the base-case scenario (Figure 10.1 in Appendix C: §10.3.1.3) which provided the background information of the scenario. After that, the participants were assigned randomly to a specific order of the six scenarios. These pre-ordered sets of the six scenarios were systematically ordered using a counter-balancing method to reduce the order effect.

After reviewing each scenario, the participants were asked to evaluate the user interfaces shown using the system usability scales (SUS) (Brooke, 1996) (§Table 5.8) and a questionnaire about their perception of how the system protected their privacy (§10.3.2.2). This questionnaire helped to understand the usability and privacy protective nature of the AUIs and this process was repeated for all the six scenarios. Finally, the participants completed a post-study questionnaire (§10.3.2.3) where they were asked about the overall usability of AUIs and possible other applications of AUIs in their day-to-day life. Then they were interviewed, inquiring about the reasoning behind the SUS ratings given to different AUIs and the answers to the post-study questionnaire. The interviews were recorded for further analysis. The entire process took approximately 45 minutes.

Pick a value from 1-5; 1 being strongly disagree and 5 being strongly agree.	
Question	Rating
I think that I would like to use this system frequently	
I found the system unnecessarily complex	
I thought the system was easy to use	
I think that I would need the support of a technical person to be able to use this system	
I found the various functions in this system were well integrated	
I thought there was too much inconsistency in this system	
I would imagine that most people would learn to use this system very quickly	
I found the system very cumbersome to use	
I felt very confident using the system	
I needed to learn a lot of things before I could get going with this system	

Table 5.8: System Usability Scale (SUS)

5.5.1.5 Data Collection

Multiple data points were collected via various tools to address the research questions. Quantitative data included: pre-study questionnaire quantitative answers, SUS scores given to each scenario, and post-study questionnaire quantitative answers. Qualitative data included: the pre-study questionnaire descriptive answers, post-study questionnaire descriptive answers, and audio recordings of the post-study semi-structured interviews.

5.5.1.6 Data Analysis

The interview data was analysed using thematic analysis based on Nielsen's 10 usability heuristics (2005) for deductive coding and theme identification. I created codes out of Nielsen's heuristics and tagged the interview data accordingly. Later I counted the occurrences to identify the key themes. Based on this analysis, 6 themes were identified: *visibility of system status, user control and freedom, consistency and standards, error prevention, flexibility and efficiency of use, aesthetic and minimalist design.* These findings were triangulated against the interview and written answers to test the findings.

ID	Age	Gender	smart home devices
PU1	36	F	Smart electricity meter
PU2	32	M	Mobile phone
PU3	38	F	Amazon echo
PU4	28	M	-
PU5	36	M	Google home
PU6	26	M	Amazon echo dot
PU7	36	M	Xiaomi Mi Band 4
PU8	36	M	iPhone, iPad
PU9	34	M	Amazon echo, Smart plug
PU10	40	M	-
PU11	27	M	-
PU12	30	M	-
PU13	29	F	Bluetooth speaker, Smart TV
PU14	30	M	Sonos one, Amazon Fire stick, Philips Hue, Smart Phone
PU15	32	F	Amazon echo

Table 5.9: Storyboard Study Demographics Data

5.5.2 Results

5.5.2.1 Participant Demographics

This section reports the demographic data of the storyboard study participants (summarised in Table 5.9**Error! Reference source not found.**). The average age of participants was 33 (SD 4.3) years, and there were 4 female participants and 11 male participants. 11/15 participants possessed at least one smart home device. The average age being 33 years could have slightly biased the results because participants may not have identified with Sally (who is an older adult), leading to them not fully considering her privacy preferences when responding to the scenarios. On the other hand, both users who experience the user interface adaptation in the scenarios, Zack and Yasmin, are depicted as younger adults of similar age to the study participants.

5.5.2.2 Quantitative Analysis

This section reports the analysis of the system usability scores (SUS) (Brooke, 1996). SUS score is a value between 0 and 100. A higher SUS scores indicates higher usability of the given product, in this case, the AUI variation for a given privacy type. Table 5.10 shows the average of SUS scores for each AUI variation when applied in different privacy contexts. Figure 5.7 aggregates the SUS score based on the AUI variation. The full list of SUS scores is provided in the Appendix (§10.3.3)

AUI type / Privacy Type	AAUI	CAUI	NAUI
Information Privacy	85.33	76	67
Physical Privacy	85.17	85.33	74

Table 5.10: Average SUS scores

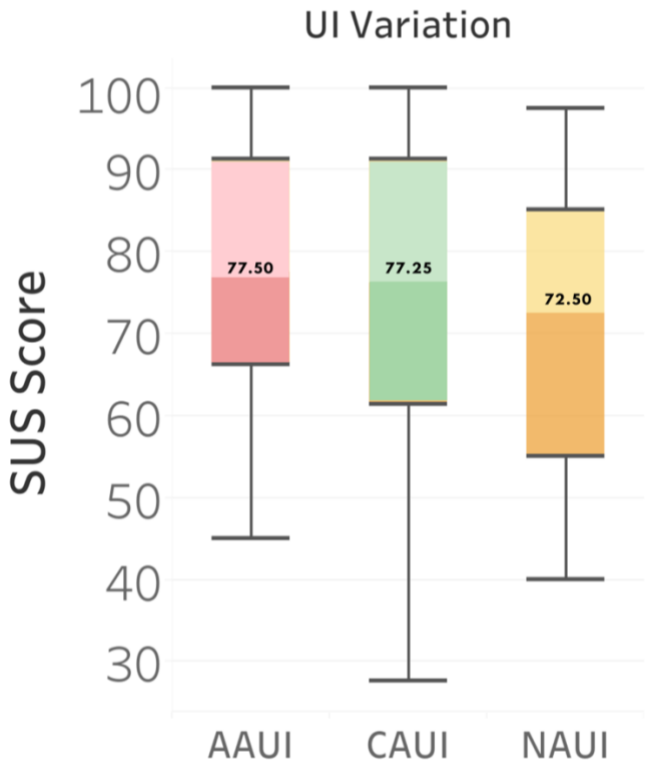

Figure 5.7: SUS-based Boxplot for the UI variations

5.5.2.3 Qualitative data

The following section reports participant comments in response to the user interface variations. As previously mentioned, the interview data was analysed using a deductive thematic analysis method based on Jakob Nielsen's 10 usability heuristics (2005), resulting in 6 themes being identified within the data-set: *visibility of system status, user control and freedom, consistency and standards, error prevention, flexibility and efficiency of use, aesthetic,* and *minimalist design.*

In the following sections, participants will be denoted by "PU" and their respective number. The index(s) of the exact quotations is also included using [] such that a quotation by participant 4 with the index of 13 would be PU4[13]. All of the interview transcripts are available in a public dataset (Wijesundara, 2021a).

5.5.2.3.1 Visibility of System Status

Visibility of system status is used to denote how each user interface type explained its internal status to the participants. Most of the participants highlighted how the CAUI made the smart home users aware in comparison to the NAUI and the AAUI. Four participants (PU3, PU4, PU6 and PU11) wished to have transparency and know why the adaptation happened. PU3 preferred to have the CAUI as it made the user-aware*: "In meditation scenario, I like the choice-based adaptation as Zack is aware of the reason for the reduction of volume.",* (PU3). PU6 explained how being unaware of the reason behind the adaptation could be unappealing in the AAUI: *"In automatic adaptation, I would like to have transparency why the adaptation happens. If my volume*

is lowered, Zack should know his mother is meditating.", (PU6[18]). PU15 felt more connected to the smart home as the CAUI explained the reason for the adaptation: *"Smart home is nice to give me the reason for the adaptation. I feel connected to the smart home as it is talking to me explaining the reason for the adaptation",* (PU15[16]).

5.5.2.3.2 User Control and Freedom

In this context, *user control and freedom* refer to the extent to which participants felt they had options to determine and control the nature of the interactions with different user interface variations. Four participants (PU2, PU6, PU7 and PU13) reported on the level of control that they felt while using the CAUI and the AAUI. PU2 thought the user was given the option to violate privacy if they wanted to: *"if one of the options can violate the privacy of the other person it will be a problem. again, it depends on human choice.",* (PU2). A couple of participants (PU2 and PU7) mentioned that they preferred the CAUI over the AAUI as it checked with the user before an adaptation: *"...I still prefer to be asked, so I prefer the choice-based adaptation.",* (PU7). PU13 preferred the AAUI over the CAUI even though the control was taken away due to its usability: *"I found automatic adaptation was much better in usability point of view compared to choice-based even though the control taken away from the user. It felt much more integrated.",* (PU13[14]). PU6 stated that the NAUI would not allow the user to control the interaction when it is in execution: *"I wish I had the option to say *shut up* to Alexa, so it would stop halfway, but I don't have that feature.",* (PU6[21]).

Lastly, PU6 and PU14 highlighted the importance of having control. PU6 thought the AUI should not be enforcing the user to take any action. *"There should be a way to always override the system. For example, If I want to disturb my mother, I should also have the option to override the system and play music loudly. It is a problem between people, you should be given the options and tools dealing with the Problem but not take a decision, they just should facilitate.",* (PU6[23, 24]

5.5.2.3.3 Flexibility and Efficiency of Use

In this context, *flexibility and efficiency of use* refers to how different user interface variations were able to make the interaction faster depending on the context and the user's needs. Furthermore, this section also covers participants' comments on design decisions that impacted the interaction. Two participants (PU1 and PU12) commented on the NAUI's usability. PU12 thought the NAUI was highly usable as it didn't require user input: *"Non adaptive UI had the highest usability, it was very easy. When there is less action required from the user, the usability is high."*, (PU12). Two participants (PU9 and PU14) thought the AUI was easier to use. PU14 reported that the AUI was doing a complex task for the user reducing the effort from the user's point of view: *"I generally thought it was easy to use and didn't require much effort, it did a lot of the work for you such as switching to different modalities"*. (PU14).

Most of the participants (PU3, PU5, PU6, PU12, PU14 and PU15) reported that the AAUI is efficient compared to CAUI. PU12 thought the CAUI having multiple layers made it complicated in comparison to the AAUI: *"In some scenarios choice-based adaptation was okay but some scenarios like adding multiple layers to the interaction made it not easy to use."*, (PU12). PU15 reported the CAUI could be time consuming in comparison to the AAUI due to human delay: *"I like the automatic adaptation, it is good, because people take time to react. When involving humans, you can't have that kind of speed."*, (PU15[13]). Lastly, PU5 mentioned his preference to have fewer components, hence appreciating the AAUI over the CAUI: *"It is like the saying "less is more". So, I don't like the choice-based adaptation as it makes things complicated."*, (PU5[18])

5.5.2.3.4 Error prevention

In this section, *error prevention* refers to how participants reported the AUIs as helping to protect privacy violations and other types of disputes among smart home users. This section also reports participants' suggestions on how to reduce errors or improve the AUI's performance.

All participants (N=15) stated that the AAUI and the CAUI could protect the privacy of smart home users. Some of the participants (PU2, PU3, PU4, PU6, PU8 and PU13) highlighted that the NAUIs were faulty and unable to preserve privacy. PU1 compared the NAUI and the AUI, consequently mentioned he would not be using the NAUI as it is not protecting privacy: *"privacy was preserved in the adaptive user interface scenario. Non adaptive user interface continued playing the conversation, so the system is faulty. I would not use the non-adaptive user interfaces as it broadcasts information without considering the privacy concerns of the user"*, (PU2[14,15]). Some of the participants (PU2, PU5, PU6, PU8, PU12 and PU15) commented on the AUI's privacy protection ability. PU2 highlighted that AUI was effective in privacy protection*: "Generally, it is a good addition to have privacy preserving capabilities in user interfaces. Privacy violating scenarios were fixed using adaptive user interfaces. They were much better usable systems."*, (PU2). PU8 explained the natural nature of the AUI's privacy protection approach: *"In a real-life scenario where there is a nurse or a doctor, if they hear or see someone else entering the room. They would stop mid-sentence to stop the privacy violation. It should happen with smart home user interfaces as well."*, (PU8[14]). A couple (PU3 and PU15) of participants highlighted automatic privacy protection of AUI: *"it didn't compromise any information. The usability was quite effective and convenient because everything was automated and the preferences of each was preserved"*, (PU3).

Two participants (PU6 and PU8) highlighted the possible after-effects of not protecting privacy. PU8 reported how the NAUI created family feuds: *"[NAUI] made family feuds because it was unable to preserve the privacy"*, (PU8[13]). PU6 thought the AUIs could avoid the unpleasant feuds between smart home users: *"Using adaptive user interfaces can avoid a lot of arguing between Zack and his mother"*, (PU6[14]).

Some of the participants (PU2, PU3, PU5, PU6 and PU10) suggested ways to improve the AUI. PU2 suggested to give choices in the CAUI a rating and sort them in the order of highest to the lowest in privacy violation probability: *"if you can provide multiple options, you can provide some prioritisation to say that one option has the highest priority which gives you the most efficient privacy maybe another one a little less privacy another one though"*, (PU2[22]). Three participants (PU3, PU5 and PU6) wished to have a default option in the CAUI: *"Having a default option in the choice-based adaptation is good"*, (PU6[13]). For the CAUI, PU6 suggested reminding the users of possible privacy violations incorporated with the choices: *"…it should remind the person using the UI that other person's privacy will be violated. Ask him "are you sure you want to do this?"*, (PU7[16]). PU10 thought it is better to remove privacy violating options from the choices: *"In choice-based systems, it is best to remove options which would violate the privacy of other people. It is okay to enough options as long as there are no privacy violating options"*, (PU10[15]).

5.5.2.3.5 Smart Home Privacy Violation Scenarios

This section summarises how participants reported their personal experiences regarding privacy violations when sharing smart home devices with co-occupants. As previously mentioned, the 6 types of privacy violations identified in Solove's taxonomy (Solove, 2002) were used in the analysis. Participants reported how different privacy dimensions – such as the right to be let alone, secrecy, control over personal information and personhood – were violated in their day-to-day activities.

Three participants (PU3, PU13 and PU14) described how sharing devices with the co-occupants can cause disturbances and inconveniences. PU13 found smart home heating to be a disturbance, as it is controlled by one person affecting all the participants: *"Heating levels can be a problem because it affects multiple people who are living in the smart home. When couples are living together, the husband would change the heating levels from outside the home to save money but if the wife is in the home and it is cold."* (P13[15,16]). PU14 thought listening to radio could disturb his partner: *"I literally was listening to music and so my wife has a radio and I have to control the volume and turn it up and down, […] it takes a while and because my wife's trying to listen to radio in the other room, so I think that's disturbing her personal space a little bit".* (PU14[22]). PU3's reported how her daughter disturbed her shopping experience accessing her shopping list via the smart speaker: *"I use Alexa to handle my shopping list, when my daughter comes she says add toys to the list Anybody in the house can change it. When we go shopping I can find random items which were put by other people.",* (PU3[8])

Most of the participants (PU3, PU4, PU5, PU6, PU8, PU9, PU10, PU11 and PU13) thought their personal information could be leaked via shared user interfaces. Two participants (PU3 and PU8) thought that their financial information could be leaked via shared user interfaces. PU3 mentioned

how she has logged in her credit card details to the smart speaker and highlighted its privacy implications: *"I access train booking via Alexa Skills. I have also added my credit card details to the payment option. It does not have any authentication, and anybody book tickets using my credit card. Kids, other family members and strangers can use this feature without my authorization…",* (PU3[9]). PU13 described how conference calls can leak conversation history: *"Areas where you use conferencing devices, it could break the privacy as it could show sensitive information and even show the last conversation the account used to have. This is a privacy violation. Even for devices like Portal where you can see the last calls that had been taken can be a privacy violation when the device is shared.",* (PU13[18]). PU5 found that there is the risk of his personal travel history being leaked to other users of the smart home: *"My travel information can be leaked to someone else who is using the system. One day I used Google maps to go to the supermarket and when I came home and asked Google Home to tell the weather, Google broadcasted the weather in the location of the supermarket.",* (PU5[27]). PU9 found it a violation of privacy when his Amazon order's delivery notification was read out by the smart speaker: *"Alexa, might allow other people to know what I ordered. And I don't want that to happen. Alexa also would notify me of deliveries. If I am ordering a surprise gift to my girlfriend, I don't want her to know that a delivery has come.",* (PU9[16]).

Four participants (PU5, PU9, PU12 and PU13) stated that their individuality as a person can be violated because of the smart home user interfaces. PU13 mentioned how their personal entertainment history can be leaked to other co-occupants via shared user interfaces: *"If I use Netflix or YouTube app on a smart TV, it would show the recent history and it would be annoying. If I share the smart TV in a dorm with other flat mates, it would be uncomfortable. It could be cumbersome as well, because if I have to log out all the time. And the usability goes down.",* (PU13[17]). Furthermore, PU12 was concerned about getting personal notifications on shared devices: *"Through a smart speaker as well as paired public screens I could get personal notifications and the system should be smart enough to avoid those kind of privacy violations.",* (PU12[17]).

5.5.3 Summary

This section presented a storyboard-based usability evaluation study and its findings. The storyboard study helped to further establish the appropriateness of the PASHI architecture to generate **usable** privacy-aware smart home user interface adaptations. The study used two privacy violating scenarios and three user interface variations (AAUI, CAUI, and NAUI) and found the following results:

- Participants preferred adaptive user interfaces (AAUI and CAUI) over NAUI for both the variations of privacy violating scenarios.

- Participants preferred AAUI over NAUI for the information privacy scenario and both the scenarios in aggregate.
- Participants slightly preferred CAUI over AAUI for the physical privacy violation scenario. This motivated a more focused study to evaluate user experience of these two AUI variations for different privacy variations.
- Apart from these, participants preferred to have the following qualities for AUI:
    a. More control and flexibility whenever possible,
    b. Visibility of the system status with explanations for adaptations,
    c. Reminding possible privacy violations before they happen.

5.6 Discussion

This chapter aimed to identify a suitable software architecture to support the generation of privacy-aware adaptive smart home user interfaces. This motivated **RQ2**: *"What is an appropriate software architecture for a privacy-aware adaptive smart home interface framework?*". It first presented the PASHI framework's software architecture and discussed its functionality. Then the chapter reported the usability study conducted to evaluate the adaptive user interfaces generated by the framework.

The PASHI framework's software architecture and algorithms adequately detected interpersonal privacy violations and generated usable user interface adaptations to mitigate them. This was demonstrated by evaluating the two key processes 1) privacy violation detection, and 2) user interface adaptation) for applicability and efficiency. The privacy violation detection process successfully detected the possible interpersonal information privacy violation where the algorithm proved to have polynomial time complexity. The user interface adaptation process generated usable user interface adaptation to mitigate the identified violations where the algorithm proved to have linear time complexity. Explaining how the PASHI framework functions, the full information flow of the health information scenario is presented in Figure 5.8.

The PASHI framework's ability to detect and mitigate interpersonal privacy violations addressed a gap in the existing smart home user interface framework literature. None of the existing frameworks discussed in the literature review (§2.2.2) provided means to detect interpersonal privacy violations nor generated user interface adaptations to mitigate the identified potential violations. The case study used a single case (information privacy violation) and the way interpersonal privacy is modelled in the PASHI framework (role-based access control mechanism) helped to extend the findings to interpersonal physical privacy scenarios and to other interpersonal privacy scenarios. However, this needs to be further investigated to better evaluate the completeness and the generalisability of the PASHI framework's applicability. In addition, some of

the PASHI framework's (Figure 5.1) components (e.g.: service model, capability model, and sensor controller) were not presented in this research as it was out of the scope of this work. Therefore, to improve the framework and to deploy it in the wild these components should be developed and evaluated as further studies.

The efficiency of the privacy violation detection algorithm and the user interface adaptation algorithm was sufficient for the scalability within a smart home setting. The privacy violation detection algorithm's polynomial time complexity had minimal impact on the PASHI framework's efficiency as the number of smart home devices and smart home users is unlikely to exceed 100. The user interface adaptation algorithm was found to be capable of generating results in linear time; hence it is efficiently scalable if the need arises. However, the case study did not test the algorithms for their completeness, and this motivates further studies.

The usability evaluation study was part of answering the PASHI framework's adequacy to generate usable privacy-aware adaptive user interfaces. The study findings demonstrated that user's experience of the AUI goes beyond the usability aspect of the AUI. In addition, the usability evaluation study was limited to two scenarios in conjunction with three variations of the AUI (one being non-adaptive). Even though the study highlighted interesting findings such as the user preferences for different types of AUI variations in different contexts, it highlighted the need for a more in-depth evaluation. Therefore, a user experience study was conducted with an increased number of different interpersonal privacy violating scenarios, user interfaces, user interface and privacy preferences, and smart home contexts. The findings related to the usability evaluation study and user experience study presented in Chapter 6 will be presented and discussed in Chapter 0.

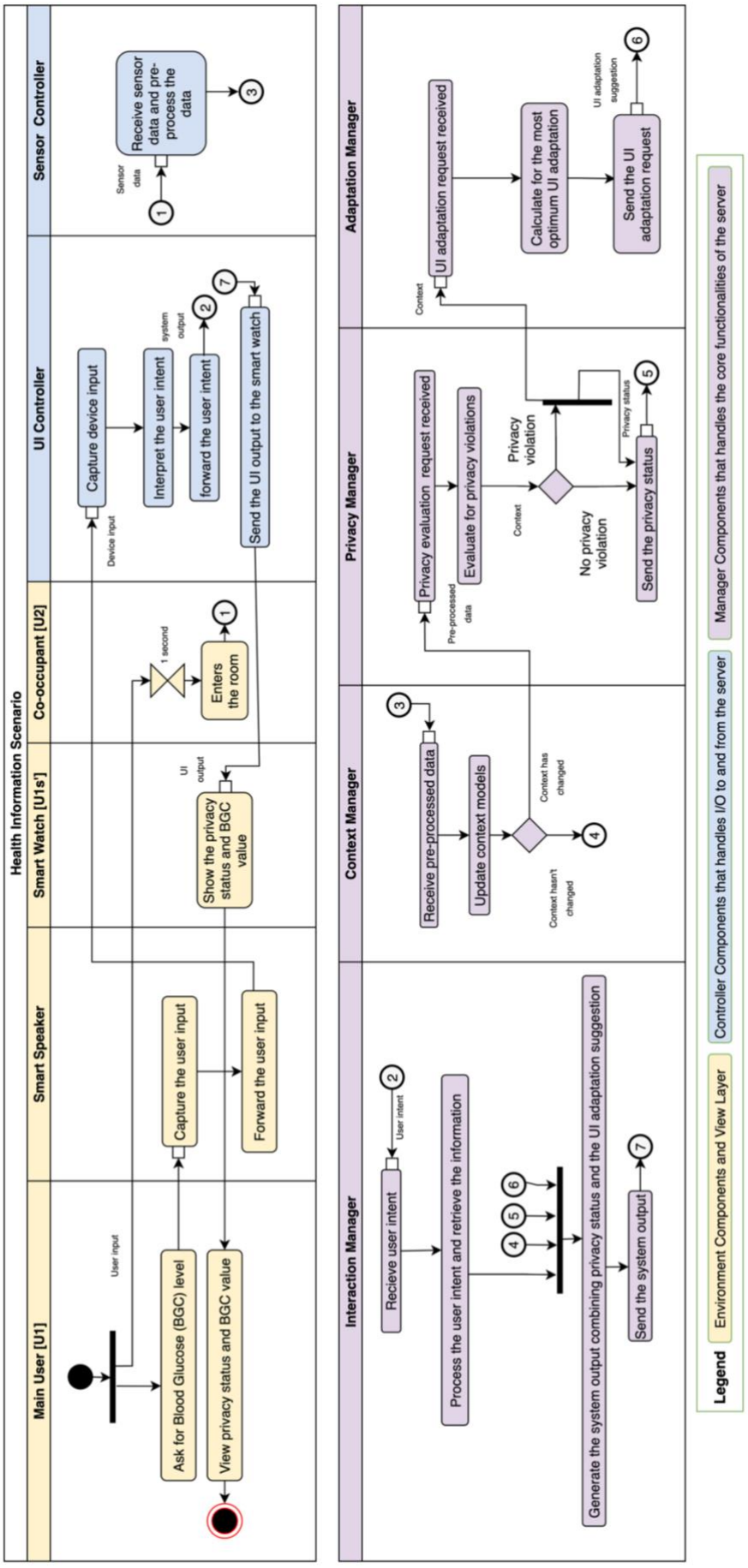

Figure 5.8: Activity Diagram for The Complete Interaction

5.7 Summary

The PASHI framework demonstrated the ability to adequately generate privacy-aware adaptive smart home user interfaces. Software architecture and the algorithms proved to be scalable without any major problems within a smart home setting. However, to address the limitations of the PASHI framework and this case study, the following recommendations can be made:

- Further studies should be conducted to evaluate the completeness and the generalisability of the PASHI framework's software architecture and algorithms.
- Components that were not presented in the PASHI framework – such as the service model, capability model and the sensor controller should be developed and evaluated in future studies.

The chapter also presented the storyboard-based usability evaluation study and its findings. The study evaluated three user interface variations (AAUI, CAUI, and NAUI) when applied for the two variations of privacy violations (information and physical). As discussed in the previous section (§5.6), this study motivated further in-depth evaluation of the AUI's experience. Therefore, the user experience study that was conducted will be presented in the next chapter (§6).

6. User Experience Evaluation

The knowledge representation models, combined with the software architecture and algorithms of the PASHI framework have demonstrated the capability and *usability* of AUIs for managing interpersonal privacy. As the next step of the evaluation, this chapter reports on the user study conducted to evaluate the *user experience* of the AUIs. It begins with an introduction discussing the aims and objectives of the study, followed by a report on the study protocol discussing how the study was conducted, how the data was collected, and how the data was analysed. The chapter concludes with a report on the findings and a summary of the chapter.

6.1 Introduction

User experience evaluation is crucial to measure the success of a user facing system. McCarthy and Wright (2004) highlighted the importance of evaluating the user experience of a system. They discussed how one lives with technology and our evaluation of technology systems should go beyond usability evaluation.

Existing smart home related adaptive UI frameworks have not explored the user experience of those systems. Blumendorf (2009) conducted a usability evaluation of the MASP framework. Loitsch et al. (2017) have evaluated GPII by conducting heuristic evaluation with the help of experts. Cronel et al. (2019) have not conducted a usability evaluation rather conducted a real-world case study. Therefore, there is a gap in research for evaluating the user experience of adaptive UI frameworks. RQ3 was formulated to address this gap and to evaluate the user experience of the PASHI framework.

RQ3: *What is the user experience of privacy-aware adaptive user interfaces?*

As discussed in Chapter 3, addressing **RQ3** would help to evaluate the user experience of privacy-aware AUIs. To collect the data required to address **RQ3**, I conducted a user study based on point-of-view video simulations. These videos showcased possible privacy violating scenarios and the interventions made by the PASHI framework generated by the AUI. This chapter reports on how the user study was conducted and its findings. Chapter 0 will discuss these findings along with the storyboard-based user study reported in Chapter 5.

6.2 Methodology

Chapter 3 established that a mixed-methods research approach would improve the accuracy of the results through triangulation and justified the utilisation of a video prototype-based user study to generate user feedback in order to answer **RQ3**. As shown in Figure 6.1, data was collected via three research tools: semi-structured interviews (qualitative data), reaction cards (quantitative data), and questionnaires (quantitative data). Inductive thematic analysis was used to analyse the semi-structured interview answers, frequency analysis to analyse reaction cards answers, and statistical analysis to analyse questionnaire answers. The data collection mechanisms will be further discussed in section §6.2.4 and data analysis mechanisms in section §6.2.5.

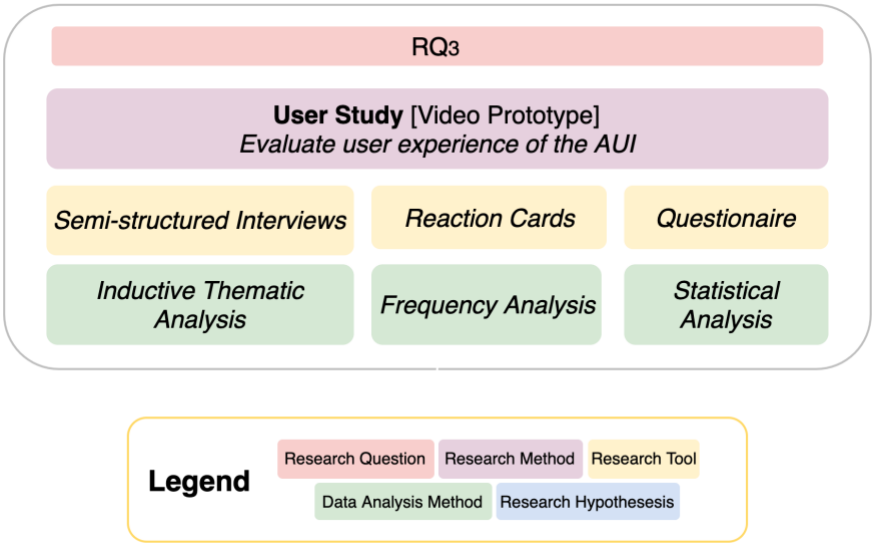

Figure 6.1: Methodology of the UX User Study

6.2.1 Implementation

Video prototypes were created depicting different privacy violating scenarios along with solutions provided by an AUI. It is important to note that the original plan was to conduct a lab-based user study, but due to the COVID-19 pandemic, it was necessary to alter the research methodology to one that could be operationalised with participants who were in physically different locations.

The scenarios were presented as video prototypes where each video had the following structure:

1. User preferences of the stakeholders in the video were presented.
2. The possible privacy violation which is about to happen was shown (only up to the point where the privacy violation is about to happen but not the privacy violation).
3. Finally, the user interface adaptation was shown where it used to avoid or minimise the privacy violation while maintaining the usability of the smart home.

Screenshots of two of these videos are shown in Figure 6.2 and Figure 6.3. Table 6.1 consists of 10 scenarios that could happen in a standard smart home setting with co-occupants (e.g., family members, flatmates etc.) and the videos are shown from the point of view of the person who experiences the system. The example scenarios described below were designed to cover 5 interaction channels: audio output, video output, gesture input, video input and audio input. For each interaction channel type there are two possible privacy violation examples where one is a *physical privacy violation*) and the other is an *information privacy violation.* However, the example where a gesture input causing *physical privacy violations* was omitted as such scenarios seem to have less impact on privacy and highly unlikely.

Each row shows a scenario that starts with the *user preferences* of the actors in the scenario, followed by the *possible privacy violation scenario* and lastly the *user interface adaptation solution* which is used to avoid the possible privacy violation. In the first column, I have also provided a three-letter tag created for each scenario, which I use to refer to the scenario across the chapter. Figure 6.2 provides screen shots from the *Meditation Scenario* (MED) and Figure 6.3 provides screenshots from the *Health Information Scenario* (HLT). All the video prototypes are available in a public dataset (Wijesundara, 2021d).

The videos were recorded using an iPhone 6S Plus Camera mounted on a tripod to simulate a first person view of the interaction. This allowed participants to have a more realistic experience of the smart home. User interface adaptations were generated in real-time via a Python based implementation of the PASHI-framework where the context changes of the smart home (e.g.: user identification) were driven by a web-based controller that simulated the sensor inputs. Apart from this, the adaptations relating to the video conferencing scenarios (SFE and FND) were added during the video editing stage.

Scenario name and [Tag]	**Interaction channel and privacy violation type**	**User preferences (Privacy and user interface)**	**Possible privacy violating incident**	**User interface adaptation solution**
Meditation Scenario [MED]	*Audio-output Disturbance*	Your co-occupant does not like to get disturbed while they are meditating.	You try to play music loudly via your smart speaker while the co-occupant is meditating.	The smart speaker automatically plays the music at a low volume while providing the reason for the adaptation on your phone. You are also given a set of alternatives to play music. You pick the Bluetooth headset option to play music.

Scenario name and [Tag]	Interaction channel and privacy violation type	User preferences (Privacy and user interface)	Possible privacy violating incident	User interface adaptation solution
Health Information Scenario [HLT]	*Audio-output Information Disclosure*	You do not like to share your health data with anyone. Your most preferred user interface choice is the smart speaker and then your smartphone.	You try to access your health data via the smart speaker. At this moment a co-occupant who is not authorized to listen to that information comes into the room.	The health information stream is diverted to your smartphone while letting you know the possible privacy violation that was avoided.
Slide Scenario [SLD]	*Video-output Disturbance*	Co-occupant does not like to get distracted while studying. You prefer the smart TV, then you would prefer your smart tablet to view photos.	You are about to go through your holiday photos on the smart TV while the co-occupant was studying in the living room.	When you try to view the photos on the Smart TV, a notification pops up about the possible privacy violation that is about to happen and guides you to use your tablet.
Netflix scenario [NFX]	*Video-output Information Disclosure*	You do not like to share your Netflix view history with anyone else at home.	You are viewing your Netflix account on the Smart TV. There are suggestions generated based on your view history. Then a co-occupant enters the room.	Smart TV adapted the sensitive sections by filling it with non-sensitive movie suggestions when the co-occupant came into the room.
Open Sesame Scenario [OPN]	*Gesture-input Information Disclosure*	you would not want anyone to access your secret cupboard other than yourself.	your secret cupboard door can only be opened by a specific secret gesture. One day you are about to open the cupboard while a co-occupant came into the room.	Smart home ignores the gesture knowing the co-occupant is in the vicinity and sends a message to your smartwatch with the reason for ignoring the gesture.
Friend Scenario [FND]	*Video-input Disturbance*	Your friend's co-occupant does not like to get disturbed by others when they are home on a weekend.	You speak to your friend via a video call. When you are on the video call, his co-occupant (who is also a mutual friend of yours) was about to walk across the camera's view.	When your friend's co-occupant was about to walk across, the background was blurred in the video call. This avoided an unnecessary conversation that the co-occupant might have had to have with you.

Scenario name and [Tag]	Interaction channel and privacy violation type	User preferences (Privacy and user interface)	Possible privacy violating incident	User interface adaptation solution
Safe Scenario [SFE]	*Video-input Information Disclosure*	Your friend's co-occupant does not want anyone to know the passcode to their safe.	You were on a call with your friend. While you were on a video call, his co-occupant was about to open the safe. The safe was in the vicinity of the video call.	The background of the video call was blurred covering the pin code of the safe.
Football Scenario [FBL]	*Audio-input Disturbance*	The co-occupant does not like to get disturbed while they are studying You like to use a smart speaker to get sports updates, if it is not possible, you would your smart phone.	You try to check the sports news on the smart speaker when the co-occupant was studying in the room.	When you asked the smart speaker for sports news, the smart speaker reminded you that your co-occupant was studying and guided you to use the smartphone. The smart home also explained the reason for the adaptation.
Bank Scenario [BNK]	*Audio-input Information Disclosure*	You would not share your bank passcode with anyone.	There is a smart speaker skill to log in to your bank account. When you initiated the smart speaker skill for the bank feature, a co-occupant entered the room.	Smart home did not prompt you for the passcode over the smart speaker, instead sent a message to your smart phone with the bank account control. The smart home also explained the possible privacy violation that was avoided.

Table 6.1: Video Prototype Scenarios

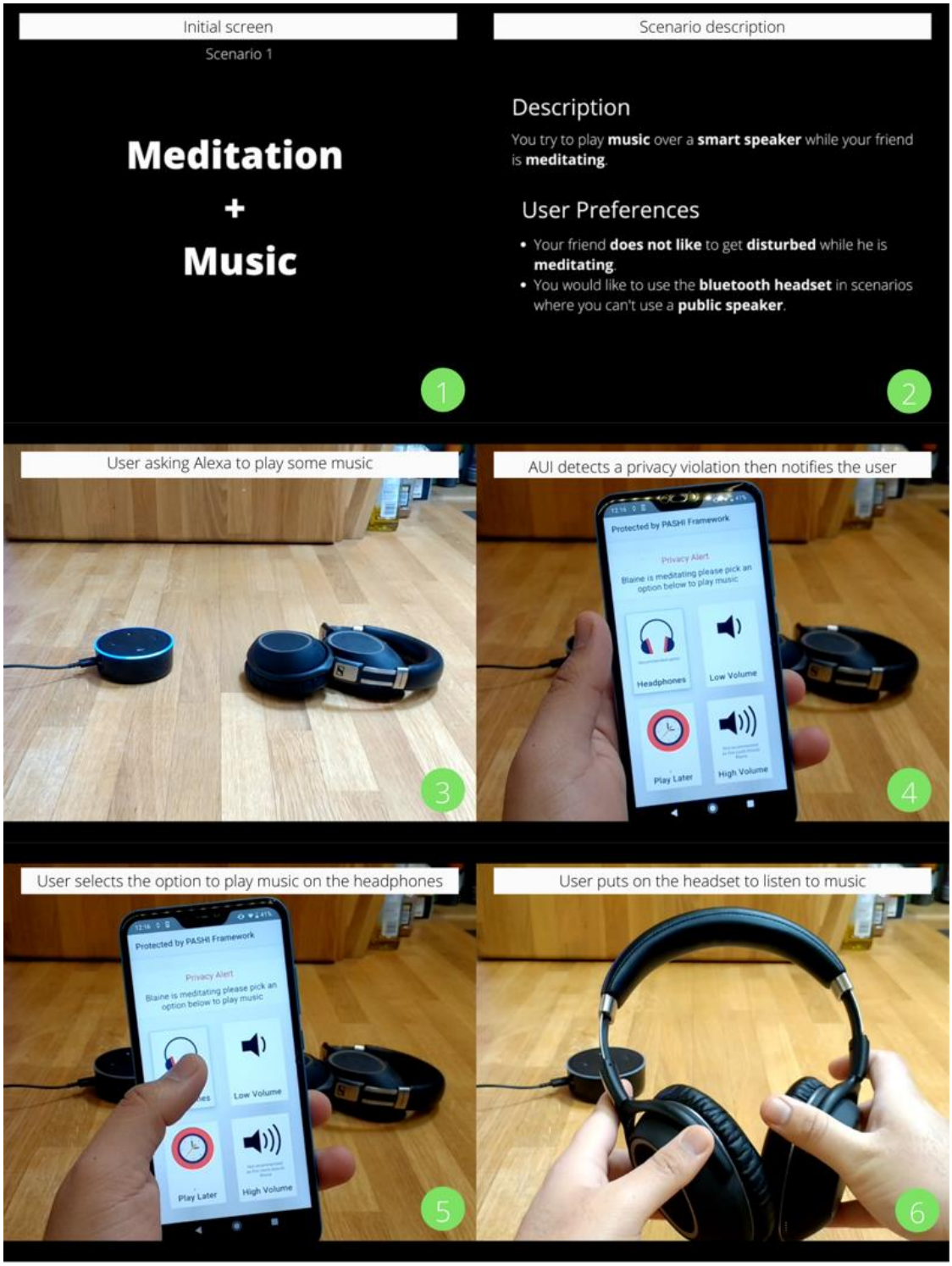

Figure 6.2: Physical Privacy Example (Meditation Scenario)

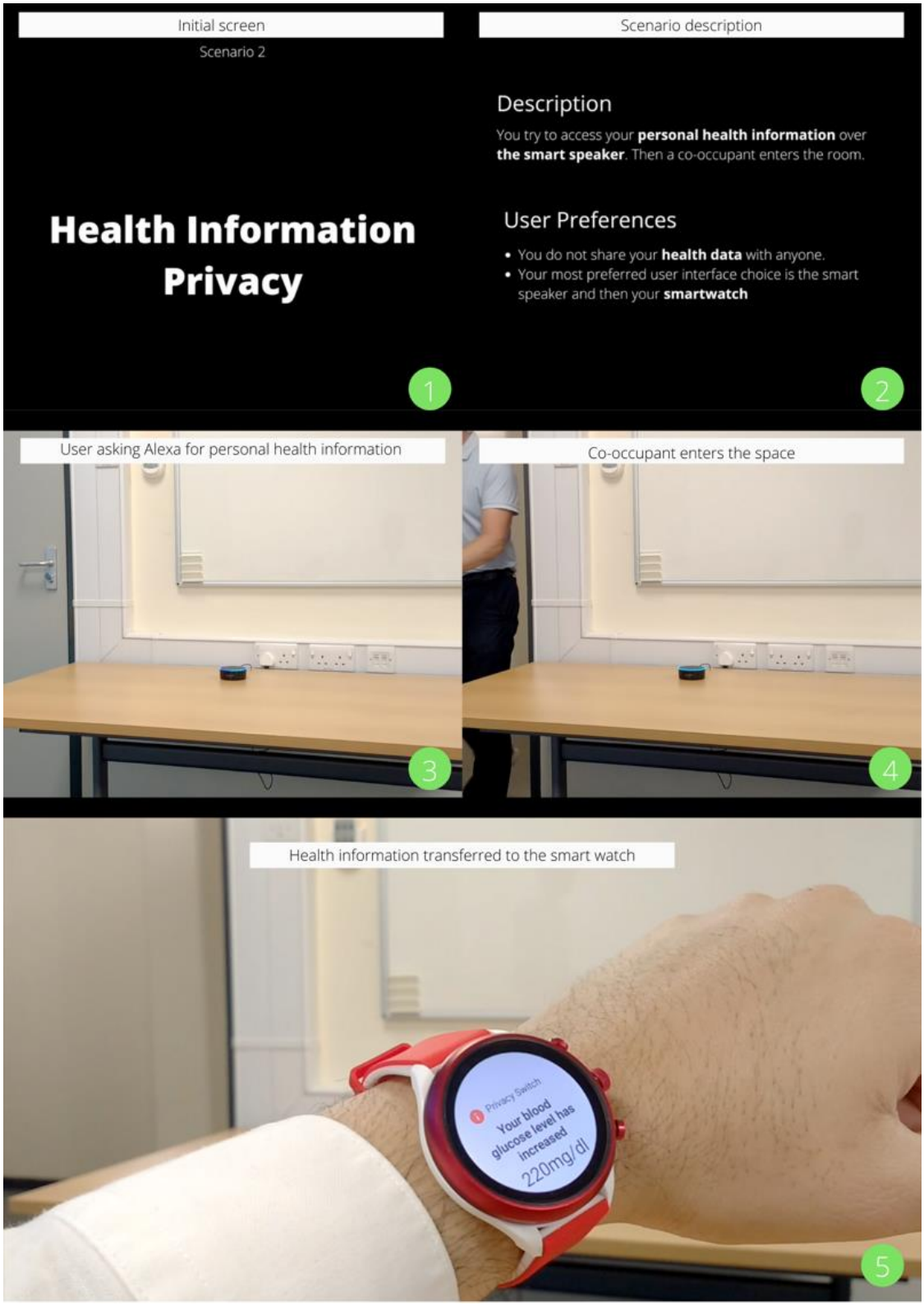

Figure 6.3: Information Privacy Example (Health Scenario)

6.2.2 Ethics Approval

I obtained ethics approval from the Open University's Human Research Ethics Committee after providing the necessary documents (HREC/3588/Wijesundara). There were no health risks for the participants as the interview was done via Skype. The only participant identifying information was on the consent forms which were stored separately from the study data. The audio recordings of the

post-study interview recordings were stored with the participants' unique number on a secure password protected Open University server. The answers to the pre-study questionnaire and the post-study questionnaires were also stored online in a secure Open University Server. The participant consent has been acquired to keep the data (i.e., consent form answers, audio recordings, and questionnaire answers) for up to 5 years after the study. However, the data is scheduled to be deleted after a year of thesis acceptance.

6.2.3 Study Protocol

Participants were recruited via online media such as mailing lists, LinkedIn, and Twitter. A total of 24 participants signed up and 23 participants participated in the study as one of the participants was not responsive after signing up to the study. All the participants were adults and had good conversational English skills (although English was not necessarily their first language).

The study was conducted online via Skype. Before the day of the study, the participants were sent an email with the description of the experiment to understand the task they would be doing (Appendix D: §10.4.1.2), if they agreed to do the study, they were presented with consent forms (Appendix D: §10.4.1.1) to digitally sign. After that, they were scheduled for the study.

Out of the 9 videos, sets of 6 videos were selected in a systematic manner where each video was seen by an equal number of participants ±1. Out of the 6 videos in a set, 3 videos represented interpersonal information privacy violation scenarios and the other 3 represented interpersonal physical privacy violation scenarios. From each set, 1 information privacy violation scenario and 1 physical privacy violation scenario were chosen as priming videos. The remaining 4 videos were selected as the main videos where they were used during the study. 24 hours prior to the time of the study, the participants were sent the 2 priming videos to view, helping them to have a fresh perspective of the two privacy variations and the nature of AUI. Along with these videos, they were provided with a pre-study questionnaire (Appendix D: §10.4.2.1) which asked them to score the level of concern they had for each type of privacy violation (physical privacy and information privacy). It is important to highlight that the priming videos are different from the main videos shown during the study.

In each set of main videos, I also systematically rotated the order in which the videos were presented within a unit (i.e., a set of four videos comprising two pairs of videos covering different types of interpersonal privacy) to reduce the learning and order effects. During the study, the participants were randomly assigned to one of these units.

On the day of the study, I connected with the participants via a Skype call. They were first greeted and provided with the instructions needed to participate in the study via a Google Doc. The Google

Doc contained the links to the four video simulations, places to answer the questionnaires and a place to pick the reaction cards (Appendix D: §10.4.2.2). I guided the participant through each scenario where I observed how they answered the questionnaire and how they picked the reaction cards. Participants were instructed to imagine they were experiencing the scenario themselves and answer the questionnaires accordingly. I encouraged the participants to think out loud when they answered a specific question or picked a specific reaction card. At the end of each scenario, I asked each participant to answer why they picked the reaction cards they selected. I also asked follow-up questions on the answers they gave to questionnaires to understand their reasoning. Finally, I inquired about their overall experience of the AUI using a post-study questionnaire (Appendix D: §10.4.2.3).

6.2.4 Data Collection

As reported earlier in this section both qualitative and quantitative data was collected. The quantitative data included pre-study questionnaire answers, post scenario questionnaire answers and the selected list of reaction cards. The qualitative data was the recording of the interview. In the interview, I collected participants think out aloud data, follow up question answers and the final post-study interview answers. The following section discusses the data analysis methodology.

6.2.5 Data Analysis

The selection of data analysis tools (inductive thematic analysis, frequency analysis and statistical analysis) was justified in chapter 3. This section discusses McCarthy and Wright (2004) approach to evaluating user experience of technology which was used to help analyse qualitative data and to synthesise themes related to the user experience of AUI. Their framework consists of two parts. The first part helped to analyse the qualitative data focusing on *four threads of experience.* The second part helped in *making sense of experience* via synthesising the findings under the six user experience dimensions.

The four threads of experience provided angles to look at the user experience when analysing the interview data. 1) *The compositional thread* referred to the structural aspect of user experience. It could be the narrative structure of the interaction, possible action sequence, consequences of an action or explanations provides for an action. 2) *The emotional thread* referred to the emotions that were generated during the interaction. These emotions could be positive emotions such as joy, satisfaction, or negative emotions such as anger and frustration. 3). *The sensual thread* referred to the user experience related to the *look and feel* of the interaction. This thread captured the immediate reactions of the user to an interaction. 4) *The spatio-temporal thread* captured the user experience that is entangled with space and time. This thread analysed how user perceives space and time during an interaction. These four threads were not mutually exclusive and only provided a way to look at the user data from different angles. After analysing the qualitative data using these

four threads, the second part of McCarthy and Wright's (2004) framework was used to synthesise themes.

McCarthy and Wright divided user experience into six parts:

1. *Anticipation* referred to the expectations that the user might have before the interaction.
2. *Connection* referred to the first moment that the user interacts with the system and the immediate experience they might have.
3. *Interpreting* referred to the experience that the user will have during the interaction.
4. *Reflecting* referred to the user's thoughts that arise immediately after the interaction.
5. *Appropriating* referred to the experience impacting the user's daily life where they would make changes to their life due to that experience.
6. *Recounting* referred to users taking the experience beyond themselves and recommending it to others. *Recounting* also captured user comments regarding how to improve the experience.

Apart from McCarthy and Wright's six themes in making sense of experience, user comments were analysed to assess the *success of the study* and *threats to validity*. Quantitative data analysis methods are discussed in their respective sections (§6.3.2). The following sections report the findings.

6.3 Results

This section provides the results of the video prototype study. First, it provides the participant demographics, then it reports the quantitative data findings and finally the qualitative data findings. In the following sections, participants will be denoted by "PX" and their respective number. The index(s) of the exact quotations is also included using [] such that a quotation by participant 4 with the index of 13 would be PX4[13].

6.3.1 Participant Demographics

Table 6.2 shows the participant demographics data of the video-protype study. The average age of a participant was 36 years (N=23) with 5 female participants and 18 male participants. Most (15/23) participants had at least one smart home device. For the questions regarding the level of concern towards the two variations of privacy violations, there was a mode of 4 for information privacy and there was a mode of 2 for physical privacy. Similar to the previous study, the average age being 36 years could have slightly biased the results to capture the user experience of a younger audience. However, this would not have much of an impact on the results when compared to the previous study (§5.5) as the scenarios in this study are not focused on a specific age group.

6.3.2 Quantitative Analysis

To help analyse the data efficiently, the scenarios were categorised into 6 categories as depicted in Table 6.3. The AUI category aggregated all the scenarios. Fully automatic AUI represented scenarios where the adaptation happened automatically without the intervention of the user. Choice-based AUI (CAUI) represented the scenario where the user was given a set of choices for the adaption. Semi-automatic AUI represented scenarios where the adaptation was automatic but was not executed until the main user accepted the suggested adaptation. Information privacy scenarios represented the scenarios that had an information privacy violation and physical privacy violation scenarios represented the scenarios which has physical privacy violation. These categories will be used in the reporting of the findings.

Participant ID	Age	Gender	Smart home devices that the participant using	Information Privacy	Physical Privacy
PX1	34	Female	None	4	4
PX2	33	Male	None	4	2
PX3	28	Male	Amazon Echo, Smart TV, Ikea smart led lights	4	2
PX4	37	Male	None	5	2
PX5	30	Female	Google home, Smart TV	2	4
PX6	34	Male	Amazon Echo, Smart Tv	4	2
PX7	31	Male	Alexa speaker (Sonos One), Phillips Hue	2	2
PX8	26	Male	Google's smartphone assistant (OK Google)	4	2
PX9	28	Male	Amazon Echo dot, Amazon smart plug, Smart TV, Smart phones, Smartwatch	1	5
PX10	52	Male	None	2	2
PX11	41	Male	Amazon Echo, Smart TVs, Smart plugs, Smart bulbs, Amazon Firestick TV	2	1
PX12	49	Male	Digital radio	4	4
PX13	54	Female	Smart TV	5	5
PX14	56	Male	Wink hub, Smart things hub, R-Pi gateway, Echo x8, Google x2, Nest, Ring, automated lights, Sprinkler, Window blinds, water Shutoffs, Gas meters, Weather station, etc.	2	4
PX15	34	Male	Smart TV, WIFI enabled camera installed in parent's home	4	4
PX16	29	Male	None	2	2
PX17	45	Male	Amazon Echo, Amazon Smart Plug, Alexa on Android Phone, Google voice search on android phone, and android tablet. Bluetooth Speaker	3	2
PX18	29	Male	None	5	4
PX19	41	Female	None	3	3

PX20	-	-	-	-	-
PX21	28	Male	Air things, Wave Devices	5	3
PX22	-	Female	None	3	1
PX23	22	Male	Smart TV	4	5
PX24	-	Male	Apple watch	1	2

Table 6.2: Video Prototype Study Participant Demographics Data

Type	**Scenarios**
AUI	All the scenarios
Fully automatic AUI	SFE, NFX, HLT, OPN, FND, BNK
Choice-based AUI	MED
Semi-automatic AUI	SLD, FBL
Information privacy scenarios	SFE, NFX, HLT, OPN, BNK
Physical privacy scenarios	FND, MED, SLD, FBL

Table 6.3: Scenario Categorisation

6.3.2.1 Reaction card frequency

Microsoft reaction cards – reduced version (Benedek and Miner, 2002) were used to capture participants reactions for different scenarios. The following section shows the summary of those reactions. Figure 6.4 shows the colour scheme used to categorise the reaction cards in this section and the following section. In each category, the bottom 10% of the reactions were omitted using the frequency of occurrence as a measurement to get the most used reactions.

Figure 6.4: Legend for Reaction Cards

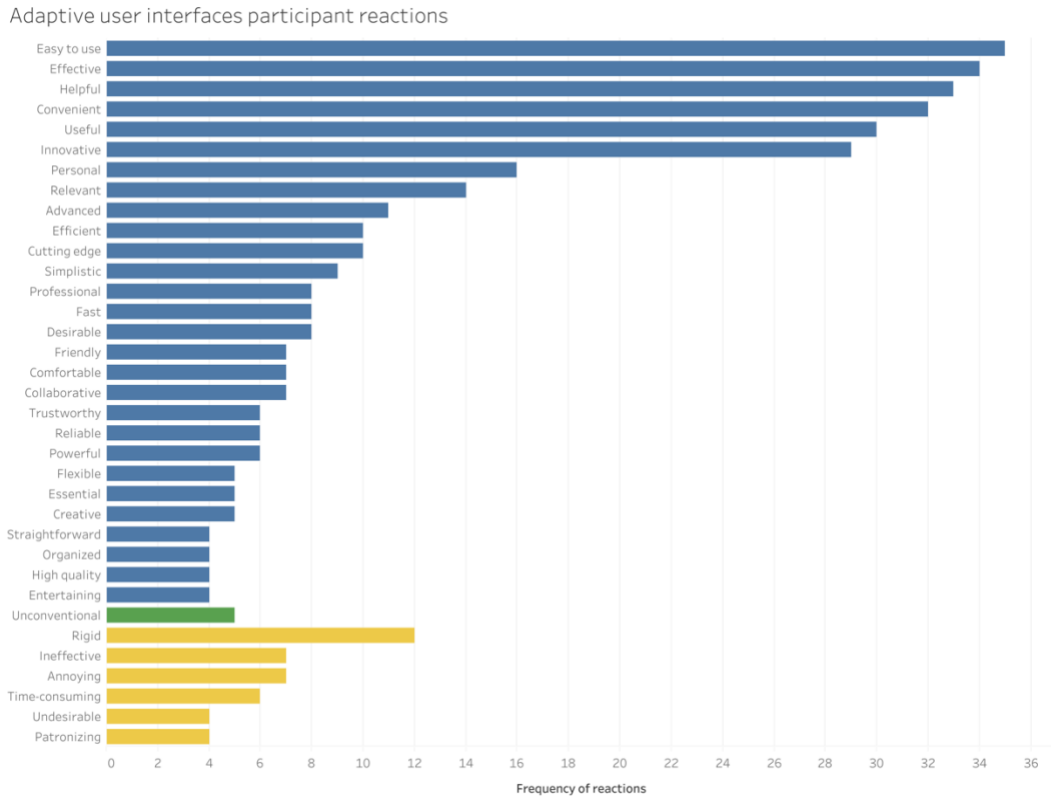

Figure 6.5: Participant Reactions for AUI

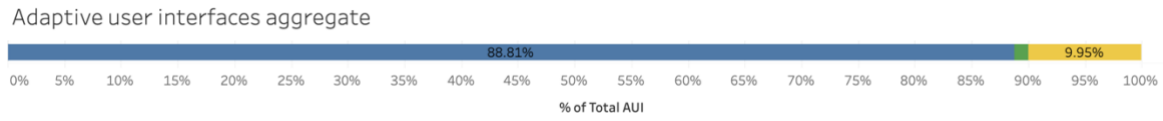

Figure 6.6: Percentage of Reactions for AUI

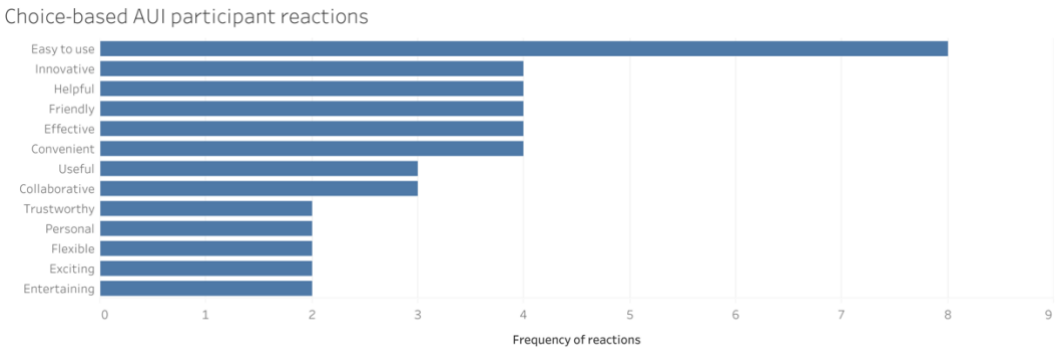

Figure 6.7: Participant Reactions for CAUI

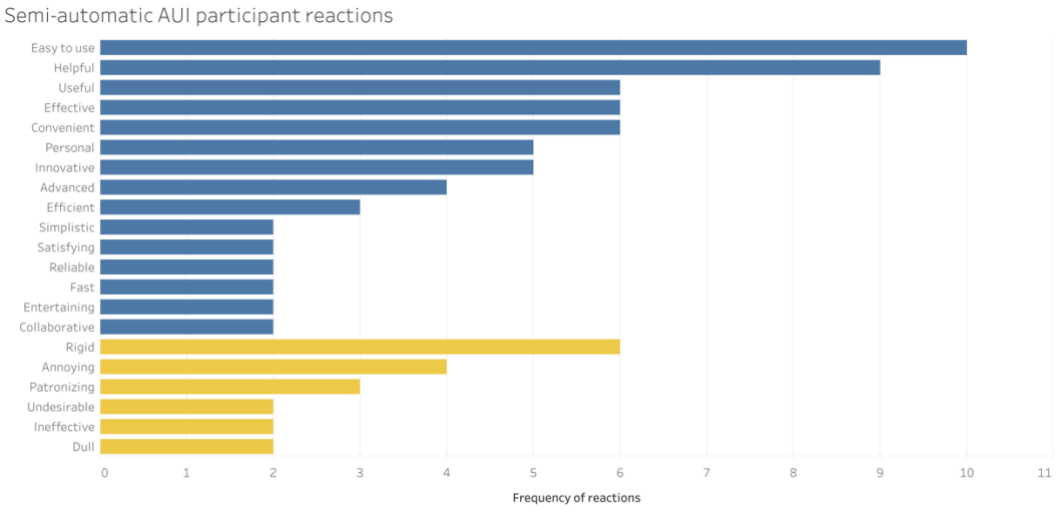

Figure 6.8: Participant Reactions for Semi-automatic AUI

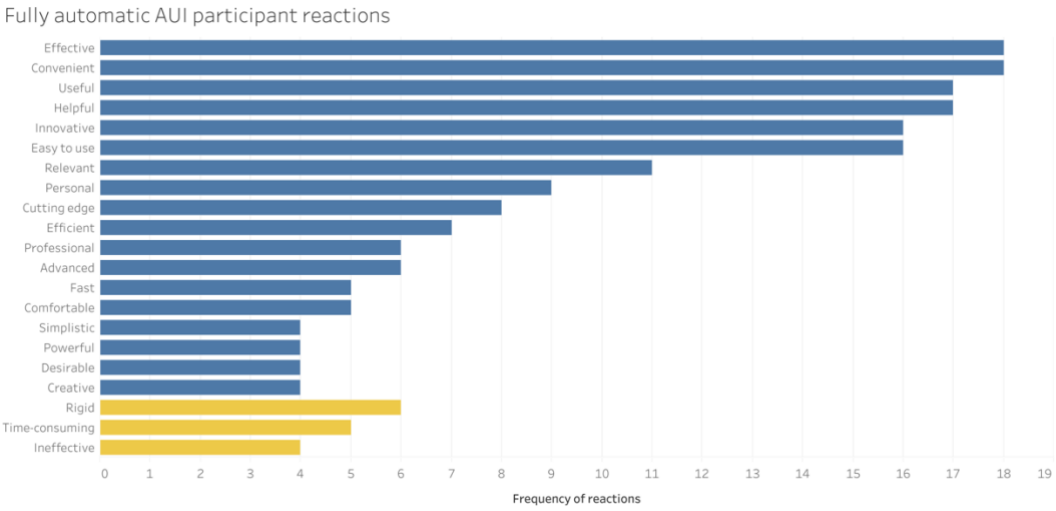

Figure 6.9: Participant Reactions for Fully Automatic AUI

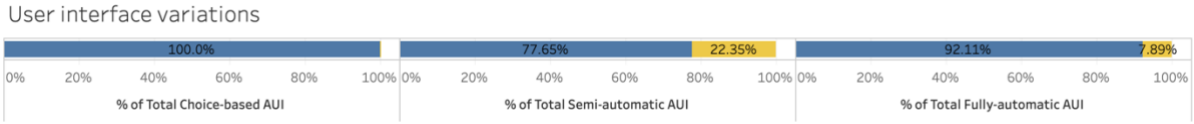

Figure 6.10: Percentage of Reactions for User Interface Variations

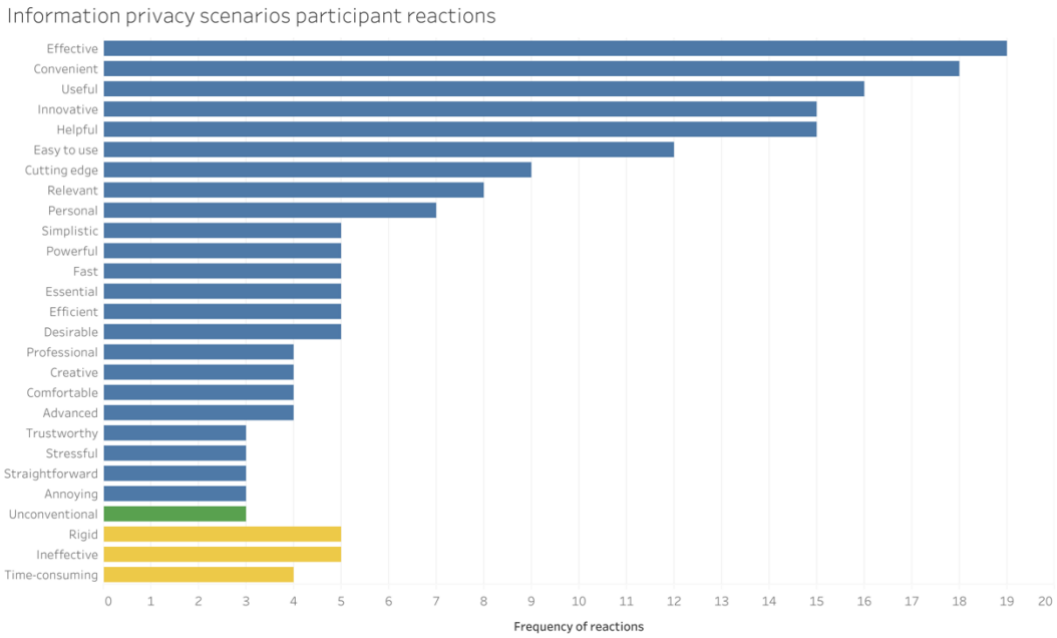

Figure 6.11: Participant Reactions for Information Privacy Scenarios

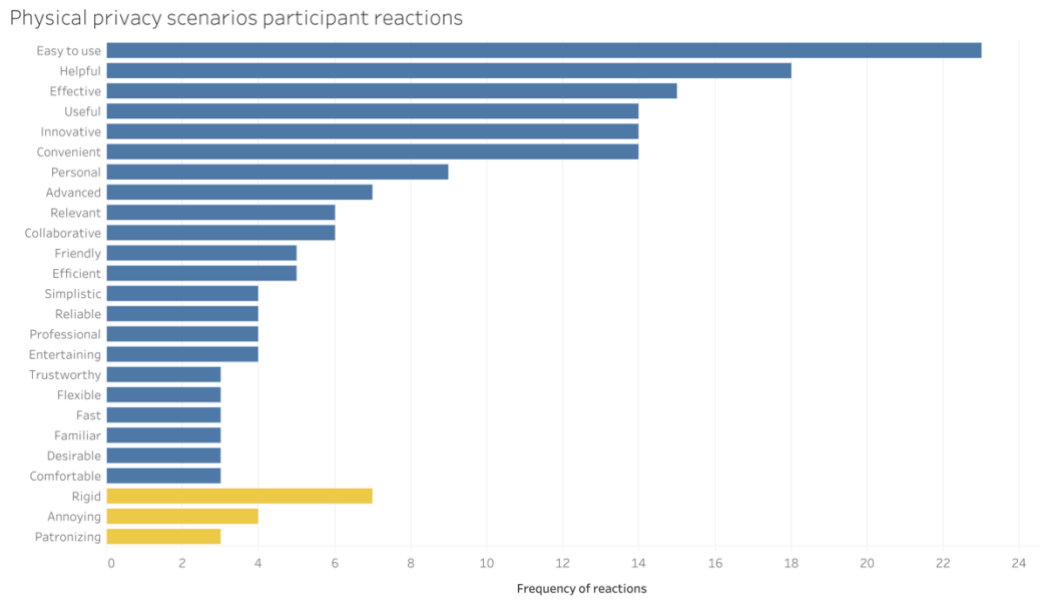

Figure 6.12: Participant Reactions for Physical Privacy Scenarios

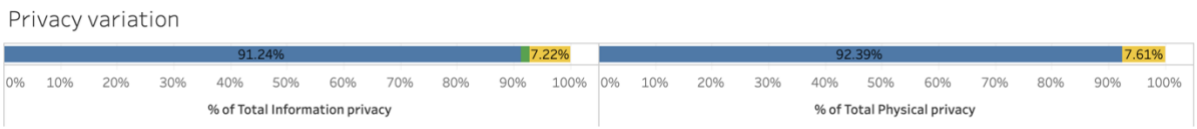

Figure 6.13: Percentage of Reactions for Privacy Variations

Variation Type	**Positive reactions (%) & Top reactions**	**Negative reactions (%) & Top reactions**	**Neutral reactions (%) & Top reactions**

UI variation			
AUI	89% *Easy to use, effective, helpful, convenient, useful, and innovative*	10% *Rigid & ineffective*	1% *Unconventional*
CAUI	100% *Easy to use, innovative, helpful, friendly, effective, and convenient*	0% N/A	0% N/A
Semi-automatic AUI	78% *Easy to use, helpful, useful, effective, and convenient*	22% *Rigid, annoying, and patronizing*	0% N/A
Fully automatic AUI	92% *Effective, conveneint, useful, helpful, innovatie, and easy to use*	8% *Rigid, time consuming and ineffective*	0% N/A
Privacy variation			
Information privacy	*91%* *Effective, convenient, useful, innovative, and helpful*	*7%* *Rigid and ineffective*	2% *Unconventional*
Physical privacy	92% *Easy to use, helpful, effective, useful, innovative, and convenient*	8% *Rigid and annoying*	0% N/A

Table 6.4: Summary of Product Reaction Card Answers

Figure 6.5 shows the aggregated results for all the scenarios where Figure 6.6 shows the percentage split for the positive, neutral, and negative reactions. The reaction cards were aggregated based on the user interface variation. Figure 6.7, Figure 6.8, and Figure 6.9 respectively show the reactions for CAUI, semi-automatic AUI, and fully automatic AUI. Figure 6.10 shows the percentage split for the positive, neutral, and negative reactions. The reaction cards were then aggregated based on the privacy variation. Figure 6.11 and Figure 6.12 respectively show the reactions for information privacy scenarios and physical privacy scenarios. The percentage split of the reactions based on the privacy variations is shown in Figure 6.13. Lastly, Table 6.4 shows a summary of the percentages depending on the user interface variation or the privacy variations and the top reactions picked by the participants.

As shown in Table 6.4, CAUI had the highest positive reactions where semi-automatic AUI had the highest negative reactions. Please note that there was a single scenario for the CAUI where fully automatic AUI and semi-automatic AUI had multiple scenarios Apart from that, there was no significant difference found between the different privacy variations.

6.3.2.2 Questionnaire

Participants were provided with a questionnaire after each scenario (Appendix D: §10.4.2.2). Q1, Q3 and Q5 were positively structured questions where Q2, Q4 and Q6 were negatively structured questions. The Likert scale was from 1 to 5 where 1 was highly disagree where 5 was highly agree.

Table 6.5 shows the mode of the answers given for the questions in the questionnaire (Appendix D: §10.4.2.2). The scenarios were categorised according to the UI variations, privacy variations and all the scenarios together as mentioned in Table 6.3. Figure 6.14 shows the box-plot graphs of the questionnaire answers.

Question / Category	Q1	Q2	Q3	Q4	Q5	Q6
AUI	5	1	2	1	5	1
Fully – AAUI	5	2	1	1	5	1
Semi - AAUI	5	4	2	1	5	2
CAUI	4	1	2	1	5	2
Information privacy	5	2	1	1	5	1
Physical privacy	5	1	2	1	5	1

Table 6.5: Video prototype Study - Modal Values of the Questionnaire Responses

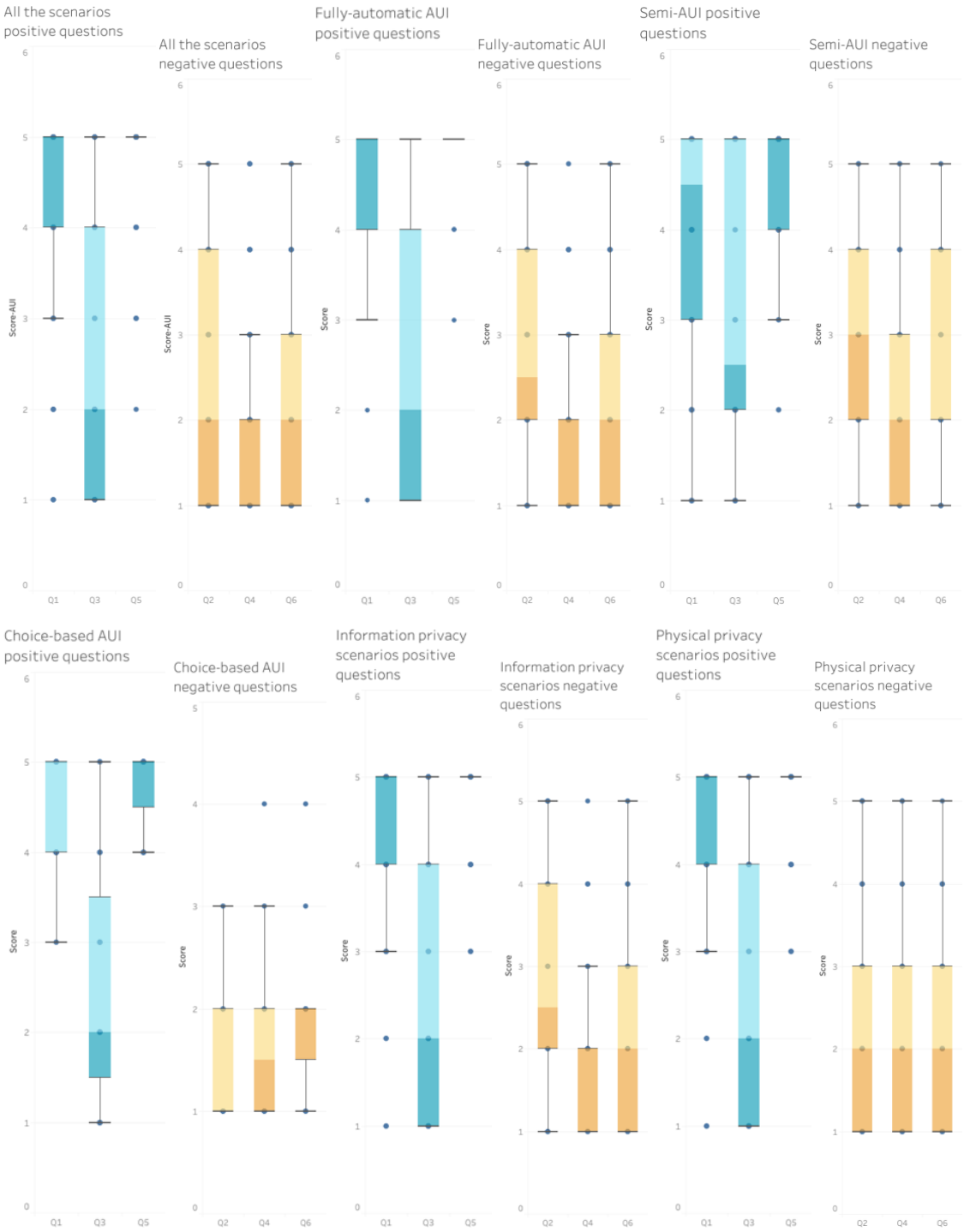

Figure 6.14: Box Plots for Questionnaire Answers

6.3.3 Qualitative Analysis

This section reports the findings of the qualitative data. As discussed in the methodology (§6.2), the user interview data was analysed using inductive thematic analysis. McCarthy and Wright's (2004) six user experience themes when using technology were used to help guide analysis. The interview data was also analysed to identify themes pertaining to the success of the study as well as threats to validity.

Each user experience theme is summarised in a table highlighting the subthemes identified, together with the IDs of the participants who contributed to these findings. The following sections describe the significant subthemes relevant to understanding the user experience and reported by many of the participants. The remaining subthemes listed in the tables (marked with '*****') are presented in the appendix. All the interview transcripts are available in a public dataset (Wijesundara, 2021c).

6.3.3.1 Anticipating

Anticipating explores how the participant's past experiences, preferences and attitudes may have contributed to the user experience of the AUI. Participants reported their experience in relation to expectations of the AUI, highlighting scenarios where the AUI exceeded their expectations as well as scenarios where they were uncertain of the AUI's behaviour. Participants also reported experience in relation to their privacy preferences where they discussed the tension between usability and privacy. Furthermore, they highlighted scenarios that could have conflicts with regard protection of certain kind of privacy that can violate another type of privacy. Some of the participants highlighted their lack of concern over having real-time privacy control. *Anticipating* plays a significant role in colouring the user experience as it dictates what the participant perceives as a positive experience or a negative experience. Therefore, it is important to understand the factors that may have contributed to the user experience of the AUI, which are reported below. Table 6.6 provides a summary of the subthemes, sub-subthemes and the participants who commented on each sub-subtheme regarding the *Anticipating* theme.

Subthemes	**Sub-subthemes** (* denotes subtheme reported in appendix)	**Participants who made comments**
Expectedness	Meeting and exceeding expectations	PX1, PX2, PX4, PX5 & PX6
	Uncertainty	PX4, PX5, PX14 & PX18
Privacy preferences	Users with varying privacy* preferences	PX10 and PX19
	Privacy concerns with smart homes*	PX10, PX11, PX13, PX15 and PX23
	Privacy and usability	PX2, PX4, PX5, PX14, PX15, PX18, PX19 and PX23
	Information vs physical privacy trade-off	PX5, PX13 and PX16
	Lack of concern regarding real-time privacy control	PX7, PX10, PX11, PX14, PX15 and PX19
	Immaturity of smart homes*	PX10 and PX23

Table 6.6: Participants who Commented on Anticipating Theme

6.3.3.1.1 Expectedness

In the context of this work, *expectedness* refers to the extent to which participants were unsurprised by the behaviour of the AUI. Prior to the study, the participants were shown two videos demonstrating the behaviour of AUIs where one video represented an example of an adaptation in response to a physical privacy violation and the other represented an adaptation to mitigate an information privacy violation (§6.2). These videos were illustrative but not representative of all the types of adaptations, which also covered variations based on feature adaptations and modality adaptations. Participant's comments were based on how much these adaptations were expected and how a first-time user would feel seeing AUIs.

Meeting and exceeding expectations: Some participants (N=5/23) discussed how the AUI met or exceeded their expectations. Two participants (PX1and PX2) thought AUI was better than expected. PX2 stated that he was expecting the AUI to be inconvenient as it could obstruct the interaction, but he was pleasantly surprised by the AUI's adaptation. *"… I thought, initially Oh, that that might be inconvenient […] actually, that's much nicer than I anticipated it was gonna be..."*, (PX2[145]). Three participants (PX4, PX5 and PX6) broadly found the experience to be in line with their expectations, only highlighting some features like automatic blurring of the background of a video call to be surprising, but still acceptable: *" I was surprised about the blurring but in general, […] but it doesn't impact too much on the conversation because you are still the face is there and everything works around it. So, it's pretty good."*, (PX6[91]).

Uncertainty: Very few participants (N=4/23) commented on the uncertainty of the AUI. Some of the participants stated that they were uncertain about how the AUI would behave, particularly with respect to the timing of adaptive behaviours (PX6) and the exact type of adaptation that would be used to protect privacy (PX4 and PX18). *"... I was expecting it. but I wasn't expecting it at that moment."*, (PX6[217]). PX18 told that he was expecting the AUI to protect his privacy but was not sure how it would achieve that: *"For what you get by sending it to the phone was innovative I didn't expect that it would come to the […] watch. But I expected that it would not say it aloud so the other person could hear the details"*, (PX18[200]). Finally, three participants (PX5, PX14, and PX18) speculated that a first-time user might not expect the adaptation: *"... new user might not exactly know that since the other person came to the room and, […] because now, I am seeing the system for the first time. So, I didn't expect what would happen."*, (PX18[185]).

6.3.3.1.2 Privacy preferences

Users' privacy preferences played a major role in how they experienced the scenarios. Participants highlighted their preferences about privacy and different biases that could influence their view of privacy. Apart from that, the participants mentioned the impact of national culture (PX18) on a person's privacy attitude where two participants (PX6 and PX19) mentioned that they were unconcerned about privacy.

Privacy and usability: More than a third of the participants (N=8/23) commented on the tension between privacy and usability. According to PX23, protecting bank credentials was more important than having convenience: *"… if your bank credentials are exposed […], is extremely dangerous than waiting it out…*", (PX23[82]). PX5 had a mindset that it is okay to not have instant control over an adaptation in scenarios where immediate action is required to protect privacy: *"Well, I will not say I didn't feel in control, because in this case, I would prioritise the sensitivity to time it needs to happen really flexibly."*, (PX5[166]). PX14 stated that some of the problems cannot be solved by AUI as those problems don't have an optimum solution even without AUI: *" it's establishing a compromise between two people.. […] I'm not sure that there's a way to get a compromise out of a smart system that fully meets everybody's requirements …"*, (PX14[60]).

Lastly, six participants (PX2, PX4, PX15, PX18 and PX19) mentioned preferring physical or direct interaction with the co-occupants rather than a technology-mediated interaction: *" …it'd be so much quicker just to be like, do you mind?... But that's because I'm like a social person."*, (PX19[83]).

Information vs physical privacy trade-off: Three participants (N=3/23) highlighted that they are worried that information privacy can be breached in trying to protect physical privacy. PX5 was uncomfortable sharing what she is doing with everyone in the smart home to only protect her physical privacy. *"…I am not comfortable with all my roommates knowing what I'm doing all the time… That's a bit of a paradox."*, (PX5[198]).

6.3.3.2 Connecting

In the scope of this work, *connecting* represents the initial reactions and feelings of the participants when they first interacted with AUI(s). Some of the participants found AUI to be familiar. This section also reports the instant positive emotions that were generated when the participants first experienced AUI. Most of the participants thought the AUI was "cool" and a few of them mentioned that the AUI made them comfortable. Apart from that, some participants commented on the generic user interface features that stood out in their experience of the AUIs. Furthermore, participants commented on the experience of speed when interacting with the AUI where they highlighted that AUIs are fast in execution and that AUIs are highly responsive. A smaller number of participants mentioned that the AUI could be time consuming due to configuration overheads. Lastly, some of the participants thought AUIs to have a humanising effect. This was due to the AUI's personalisation to the smart home user, approachability, and friendliness. Similar to anticipating, connecting contributes to how the user experiences the rest of the interaction. Table 6.7 provides a summary of the subthemes, sub-subthemes and the participants who commented on each sub-subtheme regarding the *Connecting* theme.

Subthemes	Sub-subthemes (* denotes subtheme reported in appendix)	Participants who made comments
Familiarity	AUI is familiar	PX1, PX2, PX6, PX7, PX10, PX11, PX15 and PX17
	AUI is novel*	PX1, PX2, PX6, PX7
	AUI is strange*	PX6, PX13 and PX16
Instant positive emotions	AUI is cool	PX1, PX3, PX5, PX6, PX7, PX8, PX13, PX19, PX21 and PX23
	Impressed with AUI*	PX1, PX2 and PX7
	Made the user comfortable	PX4, PX6, PX8, PX13, PX18 and PX22
Speed	Fast execution	(a) PX3, PX5, PX7, PX12, PX15, PX16, PX21 and PX22 (b) PX2, PX4, PX5, PX6, PX16 and PX16
	Time consuming	PX10, PX17, PX19, PX22 and PX23
Humanising effect	AUI was approachable and friendly	PX1, PX6, PX13, PX15, PX16 and PX21
	AUI was personalised	PX1, PX5, PX6, PX7, PX10, PX11, PX13, PX14, PX15, PX16 and PX17

Table 6.7: Participants who Commented on Connecting Theme

6.3.3.2.1 Familiarity

In the context of this work, familiarity refers to the extent to which the users found AUI to be familiar. Some of the participants found the AUI to be familiar as it extended existing technologies such as the background blurring feature of video conferencing tools and photo browsing tools.

AUI is familiar: More than one third of the participants (N=8/23) found the AUI to be familiar because of its similarity to the behaviour of existing technologies. For most of them (PX1, PX6, PX10, PX11, PX15 and PX17) the AUI's blurring technology was a common example of this familiarity: *"… I use platforms that allow me to blur out the background or put in another background. So, this builds on something that I do use…"*, (PX10[121]). Similarly, PX2 found the AUI's warning to be familiar to existing antivirus warning mechanisms: *"…the form of prevention that it takes is quite innovative, […] like a little antivirus warning come up, or like a little windows thing where it's just like, yes, no, or you know, like the cookies stuff…"*, (PX2[98]). Finally, PX7 mentioned that he got familiarised with the AUI's features as the study went along: *"I see the smart speaker. I asked the question then I've probably already seen [the co-occupant] and then the […] I hear the Bing sound. And then I know that that means 'Ah look at the phone'. Because I'm [...] aware that […] it's going to ask me to adapt if I'm disrupting somebody..."*, (PX7[61]).

6.3.3.2.2 Instant positive emotions

The participant's first interaction with AUI generated certain emotions or reactions. Most of the participants thought the AUI was 'cool'. Some of the participants also described how it made them comfortable.

AUI is cool: Many of the participants (N=10/23) found AUI to be really cool. PX1 thought AUI to cool as it's a novel application: *"First of all, that was very cool. I would not have thought about that kind of a scenario."*, (PX1.5). PX5 thought AUI to be 'mega-cool' and wished to adopt AUI to her own life: *"…this will be mega cool to work like this…"*, (PX5[117]).

Made the user comfortable: Lastly, more than a quarter of participants (N=6/23) described how the AUI made the user feel comfortable. PX8 and PX18 mentioned that it made them comfortable or avoided uncomfortable situations: *"It would have felt uncomfortable about his friend knowing about his blood glucose level."*, (PX18[181]). Four participants (PX4, PX6, PX13, PX22) commented on how the AUI was organised, clean or how easier it is to interact with. PX4 was quite happy about having larger buttons to select the choices: *"That interruption flexible because you can choose the different options […] thought it was easy to use because you had quite a few options [with] big buttons to select them"*, (PX4[113]). PX6, PX13 and PX22 mentioned that it provided clarity: *"…it was […] organised and clean […] the answer given on the watch was clear and simple."*, (PX22[51]).

6.3.3.2.3 Speed

Speed refers to how users perceive the sense of time when interacting with the smart home via the AUI. Most of the participants thought that it was quite fast in execution and to have responsive behaviour, although there were few participants who thought it could be time-consuming.

Fast execution: Over a third of the participants (N=8/23 (a)) felt that the AUI was really fast. PX22 was really fascinated by its speed and how quickly it was able to predict and adapt according to the context change "…*it was also incredibly fast because I don't know how it did, but it predicted then transformed to the other person. So again, effective it has worked well even before the other person entered. So very fast yet trustworthy because it happened before. So I think it also left the time for I mean a second measure in case it didn't work …"*, (PX22[65]).

Over a fourth of the participants (N=6/23(b)) commented on the responsiveness of AUI. PX2 and PX5 commended AUI's responsive nature to privacy violations. *"such a technology would be cutting edge, to be able to […] identify privacy risks like this on the fly, dynamically as they occur"*, (PX2[44]). PX5 felt that the AUI reacted fast to context changes: *"What I like about all these scenarios is that there was an idea of having some knowledge about the user preferences beforehand and react, reacting very quickly to the presence of other people in the same house…"*, (PX5[183]). Lastly, five participants (PX2, PX4, PX6, PX16 and PX16) mentioned that the AUI

sent notifications really fast to the user: *"… notification immediately told you what had happened and why and then provided the smartphone as an alternative…",* (PX4[174]).

Time consuming: Some of the participants (N=5/23) thought the AUI could be time consuming. PX10 and PX19 thought it could be time-consuming due to the initial configuration: *"it's so time consuming. Yes. Because at some point, I'm gonna have to give it all these conditions…",* (PX19[26]). Furthermore, PX19 and PX15 thought talking to the co-occupant to mitigate the conflict is much faster than AUI's intervention: *"I would rather just ask the person and be like, hey, do you mind if I watch some of my pictures because my pictures aren't making any noise. […] I just think it's it'd be so much quicker just to be like, do you mind?",* (PX19[83]).

6.3.3.2.4 Humanising effect

In the context of this study, *humanising effect* reports how participants felt about the AUI's ability to mimic human interaction. Participants reported that the AUI was approachable, friendly, and human-like. Participants also reported that it was personalised to the smart home users.

AUI was approachable and friendly: Some of the participants (N=6/23)) thought the AUI was approachable, friendly or human-like. PX16 felt AUI explanation was approachable: *"… because of the way the system was explaining me the context …", (*PX16[45]). PX21 thought these explanations made the AUI 'humanlike' – e.g., *"The app showed me that okay, we switch to the phone because of this it's very human as in [...] when we are conversing and if you change the mode of conversation with a human, we just tell them why things change or the status quo change…",* (PX21[27]). Four participants (PX1, PX13, PX15 and PX17) thought the AUI was quite friendly. According to PX1, the AUI made decisions to help the user's way of life: *"…I think it's very helpful and friendly that a software or a tool is able to make those decisions on behalf of me, so it doesn't interrupt my way of life.",* (PX1[32]). PX1 and PX15 thought AUI was considerate. *"… I think it's a very considerate approach.",* (PX1[21]).

AUI was personalised: Almost half of participants (N=11/23) thought the AUI was personalised. For example, PX6 was impressed with its adaptability to the user: *"…is a really a nice adaptive technology to use, […], it protects everybody, but it's not, […] a blanket, it has a bit more is adaptive towards something, like the person entering the room.".* (PX6[91]). PX5 mentioned that it is adaptive compared to existing devices: *"…more and more we're sharing spaces with other people, but these devices are sometimes are designed for just being used by one person. […] what I like about all these scenarios is that there was an idea of having some knowledge about the user preferences beforehand ...",* (PX5[183]). Lastly, PX12 stated that the AUI's information was personalised: *"…you receive the answer, […] in a very targeted way. So, it is only for yourself, basically asking information about yourself.",* (PX12[13]).

6.3.3.3 Interpreting

In this section, *interpreting* refers to the comments and thoughts that participants had while they were interacting with the AUI. *Interpreting* covers how participants made sense of the AUI behaviour. Most of the participants reported how easy it is to navigate AUIs where they highlighted dimensions such as reduced cognitive load, high learnability, and seamlessness. Most of the participants reported that the AUI provided freedom by being flexible and giving a sense of control. In contrast, some of the participants mentioned how semi-automatic-AUI and fully-automatic-AUI made them feel restricted. Some of the participants mentioned automatic adaptations, rigid and paternalistic adaptations made them feel that the AUI was restrictive. Most of the participants commended the explanations provided for the AUI's behaviour where they described how the AUI kept the user in the loop. In contrast, a few of the participants' comments implied that they were unclear about how the AUI worked and more generally smart homes worked. Furthermore, participants expressed positive emotions such as happiness, excitement, and engagement that participants felt during the interactions. This section concludes with a description of how participants perceived the AUI's capabilities. They highlighted features such as UI adaptations, discreetness, and context sensitivity of the AUI. Table 6.8 summarises the subthemes, sub-subthemes and the participants who made comments regarding each sub-subtheme under the *interpreting* theme.

6.3.3.3.1 Ease of navigation

In the context of this work, *ease of navigation* refers to participants' thoughts on how easy it is to interact with the AUI. Most of the participants found the AUI was easier to use because it reduced the cognitive load, was easier to learn, supported multiple users and was seamless. Participants also mentioned that the AUI was easier to navigate because it was reliable and made the user aware. These latter findings are reported later in a separate section (§6.3.3.4.5).

Reduced cognitive load: Almost half the participants (N=11/23) found the AUI reduced the cognitive load due to the (semi-)automated nature of the interaction. For example, PX14 stated that the AUI operated automatically according to user preferences: *"…Easy to use, because you didn't have to do anything to make it happen. It seemed to happen for you.…",* (PX14[60]). PX16 described how the AUI having smaller number of steps made the interaction convenient: *"It was really easy to use, you just gave me a ping on the app, I get a notification and I just select which one I want.",* (PX16[22]).

Subthemes	Sub-subthemes (* denotes subtheme reported in appendix)	Participants who made comments
Ease of navigation	Reduced cognitive load	PX2, PX3, PX5, PX6, PX7, PX9, PX11, PX14, PX16, PX18 and PX21
	Learnability	PX1, PX2, PX4, PX5, PX11, PX14, PX17 and PX21
	Multi-user support and accessibility*	PX1, PX6, PX10, PX15 and PX23
	Seamlessness	PX1, PX4, PX5, PX6, PX7, PX10, PX15, PX16, PX17, PX18 and PX21
Unease of Navigation	Configuration over-head*	PX10 and PX19
	Non intuitive*	PX3, PX9 and PX17
Freedom	AUI was flexible	PX2, PX4, PX5, PX7, PX8 and PX15
	AUI provided a sense of control	PX1, PX2, PX4, PX5, PX6, PX13, PX14, PX15, PX17 and PX18
Captivity	Automation and rigidity	(a) PX2, PX3, PX4, PX5, PX6, PX7, PX9, PX10, PX11, PX13, PX15, PX16, PX17, PX18, PX19 and PX23 (b) PX2, PX5, PX6, PX7, PX11, PX15, PX16 and PX19 (c) PX2, PX3, PX4, PX5, PX7, PX10, PX11, PX13, PX15, PX17, PX18 (d) PX3, PX4, PX6, PX9, PX10, PX15, PX17, PX18, PX19, PX23 (e) PX6, PX7 and PX19 (f) PX2, PX3, PX6, PX13, PX14, PX15, PX17 and PX23
	Privacy enforcement*	PX7 and PX15
	Unclear mental model*	PX13 and PX23
Explainability	User in the loop	(a) PX2, PX4, PX7, PX8, PX13, PX14, PX16 and PX18 (b) PX4, PX14, PX16 and PX18 (c) PX2, PX4, PX7, PX8, PX13, PX16 and PX18
	Understandability	PX2, PX4, PX5, PX6, PX7, PX8, PX10, PX13, PX12, PX15, PX18 and PX21
	Lack of clarity	(a) PX5, PX13, PX16, PX18, PX19 and PX23 (b) PX11, PX13, PX15, PX16 and PX17

Subthemes	Sub-subthemes (* denotes subtheme reported in appendix)	Participants who made comments
Positive emotions during the interaction	Happiness	PX2, PX6, PX8 and PX12
	Exciting and engaging	PX1, PX8, PX9, PX11 and PX21
AUI capabilities	UI adaptation	(a) PX4, PX6, PX7, PX8, PX9, PX10, PX12, PX13, PX14, PX15, PX18 and PX22 (b) PX9, PX11, PX10, PX18 and PX21
	Discreetness	PX1, PX2, PX6, PX8, PX11, PX12, PX13, PX14, PX15, PX16 and PX22
	Automation*	PX1, PX2, PX3, PX5, PX6, PX7, PX11, PX13, PX14, PX15, PX18, PX21 and PX22
	Context sensitivity	PX2, PX4, PX5, PX7, PX9, PX10, PX11, PX13, PX15, PX16, PX17 and PX19
	Timeliness*	PX1, PX4, PX6, PX15 and PX18

Table 6.8: Participants who Commented on the Interpreting Theme

Learnability: More than one third of the participants (N=8/23) found the AUI to be easy to learn, consequently easier to navigate. Some of the participants reported that this was because the AUI extended existing technologies – e.g., "*People [...] are already very used to looking at photos on their phone. So the adaptation is telling you not to do something that you know not to use them on the screen, but to use them on a device you're already very familiar with…",* (PX2[193]). PX11 stated that the AUI was easier to use as it is self-explanatory: *"straightforward similar to easy to use, it's […] self-explanatory. It doesn't have to be an introduction, a tutorial or anything ",* (PX11[33]). Three of the participants (PX1, PX2, and PX4) thought AUI was easier to use as it was presented in a convenient manner: *"…didn't look […] there were gonna be a lot of button clicks, no matter what I clicked, it was just gonna be like, here are the alternatives, choose one, single button push…",* (PX2[144]). Lastly, a few of the participants (PX1, PX5 and PX17) thought the AUI's simpler design made it easier to use: *"that is very easy to use, and design wasn't too crowded. So, it was very easy to understand. And then the, there wasn't much to interpret like the […] question was really clear.",* (PX5[40]).

Seamlessness: Almost half of the participants (N=11/23) thought AUIs were seamless and did not obstruct the interaction or their goals. PX4 thought it was successful in achieving its goal: *"I thought it was very successful at achieving the objective of giving the user the ability to still get the information, telling them why it wasn't coming through the speaker",* (PX4[224]). PX6 and PX16 found the AUI's notification was seamlessly transferred to the user's personal device: *"I think the notification that came up was […] very smooth, seamless. I think it was pretty good user experience in my point of view.",* (PX16[7]). Furthermore, five of the participants (PX5, PX7,

PX15, PX16 and PX17) thought the adaptation was seamless: *"…this is more seamless. It is a [..] small shift, I can still carry on with the activity I was doing with this smaller shift…"*, (PX7[168]).

6.3.3.3.2 Freedom

In this section, *freedom* refers to the amount of flexibility and choices participants felt while interacting with the AUIs. Some of the participants highlighted flexibility having a sense of control as reasons for this freedom.

AUI was flexible: Some of the participants (N=6/23) thought AUI was flexible. For example, PX5 mentioned AUI is flexible because it was context sensitive: *"…it was flexible as well because there was adapting to the scenario having a different portion of the image being blurred…"*, (PX5[158]). Additionally, PX1 mentioned that AUI, the user could setup when and how to blur the background. *"…it automatically blurs the background depending on like the user agreement, […] I could choose to have my background shown, but at specific times, to just switch it on and off…"*, (PX1[203]).

AUI provided a sense of control: Many participants (N=10/23) agreed that the AUI provided a sense of control. PX2 and PX4 mentioned that user could do anything they liked: *"…I think the user was in control of the smart home So even the system gave him options and he could have used, chose whatever he wanted to do…"*, (PX18[33,32]). In contrast, PX4, PX7 and PX15 mentioned that they were fine without having control at the exact moment of the interaction to have a sense of control: *"…I think there was no goal to do it in real-time. […] I see that I was substantially in control."*, (PX15[112]). Furthermore, PX2 mentioned that controlling personal privacy gives a sense of control as opposed to protecting the co-occupant's privacy: *"I feel more in control of this scenario. […] I think that that is because this scenario was about protecting my privacy, and it was something I set up. So, I feel a bit more in control than in the previous scenario when the smart home was taking action to protect someone else's privacy"*, (PX2[111]). Lastly, PX6 mentioned that AUI gives the user the control to take back the control of their immediate privacy: *"…[company X] already has my soul but some of the control will get back to me and I be able to at least control my immediate privacy around me ..."*, (PX6[223]).

6.3.3.3.3 Captivity

In contrast to the *freedom* reported above, *captivity* refers to the feeling of the user's not having control over their interaction. Participants highlighted how factors like automation and rigidity contributed to this experience. Furthermore, they mentioned that the smart home adapting to change or constrain the behaviour of the main user to protect other's privacy and not having a clear mental model of the smart home behaviour could also lead to a feeling of not having control over the smart home. A few of the participants also reported how the AUI seemed patronising and over-protective of the co-occupants.

Automation and rigidity: A quarter of the participants (N=6/23 (a)) stated that in some scenarios (physical privacy violations with fully automatic AUI solutions), automatic adaptation, lack of options, rigidity, paternalistic adaptations made them feel like not having control. PX18 thought, in scenarios where the AUI was fully automatic, it felt like not having control: *"...if I was in a very important place of the cartoon that I would have like to continue watching, it could have still, I felt like it could have still been changed, so I thought, I did not see the user was in the control",* (PX18[240]). Furthermore, quite a few of the participants (N= 8/23 (b)) highlighted the scenarios without options can be rigid and make them feel like not having control: *"…For me it was undesirable. And because I also did not get options, okay, maybe [...] the option could have been to tilt the screen. Or maybe the option could have been to do you want to go to [the co-occupant] and ask them to move to another room...",* (PX15[72]).

Another group of the participants (N=11/23 (c)) felt they were not in control in scenarios where they did not have the option to refuse the adaptation: *"…I felt like the system has its own rules. And once it's in motion, I don't feel that much of a control…",* (PX21[17]).

Many participants (N=10/23 (d)) found, the inability to pick the preferred user interface modality as not having control. According to PX21, the main user did not get the intended interaction modality: *"...the reason I asked my voice assistant to get my bank balance would have been like, all the while having a phone within my reach might have been for some reason. So, say My hands are wet or 95% occupied. So then, in that case, the voice assistant and the smartphone compromises on that user experience and switches it to a different one in order to preserve privacy, which I think is a good trade-off, but it obstructed the user experience that I wanted.",* (PX21[36]). According to PX15, the AUI might have restricted the main user from achieving his goal: *"Although there might be a bit compromise […] for the first person […] I might want to hear like ambient sound like not on the ear, not on the headphones but more like being the environment.",* (PX15[30]).

Three participants found physical (N=3/23 (e)) privacy related semiautomatic AUI to be patronising. PX10 mentioned that he finds it is problematic that the smart home telling him to do something: *"…there is a little bit of an issue around a computer system telling you these things, but I can see the, I can see the point here…",* (PX10[148]).

Some of the participants (N=8/10 (f)) thought that the AUI was over-protective and that this was a negative compromise when used in physical privacy related scenarios. For example, in the scenario where the main user tries to watch some photos on the Smart TV (Table 6.1: SLD scenario), PX6 reported: *"I found it a bit over the top. Because there's no noise, there's just visual disturbance. So, I found it a bit, too much.",* (PX6[18]). In the same scenario, PX2 mentioned that the AUI's adaptation is too much of a compromise: *"…it felt like the biggest compromise out of them […] if I really wanted to look at my photos on the TV, […] I feel like almost the adaptation went a little bit*

too far…", (PX2[213]). A few of the participants (PX15, PX17 and PX23) found it annoying to be mindful about the second user all the time. PX15 questioned why he has to be always careful about the other user where some of the scenarios might not be violating the co-occupant's privacy: *"…it seems like only I have to be mindful for privacy of the other person. I agree to it. But again, the reason he was not that strong, or I was not that sure that he will get disturbed…",* (PX15[93])

6.3.3.3.4 Explainability

In the context of this study, *explainability* refers to the extent to which participants felt the AUI provided reasons for the adaptation in a given context. Participants reported that the AUI kept them in the loop, how much they understood the adaptation and the reasons for it. This section also reports how a small number of participants were unable to understand how the AUI or the smart home operated. These were mainly due to the shortcomings of the video prototype mechanism dues to its limitations demonstrating certain aspects of the interaction.

User in the loop: Many of the participants (N=8/23 (a)) highlighted that the AUI kept them in the loop. Some of the participants (N=4/23 (b)) highlighted that they understood the reasons for the adaptations and quite a few of the participants (N=7/23 (c)) mentioned that the AUI made them aware of the possible privacy violations. PX4 described how the AUI explained the context and provided with alternatives: *"…notification immediately told you what had happened and why and then provided the smartphone as an alternative.",* (PX4[174]). Furthermore, PX21 stated that AUI's explanation was human-like: *"…it was explaining why certain changes in user interactions happen without just like suddenly changing things. […] it's very human as in when [...] I say, like when I are conversing and if you change the mode of conversation with a human, I just tell them why things change.",* (PX21[27]). PX8 stated that the AUI made the user aware of the possible privacy violation and stopped his interaction: *"…when I'm about to enter the passwords, [the co-occupant] gets in the room so that I get a message on my phone that says, hey, guys in the room, so please don't say your password out loud.",* (PX8[58]).

Understandability: The majority of the participants (N=12/23) stated that they understood the AUI. PX18 stated he understood AUI because it was in line with the user's preferences. *"I understood why the user interface adaptation happened. [..] Because we were said that the user preference and I can understand that why the user interface adaptation happened.",* (PX18[251]). PX22 mentioned that the clarity of the AUI made it easier to understand: *"it was […] organised and clean […] the answer given on the watch was clear and simple. […] easy to use because there were not complicated things…",* (PX22[51]).

Lack of clarity: In contrast to the point above, some of the participants (N=6/23 (a)) comments showed that they were unaware of how the AUI worked. PX13 preferred to have more clarity over the AUIs functionality: *"…I would like to have more disclosure in terms of to understand how it*

works […] to be able to select which kind of information I want to disclose and which not", (PX13[196]).

Apart from that, a few of the participants (N=5/23 (b)) reported uncertainty over understanding the smart home functionality and physical attributes. For example, PX13 mentioned that they were uncertain of smart home's sensing functionality: *"… It's a source of not being confident of what's of what […] the application can do. Maybe knowing more about where the information is coming from, what's exactly been recorded, or what's exactly been considered what's happened with that information, so maybe it's some sort of transparency.",* (PX13[113]). Furthermore, PX17 mentioned that they were uncertain of smart home's context sensitivity: *"it's not clear. Really, where this person is, and whether they're meditating upstairs whether the music would truly annoy them or not.",* (PX17[31]). Lastly, PX11 stated that it was hard to gauge some of the physical features of the smart home: *"…you never know I mean you could have very thin walls or the system, humans often have a difficulty telling if they're being overheard…",* (PX11[54]).

6.3.3.3.5 Positive emotions during the interaction

This section reports the positive feelings that users felt during the interaction. Participants highlighted that the AUI made them happy, was excited and engaged. One of the participants also mentioned that it made them confident.

Happiness: Some of the participants (N=4/23) mentioned that they were happy while interacting with the AUI. PX8 mentioned that the secondary user was happy to know that their privacy was protected by the smart home: *"…the person […] getting in the room in my room knows what's going on. I mean, they know that the screens been blurred, […] they'd be quite happy about it.",* (PX8[89]). Furthermore, PX6 stated that he was happy that he did not have to listen to sensitive information of the co-occupant: *"…the secondary user is super happy because he doesn't have to hear all my stuff.",* (PX6[181]).

Exciting and engaging: Some of the participants (N=5/23) reported that the AUI was exciting and engaging. PX1 stated that it was quite exciting: *"I've never seen this kind of technology before. So, it seems very innovative, advanced and quite exciting.",* (PX1[31]). PX8 stated that the AUI is an engaging experience for both the users: *"engaging because for me, this is maybe this is the best example from in all the videos where I can see a reward in both the both users.",* (PX8[133]).

6.3.3.3.6 AUI capabilities

This section reports how participants perceived the AUI's or smart home's capabilities. Participants highlighted the AUI features such as feature adaptation, modality switching, discreteness, context sensitivity, and predictivity.

UI adaptation: The majority of the participants (N=12/23 (a)) identified the AUI's capability to adapt the features of the UI layer and some of the participants (N=5/23 (b)) noted how the AUI switched its modality. PX10 highlighted the adaptive blurring feature of AUI: *"…the person who walked through wants to stay anonymous. And therefore, they got blurred when they walked through the screen…",* (PX10[109]). PX4 highlighted the sensitive audio masking feature of the AUI: *"a co-occupant of my office operating the safe and the video, the system covered up the pin number",* (PX4[68]). Furthermore, PX14 identified the AUI's sensitive video masking feature: *"…. he was browsing through cartoons. And just before somebody walked in the door, it covered that up kind of providing a kind of a privacy screen for what he was, he was actually looking at...",* (PX14[14]).

PX11 identified how the AUI switched dialogue from the smart speaker to the watch: *"…primary user asked for sports information to Alexa and Alexa, knowing that someone else who didn't want to get disturbed was in the room, switch to phone instead and then provided the information on the phone…",* (PX11[89]). Lastly, PX21 highlighted how the AUI directed the information from the phone to the smart speaker: *"…I want to actually check my bank balance. And I just speak to my works assistant. And the moment the voice assistant is about follow up on my question. I see a colleague walking in, and then I get like a push notification on my phone telling that I need to continue the same flow…"* (PX21[26]).

Discreetness: Almost half of the participants (N=11/23) highlighted how the AUI was discreet. PX14, mentioned that the second user would not know what is going on before they entered the space: *"…the other person wouldn't have known what was going on at all. […] they came in and it looked perfectly normal to them.",* (PX14[16]). PX7 mentioned that the adaptation was not distracting the co-occupants: *"I don't think it becomes much of a distraction, because there's blurredness and so kind of fades in.",* (PX7[134]).

Context sensitivity: The majority of the participants (N=12/23) identified the AUI's capabilities to sense context changes. PX11 stated that the AUI could identify the scenario and act accordingly: *"…smart home system can identify the scenario and act accordingly…",* (PX11[54]). According to PX2, it was sensing the environment on behalf of the user and protected privacy: *"I'm trying to check my bank balance. And before I, myself give out private information, the system stops me from doing it even though I'm not aware of the violation is going to take place.",* (PX2[83, 84, 85, 86]).

6.3.3.4 Reflecting

This section reports how participants reflected on their experience of the AUI. Participants appreciated the concept of the AUI stating that is a good and innovative idea. Most of the participants commented on the AUI's efficacy and they said that the AUI was successful. In contrast, a few participants thought it was ineffective where they showed how certain privacy violations could occur even with the AUI. Some of the participants commented on the fairness of

the AUI as it was an acceptable compromise. Furthermore, they reported it to be dependable due to AUI's reliability and trustworthiness. Lastly, participants reported how the AUI enhanced relationships by supporting relationships and promoting multi-user collaborations. Table 6.9 summarises the subthemes, sub-subthemes and the participants who made comments regarding each sub-subtheme under the theme of *reflecting*.

6.3.3.4.1 Conceptual appreciation

In this work, *conceptual appreciation* refers to participants positive comments regarding the concept of AUI. Participants found the AUI to be a good idea and to be an innovative idea.

AUI is a good idea: The majority of the participants (N=17/23) thought the AUI was a good idea. PX4 appreciated the adaptive blurring feature: *"…manipulating the image to protect people's privacy is a really good idea."*, (PX4[234]). PX17 appreciated its privacy-awareness: *"…being able to detect the primary user and when a secondary person is in either within a short or [...] within the confines of the room is [...] a good idea."*, (PX17[99]). PX15 appreciated the adaptation: *"…privacy choices within the family members or within the co-occupants, definitely can differ. […] I think it is good to have that kind of adaptation..."*, (PX15[182]).

Innovative: Almost half of the participants (N=10/23) mentioned that the AUI was innovative. PX18 thought it protected privacy in an innovative manner: *"…. it, like, helped me with my privacy. And also, it was provided in an innovative way."*, (PX18). PX6 stated that the AUI was innovative compared to existing technology: *"… innovative because nobody else is doing this…"*, (PX6). PX14 found it innovative as it combined multiple sources of UI: *"…innovative, because the ability to combine multiple sources of input and interpret what's going on is pretty cool."*, (PX14). PX18 thought modality switch was innovative: *"...For what you get by sending it to the phone was innovative I didn't expect that it would come [...], to the watch. But I expected that it would not say it aloud so the other person could hear the details."*, (PX18[200]). Finally, PX11 mentioned the AUI's context sensitive privacy protection was innovative: *"innovative because the […] smart home system can identify the scenario and act accordingly…"*, (PX11[54]).

6.3.3.4.2 Efficacy

In the context of this work *efficacy* means how well the AUI protected the smart home users' privacy, successfully providing the functionality that they were trying to access in each scenario.

Subthemes	Sub-subthemes (* denotes subtheme reported in appendix)	Participants who made comments
Conceptual appreciation	AUI is a good idea	PX1, PX2, PX3, PX4, PX5, PX6, PX7, PX8, PX9, PX10, PX11, PX12, PX13, PX15, PX17, PX18 and PX22
	Innovative	PX5, PX6, PX7, PX9, PX14, PX15, PX16, PX18, PX21 and PX23)
	Smart*	PX6, PX10, PX15
General appreciation*		PX1, PX2, PX3, PX6, PX8, PX10, PX13, PX14, PX15, PX17 and PX18)
Value*		PX3, PX4, PX11, PX13, PX15
Efficacy	AUI is successful	All the participants
	AUI is effective*	(a) PX2, PX3, PX4, PX5, PX6, PX7, PX8, PX9, PX10, PX11, PX12, PX14, PX15, PX16, PX18 and PX22 (b) PX2, PX4, PX6, PX7, PX8, PX9, PX10, PX11, PX12, PX14, PX15, PX17 and PX18 (c) PX1, PX2, PX3, PX4, PX5, PX7, PX9, PX10, PX13, PX15, PX16, PX18
	AUI is efficient*	PX4, PX5, PX8, PX14 and PX22
	AUI enhances the UX*	PX13, PX14 and PX16
Ineffectiveness	Information privacy violation	PX1, PX3, PX9, PX17 and PX22
	Physical privacy violation	(a) PX1, PX7, PX8, PX9, PX10, PX11, PX12, PX19 and PX22 (b) PX3, PX8, PX10, PX19 and PX22 (c) PX1, PX7, PX9, PX10 and PX11
	Possibility to violate privacy*	PX1 and PX2
Fairness	Acceptable compromise	PX4, PX7, PX15 and PX18
	Reasonable. *	PX4, PX10, PX14 and PX17
Dependability	Reliability	PX1, PX2, PX4, PX5, PX6, PX7, PX8, PX9, PX18 and PX23
	Trustworthiness	PX2, PX5, PX11, PX15, PX16, PX18, PX21, PX22 and PX23
Enhance relationships	Promoting mutual respect*	PX2 and PX15
	Supporting relationships	PX3, PX4, PX8, PX15, PX17 and PX19
	AUI Promoting multi-user collaboration	PX3, PX4, PX8, PX9, PX10 and PX21

Table 6.9: Participants who Commented on the Reflecting Theme

AUI is successful: All the participants (N=23/23) agreed that the AUI fully or partially protected the privacy of smart home users. Five participants (PX4, PX6, PX11, PX16 and PX17) explicitly stated that it worked well. In the scenario where the main user was accessing health information via the smart speaker (Table 6.1: HLT scenario), PX6 thought it was "really smart" and stated that it is how a smart home should behave: *"That's really smart. That's like what I would expect is smart home to be It's okay. It's, it works out really well",* (PX6[118]). Three participants (PX4, PX15 and PX23) said the AUI did a good job in protecting the privacy of the smart home users. PX23 highlighted its ability to protect user's personal information: *"That's a really important thing to protect your bank credentials. That's really important. So, I believe your smart home system does a really good job tackling those four situations.",* (PX23[161]).

6.3.3.4.3 Ineffectiveness

This section reports how participants found how AUI can be ineffective in some privacy violating scenarios.

Information privacy violation: A few participants (N=5/23) thought the AUI was ineffective in protecting information privacy. Four participants (PX1, PX3, PX9 and PX17) found the scenarios where the main user opened the cupboard using a smart gesture (Table 6.1: OPN scenario) to be ineffective. PX1 stated that it might have leaked the secret gesture, consequently violating the privacy: *"…the alert from Alexa came only after that secret gesture was done, right? So it doesn't matter that Alexa didn't open the cupboard, I still exposed my password basically to someone else in the room who could have seen it and then used it later on.",* (PX1[129]). PX22 thought the AUI's ping sound could make the co-occupant suspicious: *"…if that noise was lower or even non-existent, it could have been better because the second user and during I mean could've felt, could have heard the then always suspect something…."*, (PX22[65]).

Physical privacy violation: Some of the participants (N=9/23 (a)) thought physical privacy could be violated when using the AUI. PX8 reported that the "Bing" sound could be a disturbance: *"…Alexa sends the news to my phone directly, it actually beeps, really loud which is disturbing for someone who's studying…",* (PX8[117]). Five participants (N=5/23 (b)) thought the blurring effect on the scenario where the co-occupant walked in front of the camera during a video call (Table 6.1: FND scenario) might not be enough to blur the person who was passing behind: *"…if it's your flatmate, and it gets blurred, and I'm talking and speaking with you, I might know…",* (PX8[103]). Finally, some participants (N=5/23 (c)) highlighted the ineffectiveness of the initial interaction with the smart speaker. PX1 mentioned that the initial interaction with the smart speaker can cause disturbance to the co-occupant: *"…you have to verbalise your response to Alexa anyway, right? like to me like, it's almost like you disturb that person anyway…",* (PX1).

6.3.3.4.4 Fairness

In this context, *fairness* refers to how participants found the AUI to give equal consideration to the needs of the main user and the co-occupants. Participants reported the AUI provided an acceptable compromise.

Acceptable compromise: A small number of participants (N=4/23) stated that the AUI provided an acceptable compromise. PX7 would accept the AUI as it would allow the participant to achieve his original goal: *"…I could still look at my photos. […] So, the adaptation is a compromise that I welcome."*, (PX7). PX15 stated that he would not mind the compromise as it teaches them to be mindful: *"…there is a bit of more compromised on person one, but I think that high chances are there that they are happy to do it, as it teaches them to be mindful and respectful..."*, (PX15). Finally, PX18 stated the obstruction was acceptable: *"…I don't think it's a big obstruction because it's not like make me uncomfortable in any way..."*, (PX18).

6.3.3.4.5 Dependability

As part of their reflection on the user experience, many participants found the AUI to be dependable in its support for the interactions. Participants highlighted reliability and trustworthiness as dimensions of the AUI's dependability.

Reliability: Most of the participants (N=10/23) found the AUI to be reliable. PX4 mentioned that it was reliable to protect their privacy: *"…I'm saying reliable because […] I feel like I could just ask Alexa and I can rely on the fact […] if there's anyone to be disturbed that will be avoided…"*, (PX4[176]). PX23 mentioned that it worked as expected by protecting smart home users: *"…like it's obvious right? Because that's what the user wants the Smart Home security system to do right? to protect your privacy like especially when it comes to bank details…"*, (PX23[94]).

Trustworthiness: Quite a few participants (N=9/23) stated that the AUI was trustworthy. PX2 stated that they trusted it to give access to personal information: *"…PASHI framework then is sort of its growing into my personal life, and I'm giving it access to my personal life, and I'm trusting it to perform the tasks that I want it to …"*, (PX2[39]). PX21 stated that it was trustworthy as it protects the smart home users: *"…trustworthy because I know that I can actually communicate some kind of intent to the system and have trust that it won't say, it would try to minimise negative outcomes…"*, (PX21[43]).

6.3.3.4.6 Enhance relationships

This section discusses how participants reflected on how well the AUI enhanced the relationships between smart home users. Participants reported that it supported relationships and promoted multi-user collaborations.

Supporting relationships: Some of the participants (N=6/23) highlighted that the AUI helped to maintain good relationships with the smart home users. PX17 reported the importance of it to maintain a good relationship with the co-occupants: *"…it could be a good tool for […] keeping relationships in their home on a steady keel sort of thing…",* (PX17[12]).

Promoting multi-user collaboration: Several participants (N=6/23) highlighted how the AUI supported multi-user collaboration. PX15 mentioned that it made the co-occupants collaborative: *"the technology intervention suggested was friendlier to the other person and also was collaborative in a sense that both the people were able to achieve their task.",* (PX15[30]).

6.3.3.5 Appropriating

In this section, *appropriating* refers to how participants related the AUI with their past experiences and to future experiences. Participants reported that scenarios with the AUI were applicable to their daily lives and highlighted how the AUI could prevent privacy violations, avoid discomfort, and be used during the COVID-19 pandemic. In contrast, a few of the participants reported that some of the scenarios were inapplicable to their daily lives. Table 6.10 summarises the subthemes, sub-subthemes and the participants who made comments regarding each sub-subtheme under the *appropriating theme*.

6.3.3.5.1 Applicability

In this section, I refer to applicability as how well participants found the AUI to be applicable in their daily lives. Participants highlighted how it could be used to protect physical privacy and information privacy. Participants also reported how it could be used to minimise discomfort and how it can be useful during the COVID-19 pandemic. Apart from that, participants compared AUI with the existing smart home devices where they highlighted how AUIs were privacy protective, context sensitive, and personalised.

Physical privacy prevention: A majority of the participants (N=14/23 (a)) highlighted the AUI's applicability to protect their physical privacy. Some of the participants (7/23 (b)) mentioned that it could help reduce auditory disturbances at their homes. According to PX1, it could be used to stop interrupting a co-occupant's personal activities: *"…I have family members who meditate and take part in religious activities that they don't want to be disturbed, but I listen to music out loud sometimes. So, I found that really very useful…", (*PX1[184]). Three participants (PX4, PX5 and PX12) highlighted how it could be used to reduce disturbances caused to the neighbours. PX4 reported how the AUI could help to play music without disturbing the neighbours: *"…the music one […] I can relate to that it could remind me that my neighbours put their kids to bed at whatever time…",* (PX4[247]).

A few participants (PX11, PX12 and PX23) reported that the AUI could help them stay concentrated. PX12 highlighted how it solved his personal requirement of not getting disturbed

while working: *"…I'm a person that gets distracted if there is a video on the computer. […] for me this technology is a good technology."*, (PX12[68]). Lastly, three of the participants (PX10, PX19 and PX21) mentioned that they would like to use the AUI to enforce privacy rules in public or shared spaces. PX10 thought it could be used to manage the disturbances caused by his son at his home: *"…my son, who pretty much only listens to mumble rap these days. And sometimes I'm just not in the mood to be listening to mumble rap and the system reminding him to put on his damn headphones because I'm working…"*, (PX10[160]).

Subthemes	**Sub-subthemes** (* denotes subtheme reported in appendix)	**Participants who made comments**
Applicability	Physical privacy prevention	(a) PX1, PX2, PX4, PX5, PX8, PX10, PX11, PX12, PX13, PX15, PX19, PX21, PX22 and PX23 (b) PX1, PX2, PX8, PX11, PX13, PX21 and PX22
	Information privacy protection	(a) PX4, PX5, PX8, PX10 and PX15
	Avoiding discomfort	PX8, PX10, PX13, PX18, PX22 and PX23
	COVID-19	PX1, PX2, PX5, PX6, PX8, PX11, PX14 and PX18
Inapplicability		PX2, PX6, PX4, PX7, PX9, PX10, PX15, PX17 & PX21
Comparison	Privacy protection*	PX9, PX12, PX14, PX16 and PX23
	Personalisation*	PX7 and PX9
	Context sensing*	PX4 and PX9
	General comparison*	PX3, PX6, PX16 and PX21
Impact on self	User-awareness of problems*	PX12 and PX22
	Improvement to life*	PX19, PX21 and PX22
	Using in the future*	PX7 and PX10

Table 6.10: Participants who Commented on the Appropriating Theme

Information privacy protection: Some participants (N=5/23) highlighted the AUI's applicability to protect their information privacy. Some of these participants (PX4, PX5, PX8, PX10 and PX15) highlighted how it could be used to mask sensitive video content in their smart homes. PX10 explained how it could have been useful in protecting his information privacy during conference calls: *"…I was just in my underwear and I was in a conference call. […] my bell rang […] as I ran up […] someone could see that I was in the meeting in my underwear, […] I think a setting where just would have blurred it out the moment I started standing up…"*, (PX10[189]). Furthermore, a couple of participants (PX8 and PX9) thought that the AUI could be used to mask private information communicated via auditory channels. PX8 mentioned how the AUI could help to avoid his flatmate's sensitive conversation with the therapist being shared: *"…one of my flatmates goes to therapy […] she's told […] us it is actually really difficult to talk about what's going on. […] I can see these kinds of devices working in that scenario..."*, (PX8[178]). Lastly, a couple of participants (PX11 and PX23) mentioned that it could be used to protect information privacy when learning from home: *"…one of the parents might say something really embarrassing out loud while we are answering your question during a zoom meeting […] it can like, blur, mute the [...] other person's voice…"*, (PX23[167]).

Avoiding discomfort: Some of the participants (N=6/23) highlighted how the AUI could be used to avoid discomfort in their life. PX8 thought it could help to protect kids from getting shocked: *"…when you're […] logged into your YouTube account, you can get some ads. That might not be good for […], my nephew…"*, (PX8[169]). PX23 thought it could help teenagers with their social anxiety problem where they could navigate awkward social interactions with the help of AUI: *"…it's really relevant in the 21st century specially because like a lot of people living with social anxiety and do not wish to be engaged in like a certain conversation in his free time…"*, (PX23[137]). A few of the participants (PX10, PX13, PX18 and PX22) thought adaptive blurring in a professional setting could avoid unnecessary interactions: *"…in a company environment that everybody has the background somehow blurred or the people who are going through a blurred, so you don't need to explain that..."*, (PX13[166]).

COVID-19: Most of the participants (N=8/23) highlighted how the AUI could be quite useful during the COVID-19 pandemic. PX22 described how adaptive blurring can be useful: *"… most important scenario would be the one of the blurry backgrounds especially in these COVID lockdown times. …"*, (PX22[84]). A couple of participants (PX2 and PX7) reported that adaptive blurring could minimise disturbances happening to the co-occupant when working from home: *"…I definitely have walked past […] my wife's Skype when she's in a business call people. […] having a blurred thing in that scenario could be really powerful…"*, (PX7[150]).

6.3.3.5.2 Inapplicability

In the context of this work, *inapplicability* refers to participants' comments on how specific scenarios or adaptations are not applicable in their life. Some of the participants found the bank scenario, slide scenario and the football scenario to be not applicable in their life as they might not use the smart home or a smart service in that way.

Quite a few participants (N=9/23) reported that some of the scenarios did not resonate with their personal lives. A few of the participants (PX10, PX17 and PX21) reported that they would not use a smart speaker to access their bank: *someone wouldn't ask a voice assistant about like bank details.",* (PX21[27]). Some of the participants (PX2, PX6, PX7 and PX15) did not find the slide scenario to be much of a privacy concern. PX6 thought showing images on the TV might not be a privacy violation: *"…the scenario was showing only the pictures on screen. […] I don't think that there was much danger on the privacy.",* (PX6[61]). A few of the participants (PX4, PX7 and PX9) did not resonate with the football scenario. PX4 stated that he would check football scores on his phone rather than on a smart speaker. *"I would probably check the sports results much more on my phone anyway...",* (PX4[238]).

6.3.3.6 Recounting

In this section *recounting* refers to how participants considered the AUI in the context of other experiences, alternate versions of the experience that they wished to have and predictions that might happen. Participants suggested improvements to the AUI which included features such as an audio masking feature, improved notifications, and warnings. Furthermore, participants reported possible adverse effects where the AUI could impact relationships. Lastly, participants mentioned possible negative adaptations such as denial of service and unexplained adaptations. Table 6.11 summarises the subthemes, sub-subthemes and the participants who made comments regarding each sub-subtheme under the *recounting* theme.

6.3.3.6.1 Suggestions

This section reports the *suggestions* made by participants. Participants suggested ways the AUI can improve notifications and warnings delivered to the user. One participant also mentioned that it is better to remind the user at the end of the day how and when their privacy was protected by the PASHI framework.

Audio masking: Some participants (N=5/23) suggested that audio masking would be a good feature to have on video conferencing tools. PX19 stated that she would like to have a feature to mask the noise while on video calls: *"…in terms of video conferencing […] I hope […] I could […] mute you and mute me and all this […] It's almost like there's this like little sound…",* (PX19[121]).

Subthemes	Sub-subthemes (* denotes subtheme reported in appendix)	Participants who made comments
Suggestions	Reversibility*	PX4, PX8 and PX11
	Audio masking	PX1, PX6, PX7, PX17 and PX19
	Improved notifications and warnings	PX1, PX5, PX6, PX7, PX8, PX12, PX13, PX21 and PX22
Adverse effects of AUI	Impact on relationships	PX2, PX7, PX9, PX10, PX13, PX19 and PX23
	Restricting critical interactions*	PX19 and PX23
Possible negative adaptations	Denial of service	PX2, PX3, PX4, PX5, PX6, PX7, PX10, PX11, PX13 and PX21
	Unexplained	PX2, PX5, PX13, PX15 and PX18
Applicability and Beyond	Usage in smart cars*	PX16 and PX21
	Commercial value*	PX14 and PX15

Table 6.11: Participants who Commented on the Recounting Theme

Improved notifications and warnings: A considerable number of participants (N=9/23) commented on improved notifications and warnings. Several participants (PX1, PX5, PX6, PX12, PX21 and PX22) suggested ways to improve how the AUI delivered notifications and warnings. Some of the participants (PX1, PX5, PX6, PX12, PX21 and PX22) suggested discrete notifications to denote the adaptation. PX22 suggested inaudible notification is suited to avoid unnecessary suspicions from the co-occupant: *"…I would remove the sound completely on the Smart Home device* (PX22[71]). Some of the participants (PX7, PX8, PX12 and PX13) thought it was better to use the smart speaker's existing light to notify possible privacy violations: *"… Alexa […] could show some kind of visual indication that there is somebody nearby and that it's going to […], make a privacy move…".* (PX7[93]). Three of the participants (PX3, PX14 and PX19) thought the AUI could be used to warn people before entering spaces. PX19 stated that it could warn the user of possible privacy violations in a room with a conference call: *"…I'm using this space right now. If you want to be part of it, then you deal with the consequences…",* (PX19[114]).

6.3.3.6.2 Adverse effects of AUI

The following section reports what the participants thought to be the possible *adverse effects* of the AUI. Participants described how it could have a negative impact on relationships with the smart home as well as outside the smart home.

Impact on relationships: Some of the participants (N=7/23) highlighted how the AUI could have a negative effect on relationships. Three of the participants (PX9, PX13 and PX23) thought the adaptive blurring feature of AUI might disrupt relationships. PX13 thought the person on the other end of the call might get annoyed as they are avoided: *"If you are on a private environment, it's*

[…] somehow difficult. […] Because it's [...] like you are like cutting the relationship to the person…", (PX13[170]). A couple of participants (PX2 and PX19) thought the AUI might remove plausible deniability when someone else's privacy has been violated. This is because, in an area where the PASHI framework is implemented, if someone denies the AUI's suggestion and decides to violate the privacy that person would be held accountable. PX19 thought she could blame someone on the train for ignoring the adaptation: *"… I know that everyone kind of has this and that the person next to me Finally got a notification saying, Are you sure you want to play this out loud you're in a bus. […] if they then said, Yes, […] now I blame the person.",* (PX19[92]).

A couple of participants (PX7 and PX10) thought the AUI could be used to control their kids. Even though this is a good use case for the parents, it could have an adverse effect on the kids as they are restricted. PX7 wanted to use the AUI to mute kids while on conference calls: *"… you can switch off audio or switch on […] and I'm wondering if you can like, pick out particularly voices, for children …* (PX7[190,191,192]).

6.3.3.6.3 Possible negative adaptations

During the study, participants were asked to comment on adaptations that they would not have liked, and the following section covers those findings. Participants highlighted that a denial of service to the smart home adaptations without explanation would be negative adaptations.

Denial of service: Many of the participants (N=10/23) thought completely stopping an interaction would be an undesirable adaptation. PX11 mentioned the AUI stopping the interaction as there another co-occupant, might be undesirable: *"I guess no service at all would be unacceptable and if I like to just remain mute and did nothing because mom is in the room...",* (PX11[113]).

Unexplained: Some of the participants (N=5/23) stated that an adaptation without the explanation would generate a bad user experience: *"…if it switched automatically without asking. Or it doesn't play and doesn't say anything. Just it doesn't work and you don't know why...",* (PX13[151]).

6.3.3.7 The success of the study

The following section reports the factors that contributed to the success of the study. A majority of the participants reported that they resonated well with the scenarios and some of the participants commended the quality of the videos. Table 6.12 summarises the subthemes and the participants who made comments regarding each subtheme.

Subthemes	Participants who made comments
Resonating with at least one of the scenarios	All the participants
Quality of the videos	PX1, PX2, PX3, PX6, PX7, PX8, PX11 and PX17

Table 6.12: Participants who Commented on the Success of the Study

Resonating with at least one of the scenarios: Most of the participants (N=23/23) reported that all of the scenarios resonated with them, and all of the participants reported that at least one scenario resonated with their daily lives. PX2 was quite happy with the scenarios/videos as they demonstrated the use cases really well. *"The scenarios were quite good at demonstrating why you might actually want them.…",* (PX2[222]). PX1 resonated with meditation scenario quite well: *"I really like the first scenario with the music because I do have people in our household who operate at different rhythms and people who do work on very deep work…" ,* (PX1[184]). PX4 stated that he resonated well with the Netflix scenario: *"… I've got quite a few friends who've got children who have their Netflix with a mixture of their kind of what they want to watch and what their children watch on Netflix...",* (PX4[233]). PX12 resonated well with the slide scenario as it is demonstrated a personal experience of the user: *"… this technology will greatly help people stay concentrated. I'm a person that gets distracted if there is a video on the computer…",* (PX12[68]). PX4 resonated well with the safe scenario as: *"And the pin number in the background […] I understand that sort of manipulating the image to protect people's privacy is a really good idea.",* (PX4[234]). PX2 resonated well with the friend scenario as he has personal experience with conference calls where his partner appears on the camera's view. *"…there's times when I am on a call and [my wife] wants to like come in ask me if I want tea and stuff like that. And she's not sure where to stand…",* (PX2[230]). PX9 resonate well with the HLT scenario as it was relatable to a personal experience. *"…some outside person is at my home […] Alexa is just reminding me about the reminders that I have already set up. So that kind of situation is embarrassing.",* (PX9[52]).

Quality of the videos: More than a third of the participants (N=8/23) highlighted that the videos are of high quality. Three participants (PX2, PX6 and PX11) were quite pleased with the attention to detail of the videos. PX2 was impressed with the gradient of the volume: *"I thought to myself, this will be really cool if when I put the headphones on, the volume goes up. […] that attention to detail is really good...",* (PX2). PX13 mentioned that the videos of professional quality: *"… the videos were really nice and very proper professional.",* (PX13). A couple of participants (PX7 and PX8) thought the videos were realistic and they were able to see minor details of the videos such as the password: *"…I thought I was seeing your password on the video…",* (PX8). Three of the

participants (PX1, PX2 and PX3) went on to discuss the underlying technology of AUI and it was a sign of quality video where they were prompted think beyond what they see: *"… it would have to be some kind of like Bluetooth detection or Wi-Fi detection. Running a lot of the time or maybe there's door sensors or something like that…"*, (PX2).

6.3.3.8 Threats to Validity

The following section reports the aspects of the study which could be a possible threat to the validity of the findings. Participants comments highlighted that some have not resonated well with specific scenarios or that they have not understood specific scenarios. Furthermore, the comments implied some drawbacks of the video prototypes and the participant biases that could have impacted the results. In addition, a participant mentioned how a person's culture and their living condition (shared/living alone) can biases participants comments. Table 6.13 shows the summary of subthemes of theme *threats to validity* and participants who made comments under each sub-theme.

Subthemes	**Participants who made comments**
Not resonating	PX1, PX2, PX6, PX7, PX10, PX11, PX15, PX19 and PX23
The shortcomings of the videos	PX4, PX7, PX8, PX10 and PX18
Didn't understand or unaware	PX6, PX7, PX8, PX22
Issues with the questionnaire and the study structure	PX1, PX3, PX6, PX9, PX12, PX15 and PX18
User biases	3PX4, PX10 and PX23

Table 6.13: Participants who Commented on Threats to Validity of the Study

Not resonating: Some of the participants (N=9/23) reported that some scenarios did not resonate with them. Scenarios such as the slide scenario, open sesame scenario, bank scenario and football scenario were not well received by some due to the unfamiliar nature of the scenarios. For example, PX6 did not resonate with the slide scenario as the privacy violation was not justified: *"… especially for pictures, I found it a bit over the top..."*, (PX6[18]). PX6 did not resonate well with the bank scenario as he would not have used his bank in that manner: *"…I don't feel like saying a password as it should be a secret …"*, (PX6[177]). PX1 did not resonate with the football scenario as she was not a football fan: *"…I'm not a football fan as such. So I struggled to kind of associate with the scenario…"*, (PX1[91])

The shortcomings of the videos: Some of the comments were specific to the study, where some of the comments were around the drawbacks of video prototypes in general. Five participants (5/23)

highlighted the drawbacks of video prototypes. PX10 was not sure about the noise absorption of the walls, which was a drawback of video prototypes: *"…I don't know how good the noise absorption is of the door and if someone could just hear it from outside as well..."*, (PX10[73]). PX18 struggled to identify the source of the notification as it was difficult to convey via the video: *"…I'm not sure from where the sound came from…"*, (PX18[193]). PX7 told he was unable to evaluate different versions of the scenario where adaptations were different: *"…I don't know what would happen if I'd have just not pressed on the button…"*, (PX7[40]). PX8 highlighted the lack of interactive nature of videos: *"…when you get the message on your smartwatch, I don't know if you can reply or do something..."*, (PX8[38]). PX10 was a bit confused with the wording of the video. *"…the language a little confusing…"*, (PX10[98]). PX14 mentioned that the video's description went a bit faster. *"Wait, it went by a little quick for me to read it."*, (PX14[10]).

Didn't understand or unaware: The comments of four participants (N=4/23) implied that, they didn't understand some of the scenarios. PX8's comments showed that he did not understand the scenario rule-setting aspect of AUI: *"…let's say it is my wife, and I'm at home and we're sharing a bank account […] I know the password. She knows the password […] it's okay…"*, (PX8[81]). PX16's comments highlighted that he was not aware of the AUI's capability of picking the most appropriate device to deliver messages: *"…I get a notification on my smartwatch? What if I wasn't wearing a smartwatch?…"*, (PX16[65]). PX9's comments showed that he had not understood the part about the main user not knowing the second user's preferences: *"…if you know that the second person does not like being disturbed why would first person asked that question from Alexa in the first place…"*, (PX9[141]).

Issues with the questionnaire and the study structure: Some participants (N=7/23) mentioned they had issues with the style of the questions and some of the comments implied that they had problems with the study structure as well. A couple of participants (PX3 and PX18) were not clear about the definition of privacy. PX18 was not familiar with physical privacy: *"From my understanding about the privacy. It's like related to my information…", (*PX18[27]). Five of the participants (PX1, PX6, PX9, PX12 and PX15) stated the alternative question pattern (negative to positive) was a bit confusing: *"… I don't do well, too well with the double negatives..."*, (PX1[66]).

User biases: Some of the participant biases might have impacted their comments. Three of the participants (N=3/23) mentioned that they didn't like Smart homes. PX10 thought the AUI was not mature enough: *"…a lot of the Smart Home stuff is sort of gimmicky right…"*, (PX10[179]). Participants who had a strong security research background were biased towards identifying information privacy violations as opposed to physical privacy violations. PX18 mentioned he was only aware of information privacy: *"Information privacy is the only privacy currently I know."*, (PX18[282]). A couple of participants (PX6 and PX19) mentioned that they not concerned about their privacy: *"I will be relaxed about my privacy …"*, (PX6[230]).

6.3.4 Chapter Summary

This chapter evaluated the user experience of AUI generated from the PASHI framework using a video prototype-based user study. This section provides a summary of the research findings.

Personal privacy preferences impacted the user experience of the AUI: Participants had different opinions of the balance between usability and privacy, real-time control of privacy, the balance between information privacy and physical privacy. These preferences impacted how participants perceived the experience of the AUI.

Clear, simple, and explained aspects of the AUI were highly appreciated: Participants appreciated the clear and simple user interfaces of the AUI as they helped them to easily accept adaptations. They also commended the explanations provided by the AUI when an adaptation happened.

Having control and flexibility over the AUI was preferred but it varied depending on the context: Whenever possible, the participants preferred to have control and flexibility over the AUI. One of the main reasons the CAUI had 100% positive reactions was the high-level of control that it provided to the user. In contrast, some of the participants thought it was unimportant to have real-time control of privacy when the adaptation's efficacy was time-dependent or when the AUI is protecting a privacy preference with high importance.

Overall, the AUI was easy to navigate: Participants highlight that AUI was easy to navigate because it was easy to learn, reduced the cognitive load and was seamless.

The AUIs were highly applicable to mitigate interpersonal privacy violations and were much better compared to existing smart home devices in specific dimensions: A majority of the participants resonated with all the scenarios where they mentioned how AUIs can be used to address similar situations in their daily lives. In addition, they compared the AUI with existing smart home devices to show how the AUI exhibited improved privacy protection features and usability.

The AUIs supported maintaining relationships and generally were fair to all the smart home users: Participants highlighted how the AUI promoted collaborations and respect between multiple users. Participants also thought that the AUIs were fair to smart home users in most of the cases, but in some instances, the AUIs were considered to be too paternalistic and restrictive.

The AUIs were effective and dependable: Most of the participants thought the AUIs were effective in protecting interpersonal privacy. They also thought the AUIs were dependable and trustworthy, meaning that they acted in a consistent and predictable manner.

Participants suggested ways to improve AUI: They thought having an audio masking feature would be valuable. They also suggested improving the notifications and warnings to be more discreet.

The following chapter will discuss the findings from the video prototype study and the findings from the storyboard study reported in the previous chapter.

7. Discussion of Usability and User Experience Evidence

Chapter 5 presented the storyboard-based user study conducted to evaluate the adequacy and usability of the AUI. This study evaluated two variations of the AUI (excluding the non-adaptive user interfaces) when applied in two interpersonal privacy-violating scenarios where each variation represented a variety of interpersonal privacy violations (information and physical privacy). The study highlighted valuable usability-related findings of the different AUI variations and the contexts they are applied in. In addition, it motivated further inquiry to understand the overall user experience of the AUI when applied in different contexts. Hence, a video prototype-based user experience evaluation study was conducted and reported in Chapter 6. The user experience evaluation study used the findings from the storyboard-based usability study and created scenarios that provided high fidelity representations of the AUI variations, interpersonal privacy variations, user preferences, and smart home contexts which also provided a much more realistic experience. The findings of both studies are discussed together in this chapter, to have an in-depth understanding of the usability and the user experience of the AUI, and the adequacy of the AUI in protecting interpersonal privacy. It is important to highlight that both the studies were exploratory rather than confirmatory in nature. Therefore, the findings are not conclusive but provide a better understanding of how adaptive user interfaces could be used to address interpersonal privacy in smart homes, together with design guidelines and directions for future studies.

7.1 Introduction

The storyboard-based study evaluated the usability of the AUI while the video prototype study evaluated the user experience of the AUI. Both the studies evaluated the AUI's adequacy in protecting interpersonal privacy and other themes surrounding interpersonal privacy. In addition to the aforementioned high-level themes, the participants' comments on ways to improve the AUI were also evaluated. This chapter discusses the findings of the two user studies, divided into three parts:

i) the usability and the user experience of the AUIs (§7.2);

ii) privacy protection and control of the AUIs (§7.3);

iii) suggestions made by the participants on how to improve the AUIs (§7.4).

In addition to the discussion of study findings, this chapter discusses the methodology used for both the studies (§7.5).

7.2 Usability and User Experience

7.2.1 Expectations and Predictability

Users' expectations regarding the AUI's operational behaviour (predictability) and affordances influence how they experience the smart home. According to McCarthy and Wright (2004), users approach technology-mediated interactions with certain expectations based on their prior experiences. These expectations influence their user experience, in this case, the user experience of the AUI. In addition, users create mental models of the behaviour of a system as they interact with it, but this becomes harder with the AUIs, because the interface may change as the context changes. This may create confusion, which reduces the trust in the system, as it is harder to predict how the interface adapts (Duarte, 2007). To help the users of smart systems manage their expectations, Amershi et al. (2019) suggested letting them know of the system's capabilities and efficacy. In addition, providing *help and documentation* regarding the system may also help the users to understand how the system works, leading to better usability (Nielsen, 2005). This section discusses the implications of user expectations regarding its operational behaviour and affordances on the user experience of the AUI.

Findings

Adaptations were often unexpected and hard to predict, but their affordances were highly appreciated. As mentioned in the methodology section of the video prototype study, the participants were provided with two videos prior to the study, as well as the participant information sheet. Each video represented a variation of privacy (information privacy or physical privacy). This was the only orientation provided to the participants, and it would not have highlighted all the possible privacy violations or all the possible variations of AUIs. Following this orientation, some of the participants (N=5/23) went on to explain that they were pleasantly surprised as they were not expecting the AUI to be this good.

In contrast, some participants (N=4/23) had uncertainties over the AUI, where they thought the timing, or the manner of the adaptation, was not predictable with the two videos they have seen before. This unpredictability of the AUI was highlighted in one of the questions in the post-scenario questionnaire which evaluated the level of predictability of the user interface adaptation. On average, video prototype study participants disagreed with the statement: *"I expected the user interface adaptation before it happened"*, giving it a modal score of 2 (the maximum of the Likert scale was 5 - *highly agree*). This showed that majority of the participants did not expect the

adaptation. Overall, the findings highlighted that the participants were impressed with the AUI's affordances and execution, but they struggled to predict the AUI behaviour consistently.

Discussion

These findings were in line with Duarte's (2007), as participants had difficulty in predicting the AUI's behaviour. However, this seemed to be partially mitigated by the orientation videos provided prior to the study that demonstrated the AUI's behaviour and capability; this aligned with Amershi et al.'s (2019) guidelines for better Human-AI interaction and Nielsen's heuristic (2005) about providing *help and documentation*. Even though the adaptations were harder to predict, the benefits provided by the AUI seem to have improved the user experience. This point was made by Duarte (2007), who suggested that AUI users might look past the inconsistent (adaptive) nature of the interface when the perceived benefits are significantly higher.

The findings demonstrated how the user expectations (behaviour and affordances) regarding the AUI influenced the user experience. Extending the initial two videos used in the study to develop a detailed orientation for first-time users may help to manage their expectations, consequently improving the user experience. This orientation should be developed carefully to be representative of the AUI's adaptation types, the AUI's features (timing, notification etc) and different scenarios to which the AUIs can be applied. This orientation should be appropriate and user friendly (e.g., brief, succinct, and understandable without technical knowledge), improving the likelihood that users will actually view/interact with it to reap the full benefits.

In conclusion, the PASHI framework should provide the right level of orientation (prior to the interaction) and feedback (during the interaction) to help users manage their expectations, thus improving their experience of the AUI (§8.6: R3).

7.2.2 Privacy Preferences Affecting UX of Adaptive User Interfaces

The level of support provided by the smart home for accommodating different privacy preferences (both information and physical privacy) and the privacy preferences themselves affected the user experience. Westin (1967) presented three high-level information privacy personalities: *privacy fundamentalists*, *privacy unconcerned*, and *privacy pragmatists*. *Privacy fundamentalists* have strong privacy values and take the viewpoint that their privacy has been lost, and they are reluctant to take actions that may further violate their privacy. *Privacy unconcerned*, as the name suggests, do not worry about their privacy. In the middle of this spectrum is *privacy pragmatists* who take a practical approach toward using technology-based services, weighing the costs and benefits. These personality types can be used to analyse different privacy preferences smart home users may have. There is no standard taxonomy for physical privacy personalities, but the literature discusses some

of the user preferences regarding physical privacy. For example, Lee (2010) found in his study that participants prefer face-to-face interactions as opposed to computer-mediated communications because they are more effective. This section discusses how user's information and physical preferences and the support provided by the AUI for these different privacy preferences affect the user experience.

Findings

Interpersonal privacy preferences impacted the user experience of the AUI.

Two of the video prototype study participants (N=2/23) stated that they didn't care about protecting their privacy, as they thought it is too difficult to protect individual privacy against existing internet service providers, or they didn't want to hide information from others. Another set of participants (N= 8/23) had varying opinions over the criticality of privacy, where some thought a specific type of information was more important than another. For example, a participant thought bank credentials were critical information that needs to be protected, while another was not concerned about protecting what they were watching on Netflix. Furthermore, a participant mentioned that they did not care about having run-time control of privacy as they cared more about their privacy being protected as opposed to having run-time control. Some of the participants (N=6/23) preferred using direct interactions with the co-occupant to manage interpersonal privacy violations over an AUI-mediated interaction. Triangulating these findings, the reaction card findings found that the majority of the participants thought the AUI was *personal,* indicating that it was adapted to the user's preferences. Findings demonstrated that different participants had varying preferences regarding how they want to manage their interpersonal (information and physical) privacy. This led some of the participants to appreciate the privacy-preserving aspects of the AUI, where some of the features were an obstruction. Therefore, factoring in the interpersonal privacy preferences to the AUI and providing the ability to override the AUI suggestions are pertinent to the AUI user's experience.

Sometimes protecting physical privacy may violate information privacy. A very few participants (N=3/23) thought that disclosing what they were doing to other co-occupants would be paradoxical. This was only reported in the meditation scenario (Table 6.1: MED scenario), in which the co-occupant had to share their current activity (possible information privacy violation) with the other co-occupants to maintain their physical privacy. Letting everyone in the smart home know what a specific user is doing could be a privacy violation if that user wants to keep that information private. Therefore, there is a risk of the AUI's physical privacy protection introducing information privacy violations.

Discussion

Most of the privacy preferences aligned to existing privacy personalities in the literature. The participants who did not care or thought they could not protect privacy fell into the *privacy*

unconcerned category (Westin, 1967), and they were not interested in having the AUI integrated into their smart homes. This implied that the AUI might not be accepted by all the smart home users. On the other hand, users having different viewpoints regarding the criticality of privacy based on the type of information and the preferences regarding immediate privacy control fell into the *privacy pragmatists* category. In addition, the participant's preference to have direct interaction with the co-occupant to resolve a privacy conflict was partially in line with Lee's findings (2010). Lee's findings helped to explain how some people prefer to use face-to-face interactions to resolve problems, rather than allowing the AUI to solve them. Overall, the findings highlighted the need for an in-depth inquiry into different privacy personalities within ubiquitous computing and more descriptive privacy preference modelling by the smart home. As demonstrated in Chapter 4, the PASHI framework supports these nuanced privacy preference personalities via its flexible privacy preference model. This enables more users to integrate their privacy preferences into the PASHI framework, allowing a better user experience of the smart home and the AUI.

The findings highlighted the need to have a careful balance between different types of privacy preferences to protect interpersonal privacy as a whole. A user wanting to hide specific details regarding their current activity (in this case, meditation) from the co-occupants to achieve physical privacy was partially in line with the GDPR's principle of data minimization (https://gdpr.eu), even though GDPR is not directly applicable to interpersonal privacy. Even though it is not the same, a slightly similar idea was considered by Such, J., & Criado, N. (2018) where they discussed the term multi-party privacy on social networks. The authors highlighted how social network users may co-own sensitive information with a group of people and one person disclosing this information may violate other group members' privacy. This was not discussed in Westin's privacy personalities which cover information privacy whereas these findings focus on interpersonal privacy. A possible solution for this issue is to disclose enough to stop someone else from playing music but not to disclose the exact activity. Therefore, disclosing an appropriate amount of information for the required tasks could be a solution in such situations. In this way, participants' overall interpersonal privacy will be protected.

The existing privacy preference model of the PASHI framework supports conflict resolution between privacy preferences, but the studies conducted did not explore any such scenarios. This motivates further studies to identify different interpersonal privacy preference conflicts and to investigate the efficacy of the model in resolving the identified privacy preference conflicts.

In conclusion, user's privacy preferences and the accommodation for those privacy preferences by the AUI influenced the user experience. Participants had different types of privacy preferences, and some of them were competing with each other. The PASHI framework was able to support most of these nuances and rich privacy preferences, but further investigation is required on privacy preference conflicts. Therefore, future studies should investigate the completeness of the privacy

preference models and their capability to handle different types of privacy preference conflicts (§8.6: R1). In addition, allowing users to author their privacy preferences would enable more users to have a better user experience, as they would be able to define their preferences without the help of a system administrator (§8.6: R2).

7.2.3 AUI 'Look and Feel'

The initial interaction that a user has with the user interface influences how they experience the system; hence the 'look and feel' of the AUI is pertinent to the user experience. Three of Nielsen's suggestions (2005) can be used to discuss the participant responses regarding the 'look and feel' of the AUI:

- *Recognition rather than recall* suggests reducing the cognitive load of the user by explicitly providing available options and information, so the user does not have to remember information from previous steps.
- *Aesthetic and minimalistic design* suggests removing unnecessary or rarely needed information from the user interface design.
- C*onsistency and standards* suggest maintaining the meaning of different user interface attributes consistent throughout the interaction as users do not have to think every step of the way to figure out the meaning.

Further, a limited study has shown that smart homes demonstrating 'human-like' characteristics would improve users' experience (Mennicken and Huang, 2012). One of these characteristics is for the smart home to show caring behaviour when interacting with its users. This section discusses how different aspects of the AUI's 'look and feel', and the 'human-like' characteristics, were perceived by the participants and how they affected the user experience.

Findings

The AUI's clear representation of information and choices and use of familiar user interface components improved the user experience. The video prototype participants praised the simple, clean, and organised nature of the AUI (N=6/23) and the familiarity of some of the AUI's features (N=8/23). Clear presentation and separation of options – in the scenario where the main user tried to play music while the co-occupant was meditating (Table 6.1: MED scenario) – was highly praised by more than a quarter of the participants (N=6/23), as it made the decision making convenient. Participants also highlighted how simple the adaptation was with fully-automatic adaptative-UI scenarios such as the Netflix scenario (Table 6.1: NFX scenario) and the scenario where the background was blurred during the Skype call (Table 6.1: FND and SFE scenarios). Some of the participants (8/23) reported that the AUI behaviour was familiar, as it uses existing technologies such as background blurring technologies and photo browsing tools. These comments

were corroborated by the user reaction card results, as most of the participants picked reactions such as *convenient, simplistic, and organised* (presented in order of frequency) to describe the AUI.

The AUI's personalised, approachable and friendly characteristics improved the user experience. The video prototype participants highlighted how the explanations provided to the user made the AUI approachable and friendly, and how customisation to each individual and the context made it feel more personalised, consequently making users' interaction with the smart home more comfortable. These comments were corroborated in the reaction cards results, as most of the participants picked reactions such as *helpful, personal,* and *friendly* (descending order in the frequency of occurrence) to describe the AUI. Although this needs further exploration, the smart home (or the AUI) mimicking 'human-like' courteous characteristics seems to improve the user experience. Participants highlighted how the AUI providing explanations regarding the adaptations, providing choices, and asking permission before the adaptations made them consider the AUI to be more courteous compared to existing user interfaces. Therefore, personalised adaptations delivered in a consensual and flexible manner improved the user experience.

Discussion

Participants' appreciation of clear representation of information and the use of familiar user interface components were in line with the literature (Nielsen, 2005). Clear presentation of information seems to help the users consume information easily and select an appropriate adaptation without information-overload or decision fatigue. The use of familiar user interface components helped the users 'recognise' interaction segments rather than 'recall' them or figure them out from scratch, consequently improving the usability. Therefore, the clear presentation of information and using familiar user interface components contributed to the usability of the AUI.

The AUI's human-like courteous characteristics improved the user experience and this was partially in line with the literature (Mennicken and Huang, 2012). When the AUI

- personalised the interaction with the user,
- explained reasons for adaptations,
- asked for consent before an adaptation,

participants felt the AUI mimicked human characteristics complementing the interaction that they have with the smart home. These characteristics of the AUI seem to improve the trust between the smart home and the user, consequently improving the user experience. This finding is not conclusive and requires further investigation, as the video prototype study conducted a broad evaluation of the user experience rather than focussing on specific characteristics (in this case human-like features) of the AUI.

In conclusion, the recommendations are to:

- keep the AUI minimal and organised, and extend or use existing interaction methodologies (e.g., background blurring technology of video conferencing calls) with the AUI (§8.6: R4); and
- integrate courteous characteristics to the AUI and conduct further empirical research to determine which types of courteous characteristics of the AUI improves the user experience and to understand the interplay between different characteristics (§8.6: R5).

7.2.4 Efficiency and Ease of Navigation

The adaptive nature of the AUI makes it efficient as the interface is adjusted to the user's goals, which positively contributes to the user experience (Duarte, 2007). On the other hand, this adaptive nature makes the AUI disrupt the user's interaction with the system, which may affect the user experience negatively (Duarte, 2007). Nielsen's usability heuristics (2005) help to evaluate the dimensions that may relate to the efficiency and ease of navigation of the AUI. The heuristics that were mentioned in the previous section (§7.2.3: *recognition rather than recall, aesthetic and minimalistic design, and consistency and standards*) are also applicable under this theme. In addition, the *flexibility and efficiency* heuristic also support this evaluation. This section discusses the findings across the two studies related to efficiency and the ease of navigation of the AUI and its variations.

Findings

Both the AUI variations AAUI and CAUI provided efficient privacy-protected interaction affordances to the smart home users. Storyboard study participants thought the AAUI was efficient compared to CAUI as it was simpler, required a smaller number of steps, and was not time-consuming. Even though CAUI was time-consuming when compared with the AAUI, on its own CAUI reduced the cognitive load by giving fewer steps while giving choice to the user. Both the AAUI and the CAUI were efficient AUI variations, where the CAUI provided the choice regarding the adaptation with a slight trade-off regarding the efficiency. Therefore, depending on the smart home user's requirement and preferences, both these variations provide adequate means to efficiently achieve user goals in a privacy secure manner.

Overall, the AUI was efficient and made privacy-secure smart home interaction easier. Participants of both the studies thought the automatic privacy protection of the AUI was easier to interact with where AUI made the complex task of user interface adaptation simpler. Overall, the video prototype study participants thought the AUI reduced the cognitive load on the users by automating the interaction (in both fully automatic adaptive-UI and semi-automatic adaptive-UI). Participants were fascinated by the quick reaction times and the predictive nature of the AUI. Due to this, some of the participants (N=10/23) thought the "AUI was quite cool" and expressed a

desire to have it integrated into smart home devices and services. As mentioned previously, (§7.2.3) the 'look and feel' of the AUI supported ease of interaction. Participants thought the AUI was easier to learn because it extended or used existing technologies. Furthermore, participants thought AUIs were self-explanatory due to their simpler design and explanations. Most of the participants selected positive reactions to define the AUI experience (89% out of all the reactions were positive reactions), and the most selected reactions were *easy to use, fast, efficient,* and *straightforward.* In addition, the participants disagreed strongly with the statement '*user interface adaptation obstructed the user experience of using the smart home',* where the answers had a mode of 1 where 1 means highly disagree (and the maximum 5 means highly agree). This implied that the AUI didn't obstruct the user experience of the smart home. Usage of familiar technologies, simpler design, explanations for adaptations, and automation made the interaction with the AUI easier, while the predictive nature of the AUI and automatic privacy-protective adaptations made the interaction efficient. Therefore, the AUI can be considered to be an efficient and effective form of user interface for privacy-secure smart home interactions.

The AUI was seamless and discreet. Most of the video prototype participants (N=11/23) thought that the AUI was seamless. They commended the seamless adaptations where the main user was allowed to achieve their tasks without trading off the usability. They also appreciated the seamless notifications which were delivered at the right time in the right manner without disturbing other co-occupants. Adaptations are generally disruptive and may cause disturbances to the main user and the bystanders, but the findings highlighted how the seamless adaptations and discreet notifications of the AUI minimised the possible disruptions. Therefore, the AUI seems to accommodate smooth and effective interactions between the user and the smart home while minimising disruptions caused to the bystanders.

Discussion

Most of the comments made by the participants in both studies were in line with the literature while a small number of comments disagreed with the literature. The a*esthetic and minimalist design* heuristic (Nielsen, 2005) was highlighted in both the user studies. Participants appreciated the AUI's organised and minimalistic design (especially of the CAUI), which helped to reduce the decision fatigue when selecting adaptation choices and overall made the interaction easier to navigate. In addition, the *flexibility and efficiency* heuristic (Nielsen, 2005) was highlighted in both the studies as the AUI was predictive, fast, and automatically protective of privacy. This also helped the users to reduce their decision fatigue as the smart home took care of their privacy automatically in a seamless manner. This finding was also in line with Duarte's (2007) comment where he highlighted the AUI's being efficient. Both the heuristics *recognition rather than recall,* and *consistency and standards* (Nielsen, 2005) were highlighted when participants appreciated the scenarios that used or extended existing technologies/interactions. This helped the participants to quickly learn how the interface worked reducing the decision time while making the interaction

easier and efficient. In contrast to what Duarte (2007) stated about the AUI being disruptive, participants thought the AUIs were seamless and discreet. The AUIs accurately understanding the context and adapting at the correct time using the most suitable adaptations seems to have contributed to this appreciation.

In conclusion, to improve the ease of navigation and efficiency:

- use or extend existing user interface components throughout the interaction steps (§8.6: R4);
- design minimalistic user interfaces (§8.6: R4) and provide explanations whenever possible for the adaptation (§8.6: R6);
- automatically detect privacy violations and adapt the user interface to protect interpersonal privacy whenever appropriate (§8.6: R6); and
- make the adaptations seamless and less disruptive as much as possible (§8.6: R7).

7.2.5 Explanation of System Status

Keeping the users aware of the system's internal status and providing reasons for the system's behaviour helped to improve the trust between the user and the system – consequently improving the usability and the user experience. As previously mentioned (§7.2.4), creating a consistent mental model for the AUI's operational behaviour is harder. In this instance, the users try to adjust their mental model to suit the behaviour of the AUI, and the AUI tries to adjust itself to suit the user (cf. *hunting* problem (§2.2.1.2) (Duarte, 2007)). This may create confusion, which reduces the trust in the system, as it is harder to predict how the interface adapts (Duarte, 2007). To address this problem, two suggestions of Amershi et al.'s (2019) guidelines for better human-AI interaction can be used. When developing autonomous systems, they suggested providing users with the relevant information regarding context and the system status; and they also suggested explaining the reason for the system's adaptive behaviour. A similar approach was suggested by Nielsen (2005) for general product development: keep the users aware of the behaviour of the system within a reasonable amount of time (*visibility of system status*). Therefore, timely update of the smart home's context and the reasoning for the AUI's behaviour may address the *hunting* problem of the AUIs. The rest of this section discusses the impact of providing explanations of the user interface adaptations to the usability and the user experience of the AUI based on the findings of the two user studies.

Findings

Both of the studies found that keeping the user informed about system changes and explaining the reason for adaptations improved the user experience of the AUI. In the storyboard study, most of the participants who preferred CAUI over AAUI or CAUI over NAUI liked how CAUI explained the reason for the adaptation. These findings were later used when conceptualising the video prototype study, where an explanation for the adaptation was provided

whenever possible. Consequently, a third of participants (N=8/23) of the video prototype study appreciated the explanation provided by the AUIs. This was also highlighted in the answers provided for the post-study questionnaire, where they highly agreed that they understood why the user interface adaptation happened (mode of 5 where the maximum was 5) implying they had an accurate mental model of the AUI's behaviour.

The importance of explanations for the AUI is emphasised further by the dissatisfaction expressed by the participants when explanations were not provided. In the storyboard study, a couple of the participants (N=2/15) who disliked the AAUI mentioned it was due to the lack of explanations provided by the AUI, as they were not aware of the reasoning behind the adaptation. Similar comments were made during the video prototype study, where participants preferred to have explanations whenever possible. Apart from that, in some scenarios of the video prototype study, participants wished to have more clarity on how the AUI worked. This highlighted the importance of keeping the users aware of the system's behaviour.

The video prototype study participants mentioned in both the studies that they felt much more connected with the smart home as the AUI explained the reason for the adaptations. This feature seems to have reduced the emotional barrier between the smart home and the users. Some of the participants (N=6/23) reported that they felt as if the smart home is mimicking human interaction by explaining the reasoning behind the adaptation and keeping the user in the loop. This aspect of the AUI was well appreciated and seems to have improved the trust between the users and the smart home.

Discussion

Provision of explanations regarding the possible privacy violations and the adaptations resonated with the literature. As Amershi et al., (2019) suggested, letting the user know the system status and why the system behaved in a certain way improved the trust between the user and the system, consequently improving the user experience. On the other hand, in scenarios participants desiring more clarity may also have been a consequence of the limitations of the study, as video prototypes didn't allow participants to interact with the AUI in real-time to have an understanding of the functionality. This is not conclusive and requires further investigation.

In conclusion, when appropriate, provide explanations regarding the system status, consequences of adaptation choices, and reasoning for adaptations (§8.6: R6).

7.2.6 Fairness and Impact on Relationships

Algorithms that dictate the functionality of smart systems contain certain biases. These biases may produce actions that are unfair to certain users. The fairness of an algorithm as perceived by the

users affects their trust in the system, consequently affecting the user experience (Shin, 2020). This is relevant to the AUI, as adaptation may or may not be perceived as fair by the users. Further, how the algorithm adapts the user interface layer may have an impact on the relationship. This can be positive or negative, depending on how different people are benefited. Therefore, this section will discuss the findings related to fairness and the impact on interpersonal relationships within the smart home.

Findings

Apart from the less privacy critical scenarios, the AUIs provided an acceptable compromise. Some of the participants (N=4/23) in the video prototype study thought that the AUI made an acceptable compromise, apart from the scenarios where participants thought the type of privacy was not critical enough to be protected. For the question *If I were the person experiencing these user interface adaptations, I would not have accepted them,* participant answers had a mode of 1 (highly disagree) implying that they would have accepted the AUI most of the time. Later comments were reported by a few participants for the scenario in which a participant was trying to view photos on a Smart TV (Table 6.1: SLD scenario). They thought the AUI was being too careful or too protective of the other co-occupant. This was evident with the reaction card answers as well for the semi-automatic-AUI scenarios (Table 6.3). Participants selected negative reactions (22% of the reactions) such as *annoying, patronising and ineffective* for the semi-automatic AUI scenarios. Apart from that, most of the participants thought adaptations were in line with their privacy and user interface preferences.

The AUI improved interpersonal relationships. One fourth of the participants (N=6/23) mentioned that the AUI promoted mutual respect among co-occupants by not disturbing them or disclosing their personal information. They also highlighted how the AUI was collaborative between the co-occupants in protecting privacy within the smart home. These findings resonated in reaction cards as well, where most of the participants choose words such as *helpful, useful and collaborative* to describe their experience of the AUIs.

Discussion

As the literature suggested (Shin, 2020), the level of fairness felt by the users impacted how they experienced the AUI. The findings demonstrated that the AUIs' fair treatment towards all the co-occupants was highly appreciated, but there were some negative reactions towards the AUI when it adapted to protect less critical privacy types. This highlights how the users evaluate the impact of interpersonal privacy violations. If they decide the privacy violation is less critical and obstructs their interaction, users may object to the adaptation. Therefore, it is important to discuss among the co-occupants when setting privacy rules to maintain a good relationship with each other.

The AUI's awareness of privacy and user interface preferences of the co-occupants helped the smart home generate adaptations which helped to maintain a healthy relationship among the smart home users.

In summary, to generate fairer adaptations that support interpersonal relationships:

- co-occupants should discuss before when setting privacy settings which would impact multiple people (§8.6: R5); and
- as the system evolves, evaluate which type of adaptations are accepted by the co-occupants and which were declined. Those which are frequently accepted are indicative of successful adaptation suggestions and be ideal candidates for automatic adaptations. Those which are declined constantly will highlight adaptations that requires further discussion among the co-occupants (§8.6: R6).

7.3 Privacy Protection and Control

7.3.1 User Control and Flexibility

User control and flexibility are pertinent in developing effective and usable privacy-aware AUIs. To design more privacy-aware IT systems (in this case smart homes), Hoepman (2014) provided privacy design strategies, in which two suggestions were to *inform* the user and to provide *control* to the user. *Inform* refers to the notion of transparency, where the users are made aware when their information is being accessed or about to be accessed. *Control* refers to providing the users control over how their personal information is being used. Hoepman's discussion focuses on information privacy, but it can be easily extended to physical privacy management as well. Therefore, user control and flexibility are two core dimensions of the privacy-aware AUI's user experience, which will be discussed in the rest of this section.

Findings

Most of the time, having control and flexibility over privacy management provided high user satisfaction. A CAUI scenario that was based on a physical privacy violation was presented in both the user studies. The storyboard study participants (N=4/15) who preferred CAUI over AAUI, or CAUI over NAUI, mentioned that one of the reasons for that preference was CAUI's provision of choice. A couple of participants (N=2/15) mentioned that they would like to be asked before the adaptation happened, even though AAUI was much faster compared to the CAUI. Furthermore, participants highlighted how existing smart home devices lacked the control to adapt their behaviour when in execution. Therefore, participants appreciated the high-level of control provided by the CAUI. Similar to the storyboard study, the video prototype study participants also appreciated the CAUI's provision of choice and flexibility to the user. A participant reported that,

when they were able to control their immediate privacy (interpersonal-cyber-physical privacy), it gave them a sense of control. They had the impression that it is harder for them to control their privacy outside the smart home but were quite satisfied with the ability to control interpersonal-cyber-physical privacy. Therefore, providing control and flexibility over the user interface adaptations to protect interpersonal privacy (information privacy and physical privacy) and providing an explanation of the consequences of the adaptation choices, seemed to improve the user experience.

Some reported dissatisfaction toward automatic adaptations when used for mitigating physical privacy violations or when used for scenarios that the participants deemed to be less privacy-critical. In the storyboard study, a couple of participants (N=2/15) reported frustration when the smart home enforced co-occupants' physical privacy rules on to them by restricting them from certain interactions. A similar response was reported in the video prototype study, in which a very small number of participants (N=3/23) were annoyed that they had to change their behaviour to protect the co-occupant's physical privacy. Three participants (N=3/23) felt it was patronising that the smart home instructed them in scenarios where the privacy violation was not that critical. Some participants reported that interacting with semi-automatic adaptive-UI felt like not having control, as there were no choices, but they appreciated that the smart home asked the user before the adaptation. This theme was reconfirmed in the post-scenario questionnaire where participants had to rate the statement "*I did not feel that I am in control while using the smart home"*; physical privacy scenarios had a mode of 1 (highly disagree), and fully automatic AUI and information privacy scenarios had a mode of 2 (disagree), where semi-automatic AUI had a mode of 4 (agree). In addition, in reaction card analysis, semi-automatic AUI had 22% negative reactions (the highest negative percentage for any of the AUI types) with the reaction *rigid* being the most-used negative comment. Some of the participants seemed to have not considered certain physical privacy violation scenarios to be critical. Hence, when the smart home enforced adaptations obstructing the interaction, the participants felt they were not in control.

The participants didn't want to have immediate control or to have control at all for scenarios that are privacy-critical, or for which time is a critical factor for the efficacy of the adaptation. The storyboard study participants mentioned that they didn't want to have immediate control in scenarios where the adaptation was critical. Furthermore, as reported earlier (§5.5.2.2), the study found a difference between the usability scores for AAUI and NAUI on the aggregate of both scenarios, as well as for the information disclosure scenario. But there was no clear difference between AAUI and CAUI, implying that participants had divided opinions on the type of adaptive-UI to be used. This observation arose in the video prototype study findings as well, since participants who mentioned that they didn't have control with AAUI (both fully automatic and semi-automatic) made those comments for physical privacy examples or with scenarios with which they didn't resonate well. Participants also mentioned that they didn't want to have control over

adaptations which were time-critical, where the time taken for user input might make the adaptation ineffective. Therefore, automatically adapting the user interface to protect information privacy or critical privacy seems to improve the user experience. Hence, the type of privacy or the user's perception of the criticality of the privacy influences the type of adaptation.

Discussion

High user satisfaction for the CAUI-based scenario and dissatisfaction for the AAUI (fully-automatic and semi-automatic)-based scenarios with less critical privacy violations were in line with Hoepman's privacy by design strategies (2014). The reason for high user satisfaction could be the feelings of having authority over and trust in the smart home as a safe space for its occupants. The ability to control privacy within this space, having the ability to know when privacy is violated, and the consequences of different privacy control choices (user interface adaptations) seemed to improve the user experience.

In contrast to what Hoepman says on *informing* and providing user *control* regarding privacy, both the studies highlighted how participants sometimes preferred to have the smart home take care of their privacy automatically, especially regarding critical privacy variations that require reactive behaviour to mitigate (e.g., information privacy violations). Hoepman's strategies did not explain why certain types of privacy control might require different levels of user control. The findings suggest that this is a pragmatic choice, as having immediate control is less of a priority when the act of protecting privacy requires immediate action. In these instances, the smart home performs faster than a human by adapting the user interface, consequently effectively mitigating any interpersonal privacy violations.

In conclusion, the participants preferred CAUI with physical privacy violations and non-critical privacy violations where they preferred AAUI (fully-automatic and semi-automatic) with critical privacy violations and information privacy violations (§8.6: R8). The criticality of the privacy violations could depend on the time-sensitivity of the adaptation, or on the user's viewpoint about the gravity of the privacy violations. Due to the latter reasoning, it is important to discuss individual privacy preferences and UI adaptation mechanisms among the smart home users to avoid dissatisfaction at run-time (§8.6: R5), as adaptations may obstruct another co-occupant's activity/interaction. These conclusions motivate the need for:

- In-depth analysis on the level of control users might need with different types of interpersonal privacy violations to achieve optimal user satisfaction among the co-occupants or to evaluate if this can be achieved (§8.6: R8).
- Inquiry into how different interpersonal relationships affect different interpersonal privacy control mechanisms within the smart home (§8.6: R5).

7.3.2 Interpersonal Privacy Violations and Adaptive User Interfaces Applicability

The smart home user interface layer is multimodal, shared by multiple users, consists of multiple devices, hosts multiple applications, and is used in different contexts (Blumendorf, 2009). These qualities create interpersonal privacy violations (both information and physical privacy violations). Interpersonal privacy violations can be avoided or minimised by adapting the user interface layer (Schaub, 2014). The rest of this section discusses the types of interpersonal privacy violations discovered in the two user studies, and the applicability of the AUI in mitigating those violations.

Findings

Interpersonal *information* privacy violations are common with shared smart home devices, and the AUI can avoid or minimise these types of violations. The storyboard study participants reported how they experienced interpersonal *information* privacy violating scenarios with their shared smart home devices such as smart speakers and smart TVs. Some of these examples were possible disclosure of:

- financial information and credit card details via smart speakers,
- previous call records via shared conference calls on smart TVs,
- personal travel history via smart speakers,
- order histories via smart speakers,
- personal entertainment history via smart TVs, and
- personal notifications delivered on smart TVs and smart speakers.

The video prototype participants thought masking sensitive video information as well as auditory information was a possible solution for protecting privacy when having video conference calls within the smart home. One of the participants also reported how it could help students attend online classes from home with dignity and confidence from home as it would protect their *information* privacy. Therefore, the AUI is applicable in protecting the interpersonal *information* privacy violations that happen due to the shared nature of smart home devices.

Interpersonal privacy *physical* privacy violations are common with shared smart home devices and the AUI can avoid or minimise these types of violations. The storyboard study participants reported how their interpersonal *physical* privacy can be violated with shared temperature controls and smart speakers in their homes. Video prototype study participants highlighted how the AUI could help reduce the auditory disturbances that can be caused to the other co-occupants and their neighbours. Furthermore, one of these participants thought the AUI could help them to maintain concentration when working in shared spaces. A couple of them also thought the AUI could be used to enforce *physical* privacy rules in a shared space that would help to keep the disturbances among the co-occupants of the space to a minimum. Therefore, similar to

the interpersonal *information* privacy violations, the AUI can be used to protect users from interpersonal *physical* privacy violations that are caused due to shared smart home devices.

The AUI helped in avoiding uncomfortable situations that are caused due to shared smart home devices. A video prototype study participant thought the AUI could help protect kids from seeing inappropriate videos on Netflix. Furthermore, another participant thought the AUI could help them with social anxiety issues by protecting their private sphere within the smart home where they don't have to get on shared calls when they don't wish to. Therefore, the AUI can be used to mitigate certain types of uncomfortable situations and help to keep smart home users safe and happy.

The AUI is applicable during the COVID-19 lockdown-induced interpersonal privacy violations. Since people had to spend a lot of time together in the same household during the COVID-19 lockdown, the AUI was found to be useful in mitigating the increased number of interpersonal privacy violations. The storyboard study was conducted prior to the pandemic, whereas the video prototype study was conducted during the pandemic – and the participants (N=8/23) in the video prototype study highlighted the AUI's applicability during the COVID-19 pandemic. They thought the features of the AUI such as adaptive blurring (both audio and video) in video conference calls could help to keep the peace at home by protecting interpersonal privacy (information privacy as well as physical privacy).

Some scenarios did not resonate well with some of the participants. Some of the video prototype study participants (N=9/23) thought they might not use the AUI/smart home as demonstrated in a few of the scenarios:

- accessing the bank via the smart speaker (Table 6.1: BNK scenario),
- accessing sports news via the smart speaker (Table 6.1: FBL scenario), and
- opening the smart cupboard using a gesture (Table 6.1: OPN scenario).

In addition, a very few participants (N=4/23) mentioned that certain types of privacy (such as the interpersonal *physical* privacy violation caused by viewing images on the smart TV) might be less critical to consider as a privacy violation. These findings highlighted that some participants might not be happy with using the AUI in a certain way, or they might not like to use the smart home for certain types of activities. Therefore, the applicability of certain AUI types to different smart home scenarios might not always be suitable.

Discussion

Most of the interpersonal privacy violations that were reported by the participants were in line with the literature, but some novel examples were identified. Interpersonal *information* privacy violations that happen due to unauthorised access and unintended leakages of sensitive information via shared smart home devices were also discussed in the literature (Marky *et al.*, 2020). Similarly,

interpersonal *physical* privacy violations that happened due to shared smart home devices permeating personal boundaries resonated with the literature (Konings and Schaub, 2011). The discomfort caused by smart home users having to engage with their relatives via readily available smart home devices was discussed in the literature as well (Judge et al., 2011). In addition to what was discussed in the literature, novel examples were reported by the participants. Some of these examples were highlighted during the COVID-19 lockdown, such as video conferencing calls within smart homes violating interpersonal privacy. These were not previously studied in-depth in the literature and this research helped to shed light on different types of interpersonal privacy violations that may occur in different smart home contexts.

The applicability of the AUI in mitigating or minimising interpersonal privacy violations was partially discussed in the literature (Schaub, 2014), but the findings presented here expand the current understanding and demonstrate the extensibility of the AUI in different contexts (interpersonal privacy types, situations, and user interface types). The AUI's ability to detect interpersonal privacy violations and generate different types of adaptations (modality/device switching, feature adaptations) considering the various user preferences (privacy and user interface) made them an appealing solution to be used with interpersonal privacy mitigations. The AUI's extensibility was further demonstrated, as it was able to mitigate interpersonal privacy violations that arose during the COVID-19 lockdown. Even though the AUI was applicable in most of the interpersonal privacy violation scenarios, there were some scenarios for which the AUI was not the most preferred solution. This finding motivated further studies to evaluate if the PASHI framework provides a complete solution to all variations of interpersonal privacy violating scenarios.

In conclusion,

- the AUI can avoid or minimise interpersonal privacy violations and can be extended to different contexts in mitigating interpersonal privacy violations (e.g.: during the COVID-19 pandemic).
- In some interpersonal privacy violations, the choice of AUI, or the way it was delivered, was not applicable. Therefore, further studies can be conducted:
    - to understand and to create a taxonomy of different types of interpersonal privacy violations that may arise within a smart home (§8.6: R3); and
    - to evaluate the applicability of different types of AUI in different contexts (privacy preferences, user preferences, interpersonal privacy violation scenarios, and interpersonal relationships).; and to evaluate the completeness of the AUI's applicability in solving different interpersonal privacy violation scenarios (§8.6: R4).

7.3.3 Effectiveness and Dependability

With smart systems, trust is a critical factor. Trust depends on how effectively the system delivers what is promised and if it is communicated properly to the users of the system. Due to the AUI's adaptive nature, it could be less reliable at times, but the same adaptive nature makes the AUI stable and robust as it can recover from errors quickly and the services can be personalised to the user (Duarte, 2007). Amershi et al.'s (2019) work on better human-AI interaction helps to mitigate some of these problems. They suggested letting the users know what the system is capable of and why the system behaved in a certain manner will help to improve the user experience. This section discusses study findings related to the effectiveness and reliability of the AUI.

Findings

Overall, the AUI is highly effective in protecting interpersonal privacy. Participants of both studies highlighted the effectiveness of the AUI in protecting interpersonal privacy. All the storyboard study participants (N=15/15) reported that the AAUI and CAUI protected interpersonal privacy effectively. A couple of participants (N=2/15) commended the privacy protection feature of the AUI and its automated nature. Some participants (N=6/15) mentioned that they didn't like to use an NAUI (refers to standard smart home devices) as it did not protect privacy. They went on to explain how the AUI stopped possible feuds between smart home users. All the video prototype study participants (N=23/23) agreed that the AUI fully or partially protected interpersonal privacy. One of these participants mentioned that they expected a smart home to act in this manner where the smart home users' privacy will be automatically protected. In the post-scenario questionnaire, the participants highly agreed that the AUI protected the privacy of the smart home users where this answer had a mode of 5 (5 being the highest and implying highly agreed). They also selected reaction cards as *effective and relevant* to describe the experience of the AUI.

However, in some instances, the AUI was ineffective in protecting interpersonal privacy. A minority (information privacy: N=5/23, physical privacy: N=9/23) of the video prototype study participants thought the AUI was ineffective for specific scenarios. Of these participants, a very few participants (N=4/23) thought the scenario where the main user was opening a cupboard with a smart gesture (Table 6.1: OPN scenario) could have partially violated the privacy of the main user by leaking the initial gesture. They also thought the "Bing" sound might have given away to the other co-occupant of the privacy switch which could partially violate the privacy of the main user. Furthermore, they thought the "Bing" sound might disturb the co-occupant as well in scenarios related to physical privacy violations. This was also highlighted in the negative reactions (10% of the total reactions were negative) where they picked the reaction *ineffective* to describe the user experience of the AUI. These findings highlighted the aspects of the AUI that need to be improved for them to be much more effective. Therefore, the AUI is not 100% effective in protecting interpersonal privacy where there are scenarios which the current version of the AUI might not be effective or applicable.

The majority appreciated the AUI for its ability to solve interpersonal privacy. Most of the video prototype study participants (N=10/23) thought that the AUI was an innovative idea, and they were impressed with concepts such as privacy-awareness of the AUI, the ability to combine multiple user interfaces, context sensitivity, and features such as modality switching and feature adaptations. These findings were corroborated in the reaction card responses as well, where the participants picked reactions such as *innovative, cutting edge, powerful and essential.*

The AUI was trustworthy and reliable. In the video prototype study, the majority of the participants (N=10/23) mentioned that the AUI was reliable since AUI protected the privacy of the smart home users while staying consistent with the user preferences. For the same reasons, participants stated that they could trust the AUI. The majority of the participants picked reactions such as *trustworthy and reliable* corroborating these findings. Therefore, the trustworthiness and reliability of the AUI have improved the user experience.

Discussion

Participant comments regarding the AUI's effectiveness resonated with the literature while adding additional insights. Schaub (2014) partially touched upon the idea of using adaptive user interfaces for privacy protection. Extending this idea, the findings highlighted how the AUI can be used for protecting interpersonal privacy specifically. Furthermore, the AUI's ability to accurately capture user preferences and generate adaptations consistent with the preferences helped to generate more reliable, trustworthy, and effective adaptations. This countered what Duarte (2007) stated about AUI being less reliable but resonated with the AUI being stable and robust. Therefore, using accurate context information (specifically user preferences) to generate privacy-aware AUIs improves the user experience.

A small portion of participants highlighted aspects of the AUI that can be improved. For example, although the "Bing" sound provided much-needed awareness during the adaptation that generally helps to improve the usability of smart systems (Amershi *et al.*, 2019), it had unintended consequences – specifically disturbing other participants and leaking sensitive information – consequently violating the user's privacy. This motivates changing the existing notification mechanism to something discreet. The point regarding the 'initial gesture' in the smart gesture scenario (Table 6.1: OPN) violating privacy is something harder to solve using existing technology. It is harder to predict user actions in context without highly accurate models. Hence, addressing this participant comment is out of the scope of what the AUI can achieve currently.

In conclusion,

- The AUIs are effective in protecting interpersonal privacy. Therefore, in conjunction with accurate knowledge modelling features, the AUIs can be integrated into existing smart home devices.

- The notification mechanism should be improved to something more discreet. For example, something private to the user who receives the notification (private user interface). The efficacy and usability of these new notification mechanisms should be evaluated with empirical studies (§8.6: R7).

7.4 Improving Adaptive User Interfaces

In both the studies, participants commented on how the AUI can be improved, and this section discusses some of these suggestions.

Findings

The AUI's presentation of information and choices can be improved. The storyboard study participants thought that providing a rating with the possible risk of privacy violation for the choices in the CAUI and possible after-effects would be quite useful. Furthermore, they thought providing a default choice for the CAUI could be valuable to save time for the user. The video prototype study participants thought that unexplained adaptation could lead to a negative user experience and suggested including explanations whenever possible.

The AUI's privacy-preserving features and notifications can be improved. The video prototype study participants suggested that an audio masking feature could be quite useful while using video conferencing to remove background noise and other types of sensitive information. In addition to that, they suggested improving the notifications and warnings where they suggested removing the "Bing" sound as a notification. This was motivated by the view that a discreet notification mechanism would improve the user experience of the AUI as indiscreet notifications could partially violate the privacy of the main user (information privacy) as well as of the co-occupants (physical privacy).

The AUI may have certain adverse effects on interpersonal relationships. The video prototype participants mentioned how the AUI can impact relationships. Two participants thought AUI could be used to enforce privacy rules on other co-occupants, especially vulnerable smart home users such as children. Furthermore, two participants reported that it might be rude to ignore skype calls from people that they know and that could hinder their relationships if they can infer the person who walked behind the main user. Therefore, if not managed appropriately, the AUI poses a risk of negatively impacting interpersonal relationships among co-occupants due to the AUIs impact on multiple people living in the smart home.

Discussion

Participant comments on ways to improve the AUI's information and presentation were in line with the literature. For example, showing relevant contextual information and available smart home actions when selecting adaptations and providing explanations after the AUI makes a change, improves the usability and user experience of the smart home (Amershi *et al.*, 2019).

Participants' comments regarding the privacy-violating aspect of notifications and the novel privacy-preserving features were also in line with the literature. It is important not to disturb other co-occupants via smart home devices (Konings and Schaub, 2011). Therefore, replacing the "Bing" sound with a more discreet notification mechanism where possible is appropriate. In addition, smart home users may disturb other co-occupants during video conference calls (Maalsen and Dowling, 2020). The idea of masking audio (background noise) to improve physical privacy while engaging in conference calls addresses these kinds of problems.

Possible adverse effects of the AUI that were highlighted by the participants partially resonated with the literature. For example, there can be a power imbalance when sharing smart home devices (Niemantsverdriet, van Essen and Eggen, 2017). Since the AUI's actions affect multiple occupants, there is a risk of users who have more power within a household misusing the AUI to achieve their personal goals, e.g., participants suggesting using the AUI to control the behaviour of their children. Zeng and Roesener (2019) also highlighted how inadequate privacy preference authoring may lead to adversarial situations, such as domestic abuse. In addition, using the AUI as a means to *avoid* human interaction may cause conflicts between co-occupants if the need not to be disturbed is not communicated beforehand.

In conclusion,

- improve the presentation mechanism by integrating more contextual information, reasoning (explanations for adaptations) (§8.6: R6);
- sort the order of choices in a logical manner (e.g., from the greatest privacy risk to the least) as well as showing the possible outcomes of the choices to help the user make informed decisions and provide default choices whenever possible (§8.6: R4);
- improve the notification mechanism by changing the "Bing" sound to a more discreet notification, improving the overall privacy secureness of the AUI (§8.6: R7);
- introduce an audio-masking feature to microphones in the smart home, improving usability and privacy during conference calls by filtering out the background noise (§8.6: R7); and
- evaluate and support the management of possible adverse effects that arise due to power imbalances within the smart home. This requires further situated and long-term studies, analysing both interpersonal privacy dynamics within the smart homes and the impact of that on the AUI (§8.6: R5).

7.5 Methodology

In both studies, there were certain limitations that affected the validity of the findings. Some of these limitations were anticipated and discussed in Chapter 3 with steps to minimise their impact. These included shortcomings of the study stimulants and the limitations related to the applicability in real life and the generalisation of the AUI. The focus of this section is to report and to discuss further methodological issues that became apparent when the study was conducted, and data was analysed.

Findings

The video prototypes worked well for the majority of the participants. The majority of the participants reported that the scenarios resonated with their experience and were easy to relate to where all of them (N=23/23) resonated with at least one of the scenarios. Furthermore, some of the participants (N=8/23) highly praised the video quality. They highlighted how the attention details in the videos were spot on while making them realistic. This implied the video prototypes managed to generate accurate user responses. However, in the video prototype study, some of the participants (N=9/23) reported that they did not resonate well with some scenarios, especially

- the scenario with the gesture input (Table 6.1: OPN scenario),
- the scenario with the slide viewing on the smart TV (Table 6.1: SLD scenario),
- the scenario where the participants try to listen to football news on the smart speaker (Table 6.1: FBL scenario) and,
- the scenarios where the participant tries to access bank details via the smart speaker (Table 6.1: BNK scenario).

Participants who reported that they didn't resonate with these scenarios mentioned they might not have used the smart home in this manner. Therefore, apart from a few instances, the video prototypes generated accurate user responses.

The alternating nature of the questionnaire may have confused some participants. In the video prototype, the post-scenario questionnaire alternated between positive and negative questions to improve the participants' attention. A few participants (N=5/23) reported that they struggled to keep up with this alternating style. Therefore, this might have led to certain participants providing inaccurate data, as they read the questions inaccurately.

There were potential issues with the structure of the study. A couple of participants mentioned that they struggled to understand the definition of physical privacy, which might have led to answers which were focused on information privacy violations. In an isolated set of scenarios, a few of the participants' answers implied that they were unaware of certain aspects of the video or

misunderstood the scenario. These participants misunderstood the rule-setting aspect, user preferences, or certain context changes of the scenarios.

User biases impacted the findings. Different participants had varying attitudes/understanding of interpersonal privacy and smart homes. A couple of participants (N=2/23) did not care about their privacy where some participants took a pragmatic approach to protecting their privacy. In addition to that, participants who had a computer security background tend to ignore the physical privacy aspect in their answers. Apart from that, a very few participants (N=3/23) did not like smart homes in general. These type of user biases influenced the validity of the findings.

Effectiveness of the video prototype as a remote-research methodology. The pandemic forced this research to move away from a prototype-based lab-based study to a video prototype-based remote study. Video prototypes as a UX evaluation methodology had several pros and cons as follows:

Pros:

- Scenarios were consistent for all the study participants.
- Provided the ability to simulate certain aspects of the scenarios at video editing time.
- Ability to recruit a high number of participants.

Cons:

- Creation of videos took a significant amount of time as it included setting up the scenarios for the smart home, video recording, and editing.
- The participant feedback might not be fully aligned with a lab-based study. This could be due to a lack of interactive nature, or the inability of participants to immerse themselves in the scenarios by only watching videos. This could lead to some UX related information being missed.

Discussion

Notwithstanding the drawbacks mentioned above, prior research provides evidence that video prototypes can generate user responses that are in line with a lab-based study (Bajracharya *et al.*, 2013). Participants' responses indicating that the scenarios resonated with their experience and finding the videos to be closer to reality re-confirmed what the literature suggested. Therefore, the video prototypes proved to be a useful method that can be used as a remote-user evaluation mechanism especially during the COVID-19 lockdown where face-to-face user studies were harder to conduct. Furthermore, video prototypes provided the ability to quickly scale up the number of participants as the study can be conducted remotely.

Some participants reported not resonating with some of the scenarios, and user biases impacting the findings are inherent with these types of studies. When participants did not resonate with certain scenarios, it helped to understand user acceptance of those scenarios providing a high-level overview of the experience. However, their responses had a minimal contribution to the evaluation of the AUI variation that was under investigation. Therefore, their comments were mostly outweighed by a majority of participants giving a different view. Similarly, when participants did not understand a certain scenario, their comments were also outweighed by a majority of participants giving a different view as they were not valid responses regarding the user experience of the scenario under evaluation. In contrast, user biases were expected, and it is part of the experience of such studies. However, steps were put in place to get the participant's background knowledge regarding interpersonal privacy and the AUI to an adequate level and to uncover the impacts of the user biases on the findings. As one of these steps, the video prototype study participants were primed with two example scenarios of the AUI addressing interpersonal privacy violations (one from each variation of privacy violation). This helped the participants to have a sufficient understanding of the AUI's behaviour and its applicability. Furthermore, in both the studies, data analysis of the video prototype was carefully conducted with the help of a proven user experience evaluation method (McCarthy and Wright, 2004) to minimise the impact of user biases on the findings or to uncover the valid user biases (i.e. user biases that contribute to the findings) and their impact.

Limitations of the study structure (including the questionnaire) had minimal impact on the findings, but steps were taken to minimise their effect as well. The negative impact caused by the confusion with the alternating nature of the questionnaire was outweighed by the positive impact of generating accurate participant responses. The question design and structure motivated the participants to always think carefully before answering, consequently providing accurate answers. However, there was still a limited number of cases (N = 2/23) where the participants stated that they got confused by the questionnaire structure. To mitigate the impact of this and other misunderstandings of the scenarios (i.e., interpersonal privacy types, user preferences, and smart home context) the participants were asked to use the think-aloud protocol, prompting them to explain their reasoning. This step made the participants think more deeply about their answers and flagged if there were misunderstandings. Furthermore, the questionnaire answers were corroborated with the reaction card answers and the post-scenario interview answers to uncover any inconsistencies. This also helped to improve the validity of the findings. Therefore, the limitations of the study structure had minimal impact on the findings and when there were limitations, they were uncovered. Apart from this, video prototype studies proved to be quite useful as a remote UX evaluation method. Therefore, the approach taken in this research can be extended to other research studies where it is harder to conduct a lab-based user study.

7.6 Summary

This chapter discussed the usability, user experience, and privacy protection features of the AUI based on the storyboard study and the video prototype study reported previously. Overall, the conclusion of the discussion can be categorized under two main themes as follows:

AUI design features and usage:

- use CAUI for less critical privacy violations (e.g.: physical privacy) and AAUI for highly critical privacy violations (information privacy); and
- keep the AUI minimal, organised, familiar, and discreet while being courteous to the user (i.e., providing explanations and asking for consent whenever possible); and
- manage expectations of the AUI by priming the users of the smart home.

Future work:

- develop a taxonomy for different interpersonal privacy violations and use the taxonomy to evaluate the completeness of the PASHI framework's knowledge representation models, software architecture, and algorithms;
- provide users with preference authoring tools and introduce machine learning components to learn user preferences with time; and
- inquire into the impact of AUI on the interpersonal power imbalances within the smart home.

These conclusions are categorised and expanded in the following Chapter (§8).

8. Conclusion and Future Work

This research sought insight into how to achieve adaptations to the user interface layer in order to address interpersonal privacy in smart homes. This chapter will summarise the research that was conducted and the key findings (§8.1), provide recommendations (§8.6), and present the future work that can extend the insights derived from this research (§8.7).

8.1 Summary

The literature review (Chapter 2) identified a research gap in the smart home privacy literature regarding interpersonal privacy violations that are caused by the shared nature of the smart home devices. The thesis hypothesised that adapting the user interface layer could help to protect interpersonal privacy and looked to develop a framework that can generate privacy-aware smart home user interface adaptations. This was formalised as the main research question (**RQ0**): *How can smart home user interfaces be engineered to adapt their configuration and behaviour to preserve privacy between users in multi-occupancy contexts?* **RQ0** was operationalised into three sub-questions, which will be discussed in turn. Figure 8.1 *shows a summary of the* research questions, the *research methods, the key findings, and the relationships among them.*

8.2 Addressing RQ1: Characterising the Smart Home Environment

RQ1 *(How can we characterize the smart home environment adequately to drive privacy-aware user interface adaptations?)* highlighted a gap in the existing user interface frameworks – i.e., they did not model interpersonal privacy violations. Existing smart home user interface frameworks represented generic knowledge required for user interface adaptations, but those frameworks did not include the knowledge required for generating privacy-aware user interface adaptations. The literature review (§2) and the example scenarios presented in the first case study (§3.2**Error! Reference source not found.**) helped to identify the key characteristics needed to represent the context of interpersonal privacy violation scenarios: the user interface preferences, interpersonal privacy preferences, information related to the user interface layer, the smart home layout, and the environment-related information. Then knowledge representation models were developed based on the identified characteristics by either directly sourcing from the literature (e.g.: Rei for privacy preference authoring and MASP for smart home layout and environment information modelling) or modifying the models in the literature (e.g., VUMS cluster for user preference modelling, CTT and

Cameleon for user interface modelling) to suit the requirement. The first case study (§4) demonstrated that these knowledge representation models of the PASHI framework were adequate in representing the rich and nuanced context of interpersonal privacy violation scenarios in that they supported effective privacy-aware user interface adaptation generation.

8.3 Addressing RQ2: Software Architecture and Algorithms

RQ2 (W*hat is an appropriate software architecture for a privacy-aware adaptive smart home interface framework?)* concerned developing a software architecture and a set of algorithms that can generate privacy-aware smart home user interface adaptations. The software architecture used the information captured by the knowledge representation models (§4) to generate the adaptations. Specifically, the software architecture incorporated the MAPE-K architecture pattern to provide adaptive features and the MVC architecture to provide interactive features. Furthermore, two core algorithms were developed, where one detected interpersonal privacy violations using a Prolog-based rule engine, and the other generated usable user interface adaptations to mitigate the identified privacy violations. The second case study (§5) demonstrated that the PASHI framework's software architecture and the algorithms were adequate to generate privacy-aware user interface adaptations. The case study also showed that the two algorithms were sufficiently efficient and effective in a smart home setting. This was further evaluated by a storyboard-based usability study (§5.5) that depicted user interface adaptations generated from the PASHI framework. The study reconfirmed the findings of the second case study by demonstrating the adequacy of the PASHI framework's software architecture and the algorithms.

8.4 Addressing RQ3: Evaluating the experience

RQ3 (*what is the user experience of privacy-aware adaptive user interfaces?)* focused on the usability and the overall user experience of the privacy-aware adaptive user interfaces. First, a storyboard-based user study (§5.5) was conducted to evaluate the usability of different types of AUI when applied to protect different types of interpersonal privacy violations. Incorporating the findings from the usability study and expanding the coverage of examples scenario variations (i.e., more AUI variations, interpersonal privacy variations, smart home context variations, and user preference variations) a video prototype-based user experience evaluation study was conducted (§6).

Figure 8.1: Summary of the Thesis

The video prototype study was chosen to provide the participants with more realistic examples of the AUI and was a pragmatic choice given the COVID-19 pandemic that interrupted face-to-face user studies. Findings from both the studies were evaluated together and demonstrated that:

- when the appropriate AUI variation was applied to mitigate interpersonal privacy violations, it provided higher usability and user experience (e.g.: by providing run-time control of the adaptation or automating the adaptation depending on the user preference),
- the PASHI framework's effective knowledge modelling capabilities helped to capture different user preferences contributing to effective and usable adaptations,
- providing explanations for adaptations, discreet notifications to inform adaptations, together with a minimal and organised presentation of adaptation choices, provided a positive user experience.

A more detailed list of recommendations (§8.6) and future work (§8.7) will be presented in the proceeding sections.

8.5 Addressing RQ0

Overall, the research addressing the three sub-questions provides a demonstration-of-concept in response to the over-riding RQ0: *How can smart home user interfaces be engineered to adapt their configuration and behaviour to preserve privacy between users in multi-occupancy contexts?* The user interface model, privacy preference model and the user interface preference model were able to successfully model the rich and nuanced context of interpersonal privacy violations. Therefore, these models can provide the knowledge representation capability to other frameworks that need to understand the context of interpersonal privacy violating scenarios. Similarly, the software architecture can be integrated into existing smart environment user interface frameworks to enable privacy-aware adaptive user interface generation. The research both shows the feasibility of AUI and highlights key questions and challenges for future work.

8.6 Recommendations for Managing Interpersonal Privacy in Smart Homes

Based on the findings of the two case studies (Chapter 4, 5) and the two user studies (Chapter 5, 6), this section provides design recommendations for developing privacy-aware adaptive user interfaces.

R1 - Improve and evaluate Knowledge Representation Models: The user interface preference model should be extended to support other types of interaction preferences that the participants might have (e.g., human-to-human interaction) and to provide more flexibility when defining preferences. The privacy preference model should be evaluated for its efficacy in supporting privacy preference conflicts. Further, it is recommended to integrate the means to reject certain adaptations when users see fit. In addition, adaptations should be mindful of not violating other types of interpersonal privacy violations which are not the focus of protection. For example, protecting physical privacy should not violate information privacy and vice versa. Lastly, both models should be evaluated for completeness and should be remodelled to support the evolution of user preferences over time.

R2 - Provide Descriptive and Flexible Preference Authoring Tools: At the moment, the preferences are set by a researcher/engineer of the PASHI framework. As the framework evolves, the framework should allow the users to define their preferences and to change them as they see fit. The tool should provide descriptive and flexible means to define interpersonal privacy preferences and user interface preferences. With regard to interpersonal privacy preferences, the tool should represent both types of interpersonal privacy violations (information and physical), the contextual information used to define privacy preferences, and the privacy violating features of the user interfaces. With regard to user interface preferences, the tool should support both device/modality-based preferences (i.e., preferences between device/modality) and feature-based preferences (i.e., preferences within the same modality).

R3 - Manage Expectations Regarding the AUI: Managing users' expectations regarding the AUI helps to improve user experience. Therefore, it is recommended to let the users know what the AUI is capable of and how effectively it can execute those capabilities. This can be presented at run-time or prior to the interaction as an orientation (especially for first-time users). First-time users will benefit from an orientation regarding the AUI's behaviour, as it will help them to manage their expectations of the AUI, consequently improving the usability and user experience. This orientation should be representative of the different privacy violations that the AUI can address and the different operational behaviours of the AUI (i.e., adaptation variations and adaptation timing). Furthermore, all the smart home users should be informed about the AUI's affordances, prompting users to negotiate some of the conflicting privacy preferences beforehand.

R4 - Develop the AUI to be Minimal, Organised, and Familiar: Making any user interface easier to learn and operate improves the user experience. This is quite relevant to AUI, which can be generally harder to learn due to its inconsistent nature. Therefore, when presenting information or adaptation choices, it is recommended to keep it minimal and organised. Adaptation options should be ordered logically, and a default option should be provided. In addition, extending existing user interface components or modifying them minimally will help the users recall their

previous interaction with those interfaces. These features will help reduce users' cognitive load and help them learn the AUI more easily, consequently improving the user experience.

R5 - Incorporate and Evaluate 'Human-Like' Courteous Characteristics in the AUI: Studies found the participants appreciated the 'human-like' courteous characteristics of the AUI. This includes making the AUI ask for permission from the user before an adaptation and explaining privacy violation detection and the consequences of choices. Making the AUI more courteous tends to improve the user experience, but further studies need to be conducted to evaluate which of these characteristics are appreciated, the inter-play between different characteristics and their applicability in different contexts.

R6 - Provide Appropriate and Adequate Explanations for Adaptations: It is important to help smart home users maintain a consistent and accurate mental model of the privacy-aware AUI to improve their trust in the smart home. This motivates the provision of reasoning for the adaptation and the other required context information along with the adaptation. These explanations should be timely and should be adaptive on their own to provide only the necessary information required for an explanation of the reasoning. This is critical, as smart homes are occupied by multiple people who may have different relationships to each other, and different individual preferences. Hence, the explanations should take these factors into account and should not hinder any interpersonal relationships to help improve the trust in the privacy-aware AUI.

R7 - Improve Features of the AUI which may Cause Privacy Violations and Integrate New Features that will Enhance the Privacy Protection: The notification system used by the AUIs need to be designed with care, integrating more privacy-protective mechanisms such as vibrations and/or personal visual notifications should be used. Furthermore, make the adaptations seamless (i.e., less disruptive) as much as possible. In addition, features such as audio-masking should be integrated to conference calls to improve interpersonal privacy. Further empirical studies should be conducted to understand the efficacy and the user experience of these novel features.

R8 - Use CAUI for less Critical Privacy Protection and AAUI for Critical Privacy Protection: Less critical privacy violations (mainly physical privacy but may include other types of privacy depending on the user's viewpoint) needs to be handled by giving the users more choices, i.e., using choice-based adaptive user interfaces (CAUI). Critical privacy violations (mainly information privacy but may include other types of privacy depending on the user's viewpoint) need to be handled automatically by the smart home, hence the AAUI. Whenever possible, the AAUI should provide explanations for adaptions and take a 'pause and continue' approach, where the user's consent is needed to continue the suggested adaptation (presented with semi-automatic AUI). In addition, further inquiry is needed into the interplay between the appropriate level of privacy control based on the type of privacy violations, and the type of interpersonal relationships.

8.7 Future Work

The research also highlighted areas for further investigation. Some of these extend the recommendations, where others are drawing on more general issues identified during the discussion of the findings. These include ethical considerations and solutions for addressing issues when integration with existing smart homes.

Conduct Further Studies to Evaluate the Completeness of the PASHI framework's Software Architecture and Algorithms: This research only evaluated the adequacy of the PASHI framework to detect and generate user interface adaptations. This evaluation should be extended by conducting studies to evaluate the completeness of the software architecture and the algorithms in detecting in generating privacy-aware adaptive smart home user interfaces.

Implement and Evaluate the Components and Models which were not Presented in this Thesis: The service model, user capability model and the sensor control component were not presented nor evaluated in this work. Therefore, to use the PASHI framework in a real-life setting, these components should be implemented and evaluated as future studies.

Develop a Taxonomy of Interpersonal Privacy Violations: The entire research focused on two variations of interpersonal privacy (information and physical), but these variations can be further sub-divided and there could be novel interpersonal privacy violation types. Therefore, to understand AUI's applicability and to improve the AUI, it is important to develop a comprehensive taxonomy of the interpersonal privacy violations within the smart home.

Evaluate the Completeness of the AUI's Applicability in Different Contexts: Findings demonstrated that some AUI applications to different interpersonal privacy violations were not appreciated by some participants. Therefore, to better understand the applicability of the AUI in different contexts, further studies are required. These studies should evaluate the completeness of the different AUI variation's applicability in different contexts (e.g., user preferences, interpersonal privacy violation types, and co-occupant relationships). The PASHI framework was developed to support extensibility to other smart environments. Therefore, further studies can be conducted to evaluate the applicability of the framework in other smart environments such as smart offices, smart hospitals, and smart vehicles (e.g., smart offices and smart cars).

Explore How the AUI can Augment Interpersonal Power Imbalances and Mitigate Possible Adverse Outcomes: Since the AUI can affect multiple co-occupants within the smart home and is operated automatically based on rules set by a smart home user, AUIs may amplify interpersonal power dynamics. Some of these can be adversarial to certain co-occupants, especially the

vulnerable within the smart home. Therefore, situated, and long-term user studies should be conducted to understand how different interpersonal relationships affect the use of the AUI. If there are possible negative outcomes to certain co-occupants, mitigation mechanisms should be integrated into the AUI, empowering the vulnerable to avoid being harassed by powerful users within the smart homes. These mechanisms can check for possible adverse effects that a rule might have on different co-occupants at the time of authoring and block them.

Incorporate Machine Learning Component of the PASHI framework to Learn User Preferences and Capabilities with Time: Use machine learning to learn the preferences of the users while they interact with the smart home. The machine learning model can be updated based on what type of AUI recommendations are accepted or rejected. However, this should be done carefully respecting user privacy where privacy-enhancing strategies and technologies can be used. Furthermore, machine learning can be done locally reducing the risk of data being leaked to external parties.

Investigate the Ethical Implications of AUIs: As discussed earlier, AUI may amplify power imbalances within a smart home and the machine learning aspect might violate certain privacy preferences of the users. Therefore, further studies should be conducted to understand the ethical implications of the AUI and to find mechanisms to minimise those possible implications.

SDK Development for Multiple Devices: Integration of the PASHI framework with standard smart home user interfaces requires both server-side support and client-side support. The existing framework provides architecture, models, and algorithms for the server-side implementations, but SDKs (software development kits) should be developed to extend support for the client-side. This SDK should provide means to receive and process information received from the PASHI-server and to send user input back to the PASHI-server. Providing SDK support for multiple devices will improve the ease of integration of the PASHI framework.

Smart environment Physical Layout Modelling to Support in-the-wild Deployment of the PASHI framework: To generate effective adaptations, the PASHI framework should understand the physical constraints of the environments. At the moment, the PASHI framework provides a basic model for this requirement. This motivates an in-depth inquiry into understanding the pervasiveness of the different modalities (or smart devices) within the physical constraints of a smart home, and to develop mathematical models to accurately predict the reach. This would provide richer context to the PASHI framework supporting effective privacy-aware user interface adaptation generation.

8.8 Conclusion

This research addressed a research gap in the smart home privacy literature and the smart home user interface framework literature by developing the PASHI framework, which can generate privacy-aware smart home user interface adaptations that protect the interpersonal privacy of the smart home users. The dissertation presented and evaluated the required knowledge representation models, software architecture and algorithms that together supported the generation of effective and usable privacy-aware user interface adaptations. Furthermore, it evaluated the user experience of AUI demonstrating that the AUI provided a positive user experience when used in appropriate scenarios to mitigate interpersonal privacy violations. The studies found key design features to develop effective privacy-aware AUIs and highlighted possible future work.

While the PASHI framework provides the means to develop a more privacy-aware and usable smart home, it also lays the groundwork for research to develop more privacy-secure multi-user cyber-physical environments. This research has potential beyond the constraints of a smart home to smart offices and smart cars in the future. Therefore, I hope this thesis may provide the tools and the inspiration needed for a more privacy-secure future.

9. References

Aamodt, A. and Plaza, E. (1994) 'Case-based Reasoning: Foundational Issues, Methodological Variations, and System Approaches', *AI communications*, 7(1), pp. 39–59. doi: 10.3233/AIC-1994-7104.

Abdi, N. *et al.* (2021) 'Privacy Norms for Smart Home Personal Assistants', in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pp. 1–14. doi: 10.1145/3411764.3445122.

Abdi, N., Ramokapane, K. M. and Such, J. M. (2019) 'More than smart speakers: security and privacy perceptions of smart home personal assistants', in *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*. Available at: https://bit.ly/3xUktuH.

Agrawal, R. *et al.* (2005) 'XPref: A Preference Language for P3P', *Computer Networks*, 48(5), pp. 809–827. doi: 10.1016/j.comnet.2005.01.004.

Ahmad, I. *et al.* (2020) 'Tangible Privacy: Towards User-Centric Sensor Designs for Bystander Privacy', *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2), pp. 1–28. doi: 10.1145/3415187.

Akiki, P. (2014) *Engineering Adaptive Model-Driven User Interfaces for Enterprise Applications*. PhD Thesis. The Open University. Available at: http://oro.open.ac.uk/40828/.

Akiki, P. A., Bandara, A. K. and Yu, Y. (2015) 'Adaptive Model-Driven User Interface Development Systems', *ACM Computing Surveys*, 47(1). doi: 10.1145/2597999.

Alharbi, R. and Aspinall, D. (2018) 'An IoT Analysis Framework: An Investigation of IoT Smart Cameras' Vulnerabilities', in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, pp. 1–10. doi: 10.1049/cp.2018.0047.

Almeida, N. *et al.* (2019) 'The AM4I Architecture and Framework for Multimodal Interaction and Its Application to Smart Environments', *Sensors*, 19(11), p. 2587. doi: 10.3390/s19112587.

Altman, I. (1976) 'A Conceptual Analysis', *Environment and behavior*, 8(1), pp. 7–29. doi: 10.1177/001391657600800102.

Amazon Press Room (2020) *Introducing the All-New Echo Family—Reimagined, Inside and Out | Amazon.com, Inc. - Press Room*. Available at: https://bit.ly/3q99KJZ (Accessed: 8 February 2021).

Amershi, S. *et al.* (2019) 'Guidelines for Human-AI Interaction', in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Glasgow, Scotland, UK: ACM, pp. 1–13. doi: 10.1145/3290605.3300233.

Ashley, P. *et al.* (2002) 'E-P3P Privacy Policies and Privacy Authorization', in *Proceedings of the 2002 ACM Workshop on Privacy in the Electronic Society*. New York, NY, USA: ACM (WPES '02), pp. 103–109. doi: 10.1145/644527.644538.

Ashley, P. *et al.* (2003) 'Enterprise privacy authorization language (EPAL)', *IBM Research*, 30, p. 31.

Bajracharya, P. *et al.* (2013) 'How Does User Feedback to Video Prototypes Compare to that Obtained in a Home Simulation Laboratory?', in Streitz, N. and Stephanidis, C. (eds) *Distributed, Ambient, and Pervasive Interactions*. Berlin, Heidelberg: Springer (Lecture Notes in Computer Science), pp. 195–204. doi: 10.1007/978-3-642-39351-8_22.

Balta-Ozkan, N. *et al.* (2013) 'Social Barriers to the Adoption of Smart Homes', *Energy Policy*, 63, pp. 363–374. doi: 10.1016/j.enpol.2013.08.043.

Becker, M. Y., Malkis, A. and Bussard, L. (2009) 'A Framework for Privacy Preferences and Data-Handling Policies', *Microsoft Research Cambridge Technical Report, MSR-TR-2009-128*. Available at: https://bit.ly/3vAhwh7.

Bekara, K., Mustapha, Y. B. and Laurent, M. (2010) 'Xpacml Extensible Privacy Access Control Markup Language', in *The Second International Conference on Communications and Networking*. IEEE, pp. 1–5. doi: 10.1109/comnet.2010.5699807.

Benedek, J. and Miner, T. (2002) 'Measuring Desirability: New Methods for Evaluating Desirability in a Usability Lab Setting', *Proceedings of Usability Professionals Association*, 2003(8–12), p. 57.

Bernd, J., Abu-Salma, R. and Frik, A. (2020) 'Bystanders' Privacy: The Perspectives of Nannies on Smart Home Surveillance', in *10th {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 20)*. Available at: https://bit.ly/3wBf7E9.

Blumendorf, M. (2009) *Multimodal Interaction in Smart Environments: a Model-Based Runtime System for Ubiquitous User Interfaces.* PhD Thesis. Berlin Institute of Technology. Available at: https://bit.ly/2SFlOX5.

Booch, G. (2005) *The Unified Modeling Language User Guide*. India: Pearson Education.

Brooke, J. (1996) 'SUS: A "Quick and Dirty' Usability Scale', *Usability evaluation in industry*, (1st Edition), p. 189. doi: 10.1201/9781498710411-35.

Brudy, F. *et al.* (2014) 'Is Anyone Looking? Mitigating Shoulder Surfing on Public Displays Through Awareness and Protection', in *Proceedings of The International Symposium on Pervasive Displays*. ACM, pp. 1–6. doi: 10.1145/2611009.2611028.

Brusilovsky, P. (1996) 'Methods and Techniques of Adaptive Hypermedia', *User Modeling and User-Adapted Interaction*, 6(2), pp. 87–129. doi: 10.1007/BF00143964.

Burgoon, J. K. (1982) 'Privacy and Communication', *Annals of the International Communication Association*, 6(1), pp. 206–249. doi: 10.1080/23808985.1982.11678499.

Calikli, G. *et al.* (2016) 'Privacy Dynamics: Learning Privacy Norms for Social Software', in *Proceedings of the 11th International Symposium on Software Engineering for Adaptive and Self-Managing Systems*. ACM, pp. 47–56. doi: 10.1145/2897053.2897063.

Calvary, G., Coutaz, J. and Thevenin, D. (2001) 'A Unifying Reference Framework for the Development of Plastic User Interfaces', in Little, M. R. and Nigay, L. (eds) *Engineering for Human-Computer Interaction*. Berlin, Heidelberg: Springer (Lecture Notes in Computer Science), pp. 173–192. doi: 10.1007/3-540-45348-2_17.

Cárdenas, A. A. and Safavi-Naini, R. (2012) 'Security and Privacy in the Smart Grid', in *Handbook on Securing Cyber-Physical Critical Infrastructure*. Elsevier, pp. 637–654. doi: 10.1016/B978-0-12-415815-3.00025-X.

Casas, R. *et al.* (2008) 'User Modelling in Ambient Intelligence for Elderly and Disabled People', in Miesenberger, K. et al. (eds) *Computers Helping People with Special Needs*. Berlin, Heidelberg: Springer (Lecture Notes in Computer Science), pp. 114–122. doi: 10.1007/978-3-540-70540-6_15.

Choi, Y. M. and Li, J. (2016) 'Usability Evaluation of a New Text Input Method for Smart TVs', *Journal of Usability Studies*, 11(3), pp. 110–123.

Clerckx, T., Luyten, K. and Coninx, K. (2004) ‘DynaMo-AID: A Design Process and a Runtime Architecture for Dynamic Model-Based User Interface Development’, in *IFIP International Conference on Engineering for Human-Computer Interaction*. Springer, pp. 77–95. doi: 10.1007/11431879_5.

Commission, U. S. F. T. (1998) *Privacy Online: A Report to Congress*. The Commission.

Cronel, M. *et al.* (2018) ‘MIODMIT: A Generic Architecture for Dynamic Multimodal Interactive Systems’, in *International Conference on Human-Centred Software Engineering*. Springer, pp. 109–129. doi: 10.1007/978-3-030-05909-5_7.

Damianou, N. *et al.* (2001) ‘The Ponder Policy Specification Language’, in Sloman, M., Lupu, E. C., and Lobo, J. (eds) *Policies for Distributed Systems and Networks*. Berlin, Heidelberg: Springer (Lecture Notes in Computer Science), pp. 18–38. doi: 10.1007/3-540-44569-2_2.

Dasgupta, A., Gill, A. Q. and Hussain, F. (2019) ‘Privacy of IoT-Enabled Smart Home Systems’, *Internet of Things (IoT) for Automated and Smart Applications*. doi: 10.5772/intechopen.84338.

Davidoff, S. *et al.* (2006) ‘Socially-Aware Requirements for a Smart Home’, in *Proceedings of the international symposium on intelligent environments*, pp. 41–44. Available at: https://bit.ly/35APJSZ.

DeCew, J. (2002) ‘Privacy’. Available at: https://stanford.io/3gCnmsZ (Accessed: 13 April 2020).

Dillaway, B. (2006) ‘A Unified Approach to Trust, Delegation, And Authorization in Large-scale Grids’, *Whitepaper, Microsoft Corporation.* Available at: https://bit.ly/35yjYde.

Duarte, C. A. P. dos A. (2007) *Design and Evaluation of Adaptive Multimodal Systems*. PhD Thesis. Universidade de Lisboa. Available at: https://bit.ly/35uPgC0.

Edward T., H. (1966) *The Hidden Dimension*. Garden City, NY: Doubleday. Available at: https://bit.ly/35AQrQ9.

Fereday, J. and Muir-Cochrane, E. (2016) ‘Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development’:, *International Journal of Qualitative Methods*. doi: 10.1177/160940690600500107.

Ferraiolo, D., Kuhn, D. R. and Chandramouli, R. (2003) *Role-Based Access Control*. Artech House Publishers.

França, A. C. C., de Araújo, A. C. M. L. and da Silva, F. Q. B. (2013) 'Motivation of Software Engineers: A Qualitative Case Study of a Research and Development Organisation', in *2013 6th International Workshop on Cooperative and Human Aspects of Software Engineering (CHASE)*, pp. 9–16. doi: 10.1109/CHASE.2013.6614726.

Geeng, C. and Roesner, F. (2019) 'Who's in Control? Interactions in Multi-User Smart Homes', in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery (CHI '19), pp. 1–13. doi: 10.1145/3290605.3300498.

Goldberg, D. *et al.* (1992) 'Using Collaborative Filtering to Weave an Information Tapestry', *Communications of the ACM*, 35(12), pp. 61–71. doi: 10.1145/138859.138867.

Hall, E. T. (1973) *The Silent Language (Reissue edition)*. New York: Anchor.

Hoepman, J.-H. (2014) 'Privacy Design Strategies', in Cuppens-Boulahia, N. et al. (eds) *ICT Systems Security and Privacy Protection*. Berlin, Heidelberg: Springer (IFIP Advances in Information and Communication Technology), pp. 446–459. doi: 10.1007/978-3-642-55415-5_38.

Huang, Y., Obada-Obieh, B. and Beznosov, K. (Kosta) (2020) 'Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks', in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Honolulu, HI, USA: Association for Computing Machinery (CHI '20), pp. 1–13. doi: 10.1145/3313831.3376529.

IBM (2006) *An Architectural Blueprint for Autonomic Computing*. Available at: https://ibm.co/3zAVX35 (Accessed: 14 December 2020).

Iyilade, J. and Vassileva, J. (2014) 'P2U: A Privacy Policy Specification Language for Secondary Data Sharing and Usage', in *2014 IEEE Security and Privacy Workshops*. *2014 IEEE Security and Privacy Workshops*, pp. 18–22. doi: 10.1109/SPW.2014.12.

Jackson, C. and Orebaugh, A. (2018) 'A Study of Security And Privacy Issues Associated with The Amazon Echo', *International Journal of Internet of Things and Cyber-Assurance*, 1(1), pp. 91–100. doi: 10.1504/IJITCA.2018.090172.

Judge, T. K. *et al.* (2011) 'Family portals: connecting families through a multifamily media space', in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery (CHI '11), pp. 1205–1214. doi: 10.1145/1978942.1979122.

Kagal, L. (2002) ‘Rei: A Policy Language for the Me-centric Project’. Available at: https://bit.ly/3zxqvCX.

Kagal, L., Hanson, C. and Weitzner, D. (2008) ‘Using Dependency Tracking to Provide Explanations for Policy Management’, in *2008 IEEE Workshop on Policies for Distributed Systems and Networks*. IEEE, pp. 54–61.

Kaklanis, N. *et al.* (2016) ‘Towards Standardisation of User Models for Simulation and Adaptation Purposes’, *Universal Access in the Information Society*, 15(1), pp. 21–48. doi: 10.1007/s10209-014-0371-2.

Karami, A.-B. *et al.* (2016) ‘User in the Loop: Adaptive Smart Homes Exploiting User Feedback-State of the Art and Future Directions’, *Information*, 7(2), p. 35. doi: 10.3390/info7020035.

Karr-Wisniewski, P., Wilson, D. and Richter-Lipford, H. (2011) ‘A New Social Order: Mechanisms for Social Network Site Boundary Regulation’, p. 9.

Kephart, J. O. and Chess, D. M. (2003) ‘The Vision of Autonomic Computing’, *Computer*, 36(1), pp. 41–50. doi: 10.1109/mc.2003.1160055.

Konings, B. and Schaub, F. (2011) ‘Territorial Privacy in Ubiquitous Computing’, in *2011 Eighth International Conference on Wireless On-Demand Network Systems and Services*. *2011 Eighth International Conference on Wireless On-demand Network Systems and Services (WONS 2011)*, Bardonecchia: IEEE, pp. 104–108. doi: 10.1109/WONS.2011.5720177.

Konrad, M., Koch-Sonneborn, S. and Lentzsch, C. (2020) ‘The Right to Privacy in Socio-Technical Smart Home Settings: Privacy Risks in Multi-Stakeholder Environments’, in Stephanidis, C. and Antona, M. (eds) *HCI International 2020 - Posters*. Cham: Springer International Publishing (Communications in Computer and Information Science), pp. 549–557. doi: 10.1007/978-3-030-50732-9_71.

Kraemer, M. J. (2018) ‘Preserving Privacy in Smart Homes: A Socio-Cultural Approach’, in *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems - CHI ‘18*. *Extended Abstracts of the 2018 CHI Conference*, Montreal QC, Canada: ACM Press, pp. 1–4. doi: 10.1145/3170427.3173018.

Kramer, J. and Magee, J. (2007) ‘Self-managed Systems: An Architectural Challenge’, in *Future of Software Engineering (FOSE’07)*. IEEE, pp. 259–268. doi: 10.1109/fose.2007.19.

Kray, C., Kortuem, G. and Wasinger, R. (2004) ‘Concepts and Issues in Interfaces for Multiple Users and Multiple Devices’, in *Workshop on Multi-User and Ubiquitous User Interfaces (MU3I) at IUI 2004*. *Workshop on Multi-User and Ubiquitous User Interfaces (MU3I) at IUI 2004*, Funchal, Madeira, Portugal. Available at: https://bit.ly/3gIlKxA.

Kubitza, T. and Schmidt, A. (2017) ‘meSchup: A platform for programming interconnected smart things’, Computer, 50(11), pp. 38–49. doi: 10.1109/mc.2017.4041350

Kuflik, T., Kay, J. and Kummerfeld, B. (2012) ‘Challenges and Solutions of Ubiquitous User Modeling’, in Krüger, A. and Kuflik, T. (eds) *Ubiquitous Display Environments*. Berlin, Heidelberg: Springer (Cognitive Technologies), pp. 7–30. doi: 10.1007/978-3-642-27663-7_2.

Lau, J., Zimmerman, B. and Schaub, F. (2018) ‘Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers’, *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW), p. 102:1-102:31. doi: 10.1145/3274371.

Lee, C. E. (2010) ‘Face-to-face Versus Computer-mediated Communication: Exploring Employees’ Preference of Effective Employee Communication Channel’, *International journal for the advancement of science & arts*, 1(2), pp. 38–48. doi: 10.1007/978-3-030-67425-0_3.

Lewis, C. (1982) *Using the ‘Thinking-aloud’ Method in Cognitive Interface Design*. IBM TJ Watson Research Center Yorktown Heights, NY. Available at: https://ibm.co/3zrEv17.

Loitsch, C. *et al.* (2017) ‘A Knowledge-based Approach to User Interface Adaptation from Preferences and for Special Needs’, *User Modeling and User-Adapted Interaction*, 27(3), pp. 445–491. doi: 10.1007/s11257-017-9196-z.

Luria, M. *et al.* (2020) ‘Social Boundaries for Personal Agents in the Interpersonal Space of the Home’, in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. Honolulu, HI, USA: Association for Computing Machinery (CHI ‘20), pp. 1–12. doi: 10.1145/3313831.3376311.

Maalsen, S. and Dowling, R. (2020) ‘Covid-19 and the Accelerating Smart Home’, *Big Data & Society*, 7(2). doi: 10.1177/2053951720938073.

Mackay, W. E. (1988) ‘Video Prototyping: A Technique for Developing Hypermedia Systems’, in *CHI’88 Conference Companion Human Factors in Computing Systems*. Citeseer, pp. 1–3. Available at: https://bit.ly/3xwZBJJ.

Mancini, C. *et al.* (2009) ‘From Spaces to Places: Emerging Contexts in Mobile Privacy’, in *Proceedings of the 11th international conference on Ubiquitous computing*. Orlando, Florida, USA: Association for Computing Machinery (UbiComp ‘09), pp. 1–10. doi: 10.1145/1620545.1620547.

Marky, K. *et al.* (2020) ‘“I Don’t Know How to Protect Myself”: Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments’, in *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*. New York, NY, USA: Association for Computing Machinery (NordiCHI ‘20), pp. 1–11. doi: 10.1145/3419249.3420164.

Marx, G. T. (2001) ‘Murky Conceptual Waters: The Public and the Private’, *Ethics and Information Technology*, 3(3), pp. 157–169. doi: 10.1023/A:1012456832336.

Mayer, C. *et al.* (2013) ‘User Interfaces for Older Adults’, in *International Conference on Universal Access in Human-Computer Interaction*. Springer, pp. 142–150. doi: 10.1007/978-3-642-39191-0_16.

McCarthy, J. and Wright, P. (2004) ‘Technology as Experience’, *Interactions*, 11(5), pp. 42–43. doi: 10.1145/1015530.1015549.

McNaull, J. *et al.* (2014) ‘Flexible Context Aware Interface for Ambient Assisted Living’, *Human-centric Computing and Information Sciences*, 4(1), p. 1. doi: 10.1186/2192-1962-4-1.

Mennicken, S. and Huang, E. M. (2012) ‘Hacking the Natural Habitat: An In-the-wild Study of Smart Homes, Their Development, and the People Who Live in Them’, in *International conference on pervasive computing*. Springer, pp. 143–160. doi: 10.1007/978-3-642-31205-2_10.

Nielsen, J. (2005) *Ten Usability Heuristics*. Available at: https://bit.ly/3iOY9hI (Accessed: 16 June 2021).

Niemantsverdriet, K., van Essen, H. and Eggen, B. (2017) ‘A Perspective on Multi-user Interaction Design Based on an Understanding of Domestic Lighting Conflicts’, *Personal and Ubiquitous Computing*, 21(2), pp. 371–389. doi: 10.1007/s00779-016-0998-5.

Nissenbaum, H. (2004) ‘Privacy as Contextual Integrity’, *Wash. L. Rev.*, 79, p. 119.

OASIS (2013) *Extensible Access Control Markup Language (XACML) Version 3.0*. Available at: https://bit.ly/2TFIFSF (Accessed: 16 June 2021).

Oxford (2020) *Oxford Learners Dictionary*. Available at: https://bit.ly/2S4F8Nh (Accessed: 20 April 2020).

Palen, L. and Dourish, P. (2003) 'Unpacking "Privacy" for a Networked World', in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Ft. Lauderdale, Florida, USA: Association for Computing Machinery (CHI '03), pp. 129–136. doi: 10.1145/642611.642635.

Paternò, F., Mancini, C. and Meniconi, S. (1997) 'Concurtasktrees: A Diagrammatic Notation for Specifying Task Models', in *Human-computer interaction INTERACT'97*. Springer, pp. 362–369. doi: 10.1007/978-0-387-35175-9_58.

Petronio, S. (1991) 'Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information between Marital Couples', *Communication Theory*, 1(4), pp. 311–335. doi: 10.1111/j.1468-2885.1991.tb00023.x.

Petronio, S. (2002) *Boundaries of Privacy: Dialectics of Disclosure*. Suny Press.

Petronio, S. (2015) 'Communication Privacy Management Theory', in *The International Encyclopedia of Interpersonal Communication*. American Cancer Society, pp. 1–9. Available at: https://bit.ly/3zAmopw.

Reagle, J. and Cranor, L. F. (1999) 'The Platform for Privacy Preferences', *Communications of the ACM*, 42(2), pp. 48–55. doi: 10.1145/293411.293455.

Reeder, R. W. *et al.* (2008) 'Expandable grids for visualizing and authoring computer security policies', in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 1473–1482. doi: 10.1145/1357054.1357285.

Reenskaug, T. M. H. (1979) 'The Original MVC Reports'. Available at: https://bit.ly/3xnbVMg.

Ren, J. *et al.* (2019) 'Information Exposure from Consumer IoT Devices: A Multidimensional, Network-informed Measurement Approach', in *Proceedings of the Internet Measurement Conference*, pp. 267–279. doi: 10.1145/3355369.3355577.

Rogers, Y. (2006) 'Moving on from Weiser's Vision of Calm Computing: Engaging UbiComp Experiences', in Dourish, P. and Friday, A. (eds) *UbiComp 2006: Ubiquitous Computing*. Berlin,

Heidelberg: Springer (Lecture Notes in Computer Science), pp. 404–421. doi: 10.1007/11853565_24.

Rogers, Y., Sharp, H. and Preece, J. (2011) *Interaction Design: Beyond Human-computer Interaction*. John Wiley & Sons.

Samuel, S.S.I. (2016) 'A review of connectivity challenges in IoT-smart home', in *2016 3rd MEC International conference on big data and smart city (ICBDSC)*. IEEE, pp. 1–4. doi: 10.1109/ICBDSC.2016.7460395

Schaub, F. M. (2014) *Dynamic Privacy Adaptation in Ubiquitous Computing*. Dissertation. Universität Ulm. doi: http://dx.doi.org/10.18725/OPARU-3188.

Schipor, O.-A., Vatavu, R.-D. and Wu, W. (2019) 'SAPIENS: Towards Software Architecture to Support Peripheral Interaction in Smart Environments', *Proceedings of the ACM on Human-Computer Interaction*, 3(EICS), p. 11:1-11:24. doi: 10.1145/3331153.

Shang, S. *et al.* (2014) 'The Application of Differential Privacy for Rank Aggregation: Privacy and Accuracy', in *17th International Conference on Information Fusion (FUSION)*. IEEE, pp. 1–7.

Shin, D. (2020) 'User Perceptions of Algorithmic Decisions in the Personalized AI System: Perceptual Evaluation of Fairness, Accountability, Transparency, and Explainability', *Journal of Broadcasting & Electronic Media*, 64(4), pp. 541–565. doi: 10.1080/08838151.2020.1843357.

Skillen, K.-L. *et al.* (2014) 'Ontological User Modelling and Semantic Rule-based Reasoning for Personalisation of Help-on-demand Services in Pervasive Environments', *Future Generation Computer Systems*, 34, pp. 97–109. doi: 10.1016/j.future.2013.10.027.

Smirek, L., Zimmermann, G. and Ziegler, D. (2014) 'Towards Universally Usable Smart Homes – How Can MyUI, URC and openHAB Contribute to an Adaptive User Interface Platform?', *IARIA, Nice, France*, pp. 29–38.

Solove, D. J. (2006) 'A Taxonomy of Privacy', *University of Pennsylvania Law Review*, 154(3), p. 477. doi: 10.2307/40041279.

Such, J.M. and Criado, N. (2018) 'Multiparty privacy in social media', Communications of the ACM, 61(8), pp. 74–81. doi: 10.1145/3208039

W3C (2002) *A P3P Preference Exchange Language 1.0 (APPEL1.0)*. Available at: https://bit.ly/3vrM30A (Accessed: 15 January 2021).

Warren, S. D. and Brandeis, L. D. (1890) 'Right to Privacy', *Harv. L. Rev.*, 4, p. 193. doi: 10.2307/1321160.

Weiser, M. (1993) 'Hot Topics-ubiquitous Computing', *Computer*, 26(10), pp. 71–72. doi: 10.1109/2.237456.

Weiser, M., Gold, R. and Brown, J. S. (1999) 'The Origins of Ubiquitous Computing Research at Parc in the Late 1980s', *IBM Systems Journal*, 38(4), pp. 693–696. doi: 10.1147/sj.384.0693.

Westin, A. F. (1967) 'Privacy and Freedom', *New York: Atheneum*, 7, pp. 431–453.

Wijesundara, A. (2021a) 'PASHI-framework Usability Evaluation Study Interview Transcripts'. The Open University. doi: 10.21954/ou.rd.14812575.v1.

Wijesundara, A. (2021b) 'PASHI-framework Usability Evaluation Study Storyboards'. The Open University. doi: 10.21954/ou.rd.14812578.v1.

Wijesundara, A. (2021c) 'PASHI-framework User Experience Evaluation Study Interview Transcripts'. The Open University. doi: 10.21954/ou.rd.14812587.v1.

Wijesundara, A. (2021d) 'PASHI-framework User Experience Evaluation Study Video Prototypes'. The Open University. doi: 10.21954/ou.rd.14812584.v1.

Yang, J., Yessenov, K. and Solar-Lezama, A. (2012) 'A Language for Automatically Enforcing Privacy Policies', *ACM SIGPLAN Notices*, 47(1), pp. 85–96. doi: 10.1145/2103656.2103669.

Yao, Y. *et al.* (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. the 2019 CHI Conference*, Glasgow, Scotland UK: ACM Press, pp. 1–12. doi: 10.1145/3290605.3300428.

Youngblood, G. M. *et al.* (2005) 'Automation Intelligence for the Smart Environment', in *In: Proceedings of IJCAI*, pp. 1513–1514. Available at: https://bit.ly/3wA5pC6.

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)*, pp. 65–80. Available at: https://bit.ly/2TEDAtE.

Zeng, E. and Roesner, F. (2019) ‘Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study’, in *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pp. 159–176. Available at: https://bit.ly/3C6y0ko (Accessed: 13 November 2021).

Zheng, S. *et al.* (2018) ‘User Perceptions of Smart Home IoT Privacy’, *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW), p. 200:1-200:20. doi: 10.1145/3274469.

Zheng, X., Cai, Z. and Li, Y. (2018) ‘Data Linkage in Smart Internet of Things Systems: A Consideration from a Privacy Perspective’, *IEEE Communications Magazine*, 56(9), pp. 55–61. doi: 10.1109/MCOM.2018.1701245.

10. Appendices

10.1 Appendix A: Methods, Tools and Analysis Techniques

The following section presents the methods, tools and analysis techniques mentioned in Chapter 3.

10.1.1 Usability Testing

Usability testing is a method used in HCI research to understand how the users perceive the usability of a system or an interaction (Lazar, Feng and Hochheiser, 2017). Sometimes this is also called as 'user-testing' as the focus is a lot on the user's perception. There can be different tools used to conduct usability testing. Generally, it follows a process of presenting a stimulus and use that to generate user responses regarding the usability. Stimulus can vary in the level of fidelity where it can range from low fidelity paper-prototypes to high-fidelity concrete implementation of the system. In this study I have utilised a storyboard as the stimulus to depict adaptive user interfaces. User responses can be gathered quantitively, qualitatively or a mix of both.

10.1.2 Storyboards

Storyboards (verb: storyboarding) are a type of low-fidelity prototypes, which is used to demonstrate interaction tasks and to generate user responses. Storyboards can be created using a series of sketches demonstrating how a user would progress through an interaction (Rogers, Sharp and Preece, 2011). A high-level interaction task can be divided into sub tasks where each sub task can be demonstrated by a sketch. When used in conjunction with a scenario, storyboards generate richer user responses cheaply and quickly compared high fidelity prototypes. Storyboards were used in the usability study to show case how different user interface variations work with different interpersonal privacy violation scenarios within the smart home space.

10.1.3 Semi-structured Interviews

Semi-structured Interviews allow the researcher to have a direct discussion with the users about the system that they are using and gather feedback. Interviews can be free-form un-structured, semi-structured or fully structured (Rogers, Sharp and Preece, 2011). As the names suggests free-form unstructured interviews refers to discussions with the user without a specific set of questions where fully structured interviews refer to discussions with the user with a pre-defined set of questions.

Semi-structured interviews sit in between where the interviewer starts the interview with a set of pre-defined questions, but as the interview goes on, the interviewer can allow the interview to flow in the direction of interviewee is driving it. Semi-structured interviews give the best of both worlds, where the structured set of questions will generate the necessary output from the user where free-form aspect of the interview would generate ideas which the researcher might not have thought before to inquire. I would be using semi-structured interviews in both of my user studies (usability evaluation and user experience evaluation) as a tool to collect user feedback.

10.1.4 Card Sorting

Card sorting is a method used in HCI research to understand the users' mental model of a specific interaction or a system (Nawaz, 2012). Card sorting is mainly used in the information structuring of websites, but it is also used to measure other metrics such as the usability of a system. Card sorting uses cards with statement/phrase/reaction on them where participants will be asked to arrange them based on their mental model depending on the goal of the study. Therefore, card sorting used for system evaluation allows quick and cheap evaluation of user perception of that system. One of the product-specific variations of card-sorting tools is the Microsoft product reaction cards set (Benedek and Miner, 2002). The entire set has 118 reactions where I have used a reduced version with 64 words. The reduced version helped to keep the participants focused on the task without inducing too much fatigue as they progressed through multiple scenarios during the study. Microsoft product reaction cards were used in storyboard study to understand the participant-reactions to different variations of adaptive user interfaces. Apart from that reaction card choices helped to triangulate the data collected from other research tools.

10.1.5 System Usability Scale (SUS)

System usability scale (SUS) is a commonly utilised questionnaire in evaluating the usability of systems (Brooke, 1996). SUS consists of 10 questions where a respondent can pick an answer out of five responses to define the level of agreement. SUS provides a quick and cheap way to evaluate usability of a system which can also be analysed using statistical methods. I have used SUS in my user study to evaluate usability of different variations of adaptive user interfaces. SUS also provides means to conduct statistical analysis to identify statistical significance between various user interface types.

10.2 Appendix B: User Interface Frameworks and Privacy Authoring Languages

User Interface Frameworks

10.2.1 Dynamo-AID

Dynamo-AID (Clerckx, Luyten and Coninx, 2004)is a modal based runtime architecture for user interface development. They used concurrent task trees and also have focused on the distribution of information across multiple interfaces. Dynamo-AID has focused on task modelling which is an important factor for adaptation of interfaces. Dynamo-AID's modelling of tasks using concurrent task trees (CTT) (Paternò, Mancini and Meniconi, 1997) is one of the first comprehensive examples on how CTT can be used to model interaction in the ubiquitous computing domain.

10.2.2 MASP Framework

The MASP (Blumendorf, 2009) framework provides executable models, reference meta-models for UIs and a run-time architecture. Executable models define how the system should behave at run-time where they use static and dynamic content when in use. Reference meta-models for the UI were based the Cameleon reference framework (Calvary, Coutaz and Thevenin, 2001) and it manages to provide a comprehensive user interface description language for smart environments. The MASP run-time architecture connects the executable models, reference meta-models for UI and the other services together. The MASP framework takes into consideration the interaction resources and context information during the adaptation.

10.2.3 AALuis User Interface Generation Framework

The AALuis user interface generation framework (Mayer *et al.*, 2013) focuses on a middleware for giving a personalised interface for users with different abilities (especially for older adults). Mayer et al. speak about user context models, device context models, service context models and environmental context models. The AALuis focuses on extendibility, where they discuss integrating personalised user interfaces to multiple middleware services. They use concurrent task trees (Mori, Paternò and Santoro, 2002) to model tasks, in the same manner as Dynamo-AID (Clerckx, Luyten and Coninx, 2004).

10.2.4 AALFI

AALFI (McNaull *et al.*, 2014) focuses on adaptive context aware sensitive interface for ambient assisted living during night time. Architecture consists of a feedback module which takes into account the interventions that occur, and the framework learns from its interaction and intervention history.

10.2.5 CEDAR Architecture

The Cedar architecture (Akiki, 2014) is a reference architecture for developing adaptive model-driven enterprise application UIs. They have based their framework on the Cameleon reference framework (Calvary, Coutaz and Thevenin, 2001), three-layer architecture (Kramer and Magee, 2007) and the Model-View-Controller architecture (Reenskaug, 1979). They have also provided an IDE to define and generate adaptive UIs for enterprise application named Cedar Studio and algorithms to adapt the UIs which they named as Role-Based UI Simplification (RBUIS) mechanism. They have used feature-set minimisation and layout optimisation to adapt the UI layer. The Cedar architecture has used CTT (Paternò, Mancini and Meniconi, 1997) (Mori, Paternò and Santoro, 2002) to design the interactions and have used RBUIS to pick the simplified UI.

The main focus of the RBUIS mechanism has been improving the usability by simplifying the cluttered GUI of enterprise applications. Therefore, the Cedar architecture has not focused on multimodal UIs for smart homes nor users' privacy preferences. Even though the Cedar architecture has not focused on the smart home domain, their architecture for adaptive UI generation, use of CTT to define adaptive UI and the use of the RBUIS mechanism to create the most appropriate UIs can be quite valuable when focusing on the privacy aware smart home UIs.

10.2.6 GPII Personalisation Infrastructure

The GPII personalisation infrastructure presents a knowledge-based framework which guides the generation of different layers of multi-modal application to provide universal accessibility. They discuss transferring user profiles across smart spaces and also adaptation happening at the operating system level. They have also discussed conflicting configurations when multiple users are there, but the assessment was only focused on application-level conflicts. GPII presents components to evaluate the context, to evaluate the users and their preferences and devices. These features help to handle the dynamics of smart environments as multiple users tend to have varying preferences and when they move from one smart environment to another, their personal devices should be considered as part of the new environment removing from the environment they left.

Apart from the aforementioned features of GPII, it has multiple drawbacks as a framework defined to generated adaptive multimodal UIs in smart environment. They have not modelled the physical layout of a smart environment, leaving out features such as user location in the smart space. The support for privacy preservation is also not sufficient to cover the full spectrum of issues that could

arise when there are simultaneous users. The GPII framework is mostly for single user-based system where they have focused a lot on migrating user profiles across multiple smart spaces, but they have not focused on scenarios where there are different users with different goals. Another drawback was with the evaluation as they have only been tested with expert users not with real users (heuristic evaluation).

10.2.7 MIODMIT

MIODMIT (Cronel *et al.*, 2019) is a model based generic architecture for smart environments supporting multimodal UIs. The architecture focused on software as well hardware aspects of the smart environments. Since they have focused on hardware aspect of smart environments, they have highlighted device drivers in their architecture. There has been no mention on user preference modelling and smart environment layout modelling within their architecture. They have also not described how UI modelling happens during implementation as the architecture discusses most of the components at a high-level. Therefore, the MIODMIT architecture has to be improved to meet our requirements of privacy-aware adaptive UI.

10.2.8 AM4I Architecture and Framework

AM4I (Almeida *et al.*, 2019) provides and architecture and a framework to design multimodal and multi-device smart home UIs. The architecture provides components support input and output modalities, fusion and fission, and models to handle context and users. The framework supports concrete deployment of the architecture to create interactions within the Smart home. AM4I gives basic support for user modelling and context modelling, in that they have touched upon user's privacy and user interface preferences. They mentioned the possibilities of interpersonal cyber physical privacy violations that could happen at the UI layer.

AM4I has some drawbacks where it needs to be improved to suit our requirement of a privacy aware adaptive UI. One of the drawbacks of the framework was the lack support for multiple users in real time. Furthermore, the context models and the user models need to be developed further. Improvement of the context models would allow the framework to handle the spatial layout of the smart home which is required for privacy violation detection. User modelling needs to be improved to provide more detailed user capabilities, privacy preferences and user interface preferences. This improvement is required to handle the all the possible interpersonal cyber physical privacy violations.

10.2.9 SAPIENS

Sapiens (Schipor, Vatavu and Wu, 2019) is an engineering framework for interactive smart home systems. They have built upon the EUPHORIA engine (Schipor, Vatavu and Vanderdonckt, 2019)

to create the Sapiens framework. Apart from components to handle generic multimodal UI, the framework provides modes to support user and device tracking, priority management, context awareness, prediction of interruptions, and device interchangeability.

The Sapiens framework has a few drawbacks. Even though it has components to predict possible interruptions, it does not have components to capture users' privacy preferences and UI preferences. It has provided spatial modelling for smart home entities, but it was only tested using a web-based prototype. Therefore, it needs to be tested with real-world applications. Furthermore, it does not discuss in detail how the UI adaptations are executed.

Privacy authoring languages

10.2.10 P3P

P3P (Reagle and Cranor, 1999) provided means to manage privacy of data requests that happen via the web. P3P sends a machine-readable and partially human-readable proposal of the service provider's privacy practices when accessing web-services. From the user's point of view, they could use software tools (user agents) such as web browsers, browser plugins or proxy servers to automatically parse these proposals. To cater for different user privacy preferences, an organization can create multiple proposals with varying user services. In this manner, P3P provides a level of flexibility for service providers as well as the users. P3P uses XML and RDF based syntax to write the privacy proposals and can be implemented on existing HTTP/1.1. compliant web services. An example of the company's privacy practices (Listing 10.1) and the P3P version (Listing 10.2) of the policy from Reagle and Cranor's is shown below (Reagle and Cranor, 1999).

```
CoolCatalog makes the following statement for the Web pages at
www.CoolCatalog.com/catalogue/. We collect clickstream data in our HTTP
logs. We also collect your first name, age, and gender to customize our
catalogue pages for the type of clothing you are likely to be interested
in and for our own research and product development. We do not use this
information in a personally identifiable way. We do not redistribute any
of this information outside of our organization. We do not provide
access capabilities to information we may have from you, but we do have
retention and opt-out policies, which you can read about at our privacy
page CoolCatalog.com/PrivacyPractice.html. The third-party Privacy
Seal.org provides assurance that we abide by this agreement.
```

Listing 10.1: Company Privacy Policy Description

```
<PROP realm=“http://CoolCatalog.com/catalogue/” entity=“CoolCatalog”
propID=“94df1293a3e519bb”> <USES>
<STATEMENT purpose=“1” recipient=“0” id=“0”> <REF
name=“Web.Abatract.ClientClickStream”/>
    </STATEMENT></USES>
  <USES>
<STATEMENT purpose=“2,3” recipient=“0” id=“0” consequence=“a site with
clothes you’d appreciate.”> <WITH><PREFIX name=“User.”>
<REF name=“Name.First”/>
<REF name=“Bdate.Year” OPTIONAL=“1”/> <REF name=“Gender”/>
</PREFIX></WITH>
</STATEMENT></USES>
<DISCLOSURE discURI=“http://CoolCatalog.com/
PrivPractice.html” access=“3” other=“0,1”/>
<ASSURANCE org=“http://PrivacySeal.org” text=“third party”
image=“http://PrivacySeal.org/Logo.gif”/>
</PROP>
```

Listing 10.2: Company Privacy Policy - P3P Version

The creators of P3P predicted that it would revolutionize web-services, but it was not adopted by many users. Consequently, P3P was discontinued. One of the reasons was that, to reap the full benefits of P3P it had to be widely adopted where service providers were reluctant to adopt due to the same reason. Furthermore, P3P was also slowed down the web interactions as it consists of lot of processing overhead (Electronic Privacy Information Center, 2000). Even though P3P did not live up to its expectations, it highlighted the importance of giving users the control of their privacy and automating privacy control when surfing the web

10.2.11 Ponder

Ponder is a policy language created by the Imperial College, London (Damianou *et al.*, 2001) for access control in management and security of complex distributed systems. Ponder is an object oriented, declarative, strongly typed language. Therefore, it is flexible, extensible and supports easy analysis of policies. Ponder is based on roles-based access control where it can be associated with a certain position in the organisation. There can be groups of people assigned to a certain role where the level of access certain roles has over resources can be controlled using Ponder policies.

Ponder provides four types of access controls namely authorisation policies, delegation policies, information filtering policies and refrain policies. Authorisation policies provides the policy author to define who can access a certain resource (positive rule) or who is not allowed to access a certain resource (negative rule). Listing 10.3 shows the syntax of a standard authorisation policy where terms in bold are keywords. *Subject* represents the role which tries to access a certain resource where *target* represents the resource that is the policy is defined for. *Action* represents the action which the subject is allowed/restricted to enact upon the resource and *when* is used to define the constraints. Choices are represented using round brackets "( )" where the options are separated by the " | " sign. Elements within square brackets " [ ] " are optional where braces "{ }" represent repetitions.

```
Inst ( auth+ | auth- ) policyName "{"
      subject [<type>] domain-Scope-Expression ;
      target  [<type>] domain-Scope-Expression ;
      action           action-list ;
      [ when           constraint-Expression ; ]     "}"
```

Listing 10.3: Ponder Authorisation Policy Syntax

Listing 10.4 shows an example extracted from the original Ponder document. Policy description defines a scenario where the Role: NetworkAdmin is allowed to do certain actions on the objects of the type PolicyT within the domain Nregion/switches.

Policy description: Members of the NetworkAdmin domain are authorised to load, remove, enable or disable objects of type PolicyT in the Nregion/switches domain.

```
inst auth+ switchPolicyOps {
subject /NetworkAdmin;
target <PolicyT> /Nregion/switches;
action load(), remove(), enable(), disable() ;

}
```

Listing 10.4: Ponder Authorisation Policy Example

Information filtering policies enables the policy author to define the level of disclosure for certain resources. Depending on the context, these policies can limit the exposure of certain details of the restricted resource. Delegation policies allow the author to write policies to transfer the access rights to certain roles depending on the context. Refrain policies are written from the resources' point of view where it defines what sort of actions are not allowed to be performed on the said resource. Later on, Ponder 2 was introduced (Kagal, 2002) improving on Ponder. Ponder 2 was based on the fundamentals of ponder where they defined a new language named Ponder-talk which was based on Smalltalk to define policies.

10.2.12 Rei

Rei (Kagal, 2002) is a general-purpose policy language and uses first order logic. It was created to make policy authoring simple and universally applicable. Furthermore, Rei can be used to multiple domains such as security domain, management domain and pervasive computing domain. Rei uses deontic logic which consists of four policy objects: *rights, prohibitions, obligations and dispensations* to compose its rules. These policy objects (@) are written according to Listing 10.5, where *Actions* refer to domain dependent actions and *Conditions* refer to restrictions which are domain dependent.

```
@(Action, Conditions)
```

Listing 10.5: Rei Policy Object

These policy objects are paired with subjects (roles) using *has* constructs as shown in Listing 10.6.

```
has(Subject, Policy Object)
```

Listing 10.6: Rei Policy Object and Subject Linking

Four policy objects are used to construct different policies. *Rights* refer to the subject's permissions. *Prohibitions* refers to subject's restrictions or negative permissions. *Obligations* refer to actions which needs to be executed after a certain event is triggered. Lastly, *Dispensations* refers to subject's obligations which are expired. Rei also described action specifications (Listing 10.7), which are used to write policies with more descriptive contextual information.

```
Action (ActionName, TargetObjects, Pre-Conditions, Effects)
```

Listing 10.7: Rei Action Template

ActionName refers to the identifier of the action where *TargetObjects* are the objects that subjects try to access. *Pre-Conditions* refer to different conditions that needs to be fulfilled for the rule to be valid. *Effect* means the final result of the rule.

Listing 10.8 shows an example I have extracted from the original paper. This defines a rule where John has access to read papers at work as long as those papers are technical papers.

```
has(john, right(action(readingTechPapers, X, [technical-paper(X), not-
read(X)], [assert(read(X))]), [atWork(john)]))
```

Listing 10.8: Rei Policy Language Example

10.2.13 XACML 3.0

XACML (OASIS, 2013) is a comprehensive attribute-based access control (ABAC) policy language which was introduced in 2003 with its first version where its latest version (3.0) was released in 2013 with multiple improvements to its architecture and with JSON support (XACML to refer to XACML 3.0 unless specified otherwise. XACML).

At the time of introduction, a key feature of XACML in comparison with other policy languages was the separation of models of its data flow model. XACML data flow model consists of multiple models which are responsible for different aspects of the policy language and its execution. Policy administration point (PAP) is the system entity which creates policies or policy sets on a specific target. Policy enforcement point (PEP) is used to make decision requests and to enforcing those requests. Policy decision point (PDP) will evaluate authorization requests and decide if the request can be authorized. Policy information point (PIP) would provide the attribute values required for the decision making. This type of separation of concerns allowed XACML to be used in complex systems with changing policies.

the XACML policy language model consists of three main components: 1) Rule 2) Policy and 3) Policy set. A policy set may contain multiple policies where a policy may contain multiple rules.

A *Target* is a set of simplified conditions which needs to be fulfilled for a rule, a policy or a policy set to be applied for a given request. A target may also define that it applies to any request. *Condition* further refines the context in which the rule can be applied using a Boolean expression, but they only exist in rules. XACML also provides obligation expression and advice expressions. An obligation expression directs the PEP to take certain actions after or before a request is approved. Advice expression is similar to obligation, but its execution is optional. *Effect* denotes the outcome of a rule, where it can “permit” or “deny” access of the request.

XACML also provides the option to combine rules using the “rule combining algorithm” and the option to combine policies using the “policy combining algorithms”. These algorithms are quite useful when it is needed to aggregate rules or policies as well as to resolve conflicts between rules or policies.

In the Listing 10.9, provides an example from the original XACML 3.0 publication by OASIS standard. In this example, a cooperation named Medi Corp (domain name: med.example.com) has an access control policy for users with an email of the type “med.example.com” to perform any

action on any of the resource of the corporation. The example includes additional information which would have been the standard in a real implementation of the XACML.

```
<?xml version="1.0" encoding="UTF-8"?>
 <Policy
   xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="urn:oasis:names:tc:xacml:3.0:core:sch
ema:wd-17
   http://docs.oasis-open.org/xacml/3.0/xacml-core-v3-
schema-wd-17.xsd"
   PolicyId="urn:oasis:names:tc:xacml:3.0:example:SimplePoli
cy1"
   Version="1.0"
   RuleCombiningAlgId="identifier:rule-combining-
algorithm:deny-overrides">
  <Description>
    Medi Corp access control policy
  </Description>
  <Target/>
  <Rule
    RuleId=
"urn:oasis:names:tc:xacml:3.0:example:SimpleRule1"
    Effect="Permit">
    <Description>
      Any subject with an e-mail name in the med.example.com
domain
      can perform any action on any resource.
    </Description>
    <Target>
      <AnyOf>
        <AllOf>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:r
fc822Name-match">
          <AttributeValue
            DataType="http://www.w3.org/2001/XMLSchema#strin
g"
              >med.example.com</AttributeValue>
          <AttributeDesignator
            MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subjec
t:subject-id"
            DataType="urn:oasis:names:tc:xacml:1.0:data-
type:rfc822Name"/>
          </Match>
        </AllOf>
      </AnyOf>
    </Target>
  </Rule>
</Policy>
```

Listing 10.9: XACML Policy Example

10.3 Appendix C: Usability Evaluation Study

10.3.1 Study Resources

10.3.1.1 Consent Form

Informed Consent Form (01/11/2019 Version 1.0)

Participant Identification Number: _____

CONSENT FORM

Title of Project: Privacy Aware Adaptive User Interfaces in Smart Homes

Name of Researcher: Akshika Wijesundara

	Please initial all relevant boxes
1. I confirm that I have read and understand the information sheet for the above study (version 1.0, 01/11/2019).	☐
2. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.	☐
3. I understand that my participation is voluntary and that I am free to withdraw at any time without giving any reason.	☐
4. I understand that if I withdraw after the study period it may not be possible to delete my anonymised data if it has already been analysed for publication.	☐
5. [OPTIONAL] I have provided an e-mail address and/or mobile phone number below so that the research team can send me updates relating to this study.	☐
6. **I agree to take part in the above study.**	☐

Name of Participant (please print)	Date	Signature
Participant e-mail address (optional)	Participant Mobile Phone (optional)	

10.3.1.2 Participant Information Sheet

Usability and Accuracy of Privacy Aware Adaptive User Interfaces as Opposed to Non-adaptive User Interfaces

Participant Information Sheet (Version 1.0, 24/11/2019)

We would like to invite you to take part in our research study. Before you decide we would like you to understand why the research is being done and what it would involve for you. We suggest that it may take about 5 minutes to read thoroughly. If, after reading this information sheet, you think you may be interested in taking part you will have the opportunity to ask any questions before you agree to anything.

Summary

Our homes are becoming smarter by the day. We interact with our homes using user interfaces such as smart speakers, smart TVs and other types of smart home interfaces. While interacting with these user interfaces there is a risk of our privacy being violated as our interactions could leak information to other users in the vicinity. There is also the possibility of these interactions over public user interfaces disturbing the other users in the smart home. This study involves my solution of privacy aware adaptive user interfaces which would protect privacy of the smart home users while preserving the usability.

What's involved?

After reading this sheet and having any questions answered, if you would like to take part you will be asked to sign a consent form. The entire study (including the questionnaires) will take ~40-45 minutes to complete.

Your first task will be to read two hypothetical scenarios in a smart home setting and evaluate the different configurations of the smart home's user interfaces for their accuracy and usability. You will be given a usability measurement questionnaire to fill after reviewing each interface configuration.

In the end we will conduct a brief interview and ask you to fill in a small questionnaire with regard to your experience with the system.

What are the potential benefits and risks?

The only direct benefit to you is the opportunity to experience some leading-edge research. There are no foreseeable risks arising from participation in this research and while you will not receive any payment, you will make a vital contribution to privacy aware adaptive interfaces in smart homes research and possibly improving the experience for others.

What will happen if I don't want to carry on with the study?

Your participation in the study is entirely **voluntary**, and you can choose to withdraw at any time without giving a reason. You may also ask to have your data deleted at any time, although if we have analysed and combined your data with others' this may not be possible. Your data will be analysed within a period of one month from the date that you have participated in the study. After the period of one month, we are unable to delete your data.

How will my information be kept confidential?

The data collected will only be accessible to the named researchers on this study. Personally, identifying information will not be electronically stored with your data. Instead, a unique ID will be generated to record your data and we will ensure that you can never be identified by any data we publish.

The data will be retained for up to 5 years after the study. The results of this study may be published in a scientific journal. If you would like to receive the results of the study, you can indicate this on the consent form.

Who is organising and funding this study?

This research is in part being supported by a research grant from the Engineering and Physical Sciences Research Council and researchers from the Open University.

Who has reviewed this study?

This research has been reviewed and approved by the Open University's Human Research Ethics Committee and has been given a favourable opinion (REF HREC/3417/Wijesundara)

Invitation to ask further questions

Please feel free to ask any member of the researcher team if you have any concerns or questions in relation to this study before agreeing to the Consent Form. You may also ask any questions throughout and after completion of the study.

You can contact the researchers as follows:

Akshika Wijesundara (Researcher): akshika.wijesundara@open.ac.uk (Phone: 07754312540)
Prof Arosha Bandara (Supervisor): arosha.bandara@open.ac.uk
Prof Blaine Price (Supervisor): b.a.price@open.ac.uk
Prof Bashar Nuseibeh (Supervisor): bashar.nuseibeh@open.ac.uk

Thank you for taking the time to read this information sheet and considering taking part in this study

10.3.1.3 Storyboard Study Scenarios

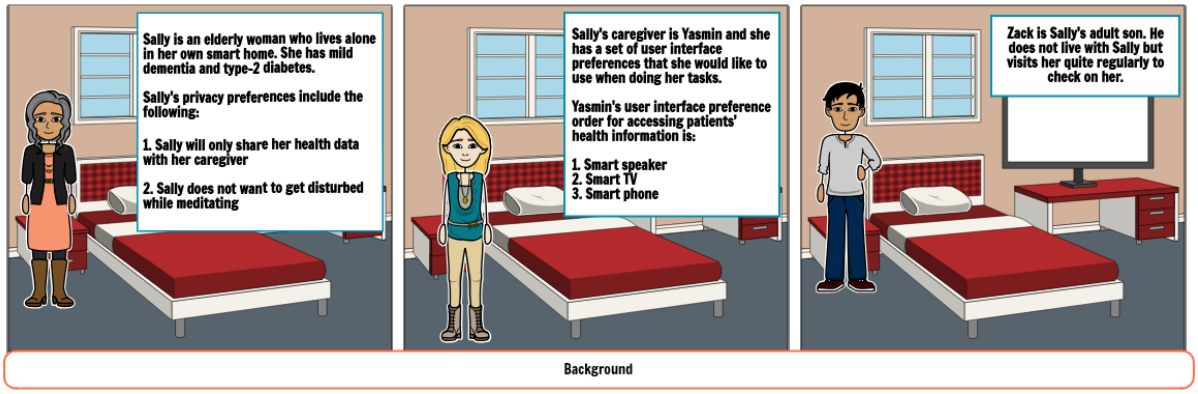

Figure 10.1: Base Case Storyboard

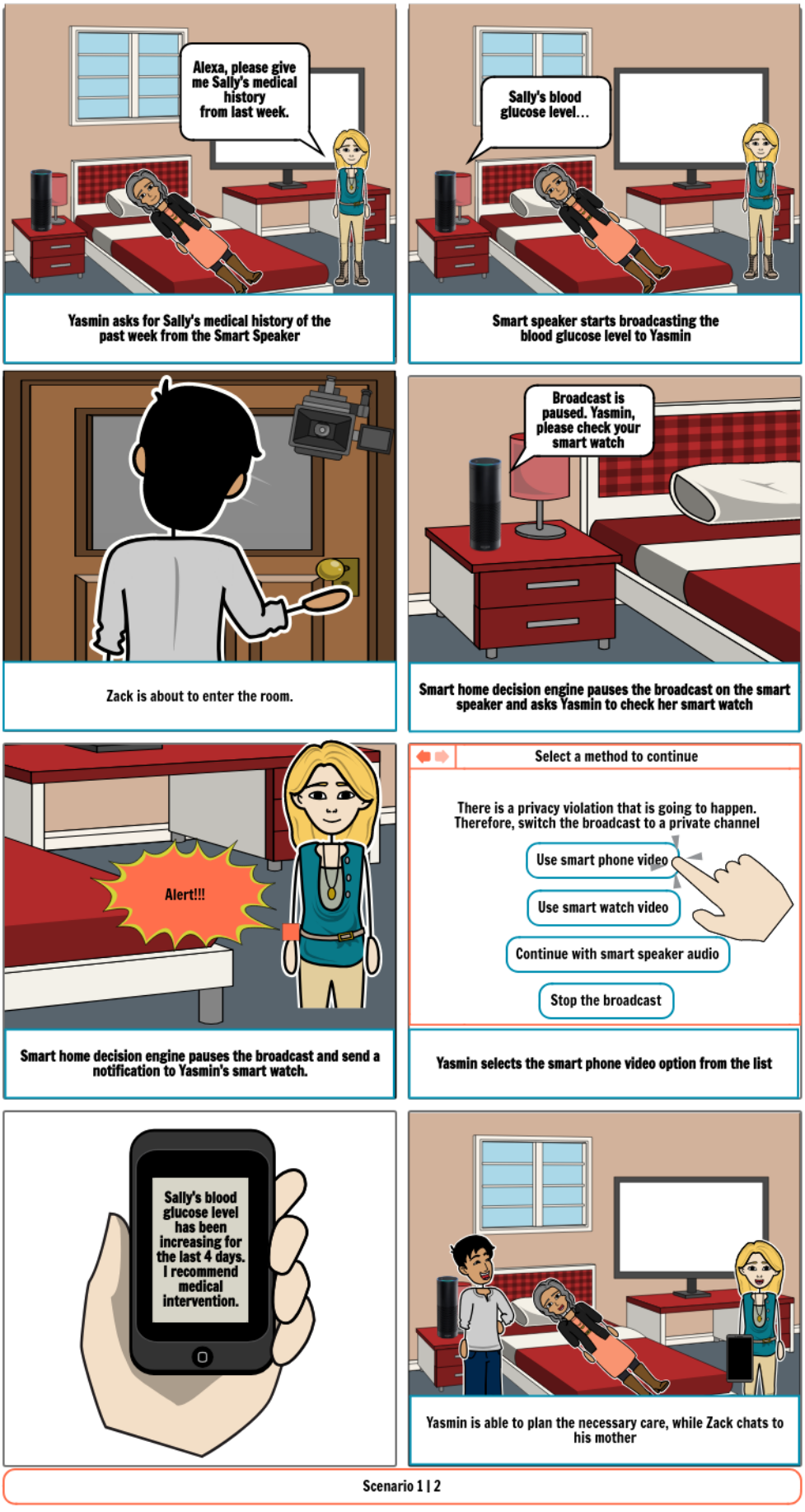

Figure 10.2: CAUI Information Disclosure Scenario Storyboard

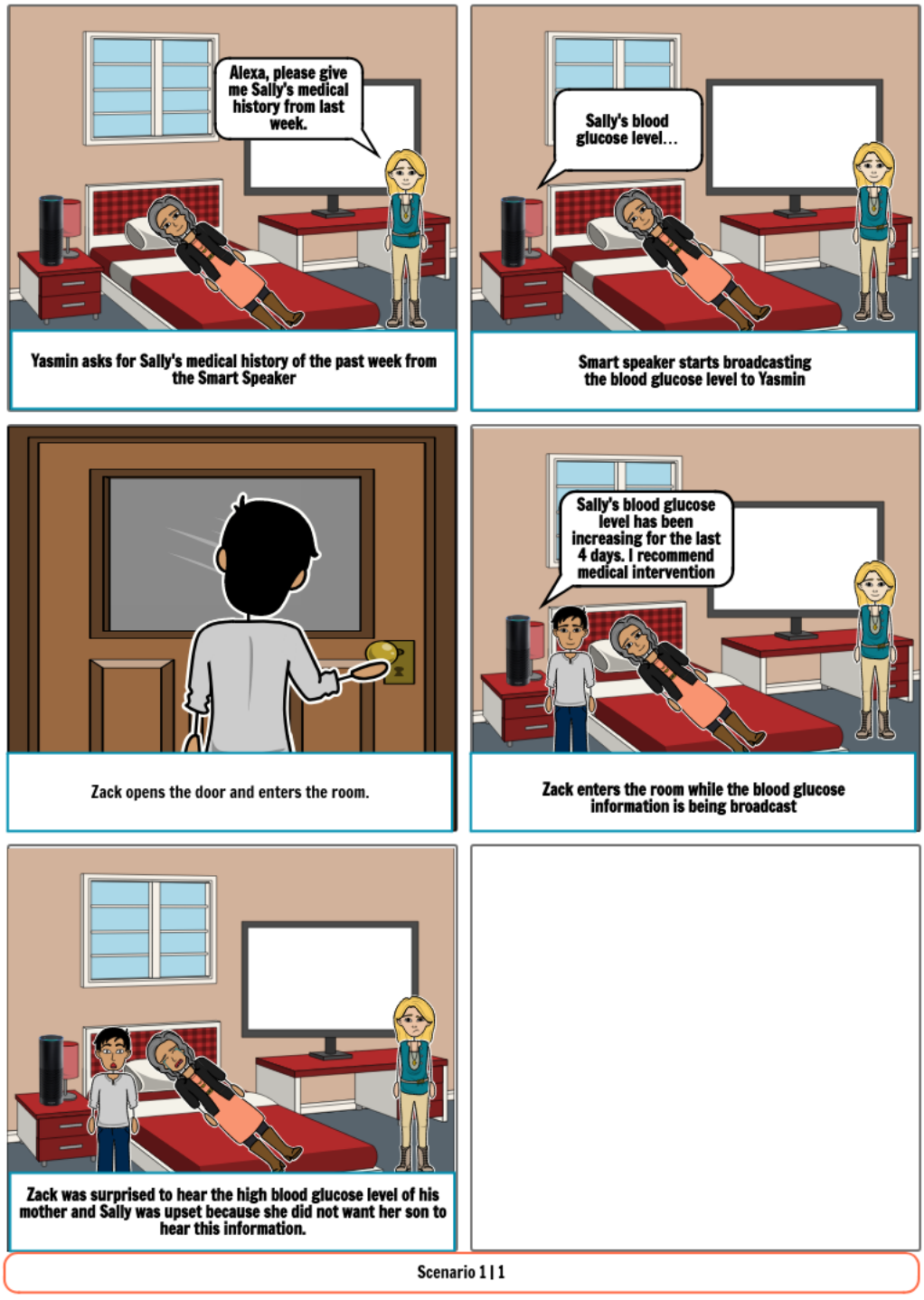

Figure 10.3: NAUI Information Disclosure Scenario Storyboard

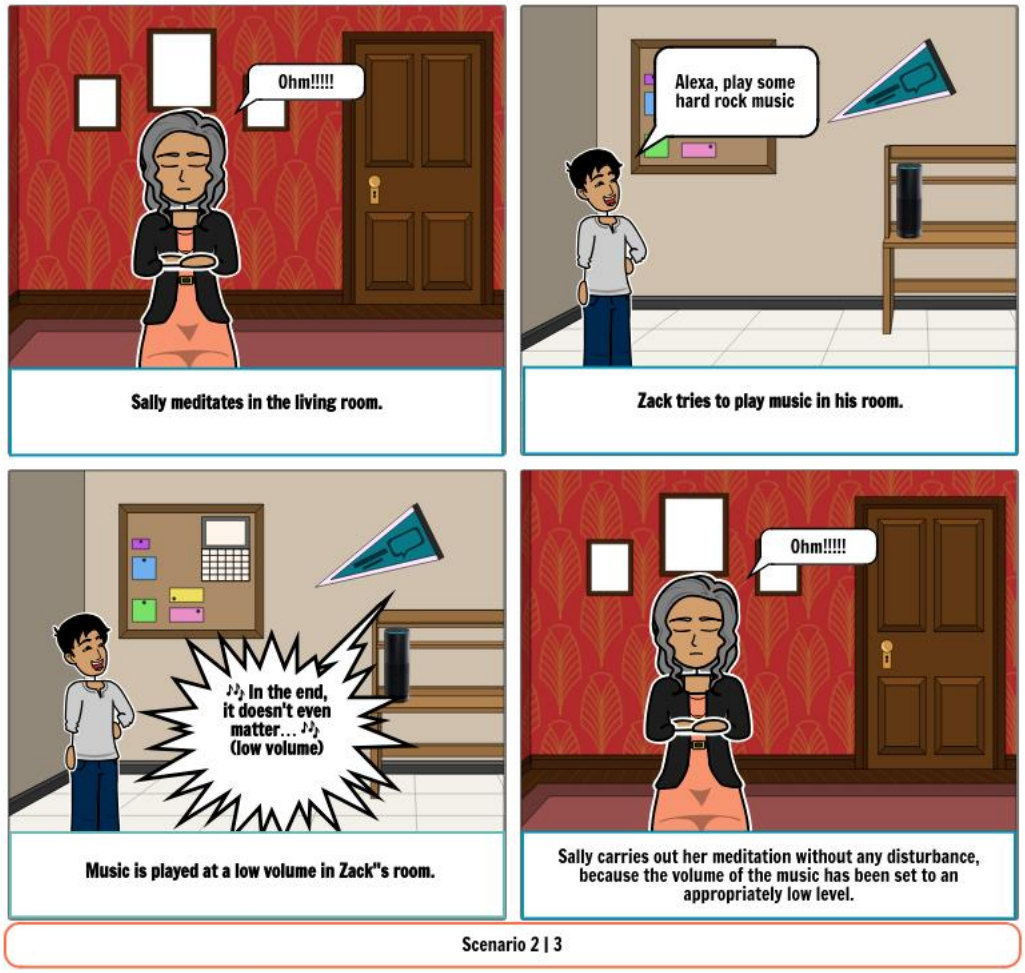

Figure 10.4: AAUI Disturbance Scenario Storyboard

Figure 10.5: NAUI Disturbance Scenario Storyboard

10.3.2 Questionnaire (s)

10.3.2.1 Pre-interview Questionnaire

Adaptive UI Pre Study Questionnaire Version 1.0 (01/11/2019)

Participant ID _____

Please fill this in before you engage with the simulated smart home scenarios.

Age –

Gender –

Do you use any smart home devices? If yes, please list them below

---

10.3.2.2 Usability Questionnaire

Please fill this in after you have finished reading a scenario.

1) Pick a value from 1-5; 1 being strongly disagree and 5 being strongly agree.
   a) I think that I would like to use this system frequently: ……
   b) I found the system unnecessarily complex: ……
   c) I thought the system was easy to use: ……
   d) I think that I would need the support of a technical person to be able to use this system: ……
   e) I found the various functions in this system were well integrated: ……
   f) I thought there was too much inconsistency in this system: ……
   g) I would imagine that most people would learn to use this system very quickly: ……
   h) I found the system very cumbersome to use: ……
   i) I felt very confident using the system: ……
   j) I needed to learn a lot of things before I could get going with this system: ……

2) How effectively did the smart home user interfaces preserve the privacy of the smart home users? Please explain your answer.

3) If you have any comments or suggestions, please write them here:

10.3.2.3 Post-Study Interview Questionnaire

1. Could you explain the reasons for the usability ratings that you gave for the different scenarios?
2. Can you think of any other scenarios that violate privacy of users in a smart space?
3. What would you suggest to improve the usability and privacy protection capabilities of the smart home interfaces?

10.3.3 Quantitative Data

The study was conducted analysing privacy violation variations (information disclosure vs physical) and user interface variation (AAUI, CAUI and NAUI) by aggregating the results. The analysis was conducted for individual scenarios as well. Acronyms (-I and-P) have been appended to each user interface variation to denote the aggerated category. "-I" refers to information privacy, "-P" refers to physical privacy. For example, AAUI-I refers to the information privacy scenario with automatic adaptive user interfaces.

Participant_ID	AAUI-P	NAUI-P	CAUI-P	AAUI-I	NAUI-I	CAUI-I
1	92.5	75	90	90	77.5	77.5
2	75	50	72.5	67.5	40	67.5
3	65	65	75	65	50	50
4	45	87.5	75	82.5	50	67.5
5	100	42.5	62.5	72.5	82.5	60
6	92.5	80	100	100	82.5	95
7	95	60	87.5	92.5	55	87.5
8	100	92.5	92.5	97.5	85	82.5
9	97.5	85	97.5	67.5	72.5	95
10	100	95	100	100	97.5	100
11	90	90	100	57.5	57.5	72.5
12	97.5	97.5	90	97.5	85	77.5
13	90	57.5	100	100	62.5	90
14	50	52.5	37.5	77.5	45	27.5
15	87.5	80	100	90	62.5	90

Table 10.1: Summary of SUS scores

10.4 Appendix D: UX Evaluation Study

10.4.1 Study Resources

10.4.1.1 Consent form

Informed Consent Form (30/04/2020 Version 1.0)

Participant Identification Number: ----------

Consent Form

Title of Project: **Privacy Aware Adaptive User Interfaces in Smart Homes**

Name of Researcher: Akshika Wijesundara (akshika.wijesundara@open.ac.uk)

3rd party contact: Professor Andrea Zisman (andrea.zisman@open.ac.uk)

Department address: School of Computing & Communications, The Open University, Walton Hall Milton Keynes MK7 6AA UK

	Please initial all relevant boxes
1. I confirm that I have read and understand the information sheet for the above study (version 1.0, 30/04/2020).	☐
2. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.	☐
3. I understand that my participation is voluntary and that I am free to withdraw at any time without giving any reason. I understand that if I withdraw after the study period (31/08/2020) it may not be possible to delete my anonymised data if it has already been analysed for publication.	☐
4. I give consent to record the audio of our conversation during the study via Skype.	☐
5. I give consent to process the data (verbal and typed in answers) gathered during the study and to use them as anonymised quotations in presentations and publications.	☐
6 [OPTIONAL] I have provided an e-mail address and/or mobile phone number below so that the research team can send me updates relating to this study.	☐

7. **I agree to take part in the above study.** ☐

Name of Participant (please print)	Date	Signature
Participant e-mail address (optional)	Participant Mobile Phone (optional)	

10.4.1.2 Participant Information Sheet

Privacy Aware Adaptive User Interfaces in Smart Homes

Participant Information Sheet (Version 1.0,30/04/2020)
We would like to invite you to take part in our research study. Before you decide we would like you to understand why the research is being done and what it would involve for you. It should take about 5 minutes to read this thoroughly. If, after reading this information sheet, you think you may be interested in taking part you will have the opportunity to ask any questions before you agree to anything.

The aim of this study is to understand the user perception to adaptive user interfaces when used in protecting privacy of users in multi-occupancy environments. The study is conducted by Akshika Wijesundara, who is a PhD student studying usable privacy in cyber physical systems and a member of SEAD research group.

In order for you to participate in the study you should be more than 18 years old and should have good conversational English skills.

Summary
Our homes are becoming smarter by the day. We interact with our homes using user interfaces such as smart speakers, smart TVs and other types of smart home interfaces. While interacting with these user interfaces there is a risk of our privacy being violated as our interactions could leak information to other users in the vicinity. There is also the possibility of these interactions over public user interfaces disturbing other users in a smart home. This study involves my solution of

privacy aware adaptive user interfaces to protect privacy of smart home users while maintaining usability.
After reading this sheet and having any questions answered, if you would like to take part you will be asked to sign a consent form. The entire study (including the questionnaires) will take ~40-45 minutes to complete.

The interview would be conducted via a Skype call where only audio of the call will be recorded in order to be used in data analysis stage. First you will be given questionnaire to complete. This questionnaire consists of basic information about you and your perception with regard two types of privacy. Then you will be asked to watch four video prototypes depicting possible privacy violation scenarios in a smart home setting and user interface adaptations used in each scenario to mitigate those privacy violations. In the context of this study the term "video prototype" is referred to a video which simulates the novel user interface mechanism that has been proposed. These videos are recorded from a first-person point of view to simulate the environment around you. This was done in order to give the participant a realistic viewpoint of the smart home system. We would also like you to think out aloud (voice your thoughts) while you are watching the videos as this information would be useful for us in the data analysis stage. You will be given a questionnaire to complete after reviewing each scenario. At the end we will conduct a brief interview to understand your overall experience with the system.

You will be not compensated for participating in this study, but you would get the opportunity to experience some leading-edge research. There are no foreseeable risks arising from participation in this research, you will make a vital contribution to privacy aware adaptive interfaces in smart homes research and possibly improving the experience for others.

Your participation in the study is entirely **voluntary**, and you can choose to withdraw at any time without giving a reason. You also have the freedom to skip individual scenarios if you are not comfortable with them. You may also ask to have your data deleted at any time, although if we have analysed and combined your data with others' this may not be possible. Your data will be analysed within a period of one month from the date that you have participated in the study. After the period of one month, we are unable to delete your data as we would have anonymised the data in order to conduct the data analysis. The last date that you can withdraw your data is 31/08/2020.

The data collected will only be accessible to the named researchers on this study. Personally, identifying information will not be electronically stored with your data. Instead, a unique ID will be generated to record your data and we will ensure that you can never be identified by any data we publish.

The data will be retained for up to 5 years after the study. The results of this study may be published in a scientific journal. If you would like to receive the results of the study, you can indicate this on the consent form.

This research is in part being supported by a research grant from the Engineering and Physical Sciences Research Council and researchers from the Open University.

This research has been reviewed by the Open University's Human Research Ethics Committee and has been given a favourable opinion (REF HREC/3588/Wijesundara)

Please feel free to ask any member of the researcher team if you have any concerns or questions in relation to this study before agreeing to the Consent Form. You may also ask any questions throughout and after completion of the study.

You can contact the researchers as follows:
Akshika Wijesundara (Researcher): akshika.wijesundara@open.ac.uk (phone: 07754312540)
Prof Arosha Bandara (Supervisor): arosha.bandara@open.ac.uk
Prof Blaine Price (Supervisor): b.a.price@open.ac.uk
Prof Bashar Nuseibeh (Supervisor): bashar.nuseibeh@open.ac.uk

Thank you for taking the time to read this information sheet and considering taking part in this study

10.4.2 Questionnaires

10.4.2.1 Pre-study questionnaire

Privacy Aware Adaptive User Interfaces Pre-Study Questionnaire Version 1.0 (30/04/2020)

Participant ID _____

Please fill this in before you engage with the study.

Age –

Gender –

Do you use any smart home devices? If yes, please list them below
(E.g.: smart speakers (Amazon Echo, Google home etc.), smart TVs etc.)

Please consider the following statements and rate how concerned you would be with each incident.

Information privacy

Watch this video to understand the scenario - Link

If you were the person experiencing the scenario in the previous video, how concerned would you be with this type of a privacy violation?

Not Concerned at All				**Very Concerned**
1	2	3	4	5

Disturbance privacy

Watch this video to understand the scenario – Link

If you were the person experiencing the scenario in the previous video, how concerned would you be with this type of a privacy violation?

Not Concerned at All				**Very Concerned**
1	2	3	4	5

10.4.2.2 Post Scenario Questionnaire

Post Scenario - Questionnaire

Version 1.0 (30/04/2020)

Participant ID _____

Please explain what you saw in the video and describe your experience of the smart home.

--

Please underline the top five words which defines the “privacy aware adaptive user interfaces” in the video you reviewed last. Imagine you are the person who is experiencing the system.

Entertaining	Patronizing	Irrelevant	Predictable	Organised
Innovative	Impersonal	Poor quality	Effective	Inviting
Convenient	Trustworthy	Professional	Stressful	Confusing
Cutting edge	Annoying	Familiar	Straight Forward	Efficient
Essential	Flexible	Powerful	Dated	Exciting
Attractive	Approachable	Simplistic	Difficult	Clean
High quality	Complex	Engaging	Dull	Desirable
Unrefined	Comfortable	Time-consuming	Unpredictable	Intimidating
Inconsistent	Satisfying	Fast	Exceptional	Useful
Easy to use	Comprehensive	Inspiring	Overwhelming	Unattractive
Consistent	Advanced	Busy	Undesirable	Friendly
Relevant	Personal	Rigid	Helpful	Reliable
Unconventional	Creative	Collaborative	Ineffective	

Please explain why you picked those reaction cards?

--

Please consider the following statements and rate how much you agree with those statements.

1. Privacy aware adaptive user interfaces protect privacy of smart home users.

Strongly Disagree		**Don't agree or disagree**		**Strongly Agree**
1	2	3	4	5

2. I did not feel that I am in control while using the smart home

Strongly Disagree		**Don't agree or disagree**		**Strongly Agree**
1	2	3	4	5

3. I expected the user interface adaptation before it happened.

Strongly Disagree		**Don't agree or disagree**		**Strongly Agree**
1	2	3	4	5

4. If I were the person experiencing these user interface adaptations, I would not have accepted them.

Strongly Disagree		**Don't agree or disagree**		**Strongly Agree**
1	2	3	4	5

5. I understood why the user interface adaptations happened.

Strongly Disagree		**Don't agree or disagree**		**Strongly Agree**
1	2	3	4	5

6. User interface adaptation obstructed the user experience of using the smart home.

Strongly Disagree		**Don't agree or disagree**		**Strongly Agree**
1	2	3	4	5

10.4.2.3 Post-Study Semi Structured Interview Script

Version 1.0 (30/04/2020)

Overall, how do you feel about adaptive user interfaces being used in protecting privacy of smart home users?

_____

_____

Did any of these scenarios resonate with your daily activities? If the answer is yes, could you please elaborate?

_____

_____

Did any of these scenarios inspired you to think of other scenarios in your daily activities? If the answer is yes, could you please elaborate?

_____

_____

COVID-19 lockdown and working from home made us spend more time sharing our home with co-occupants. Has the current situation created any privacy violating scenarios that could have been avoided by adaptive user interfaces? Please elaborate on your answer.

_____

_____

10.4.3 Findings

10.4.3.1 Anticipating

10.4.3.1.1 Privacy Preferences

Users with varying privacy preferences: Two participants (N=2/23) highlighted how different users could have different privacy attitudes. PX19 highlighted how the smart home can adapt to different privacy attitudes of the users. *"…I do think that a lot of […] of people are more and more squeamish with what they want to share and not and how much they want to keep private? […] It's almost like getting to know where you where you live on that privacy range. And based on that, what kind of features you might be interested in",* (PX19[117]). PX10 stated that he is more concerned about the privacy of others in the smart home as oppose to his personal privacy. *"…So, there are things like my little girl running through, I might just not want them, my little girl just running through in her underwear. I just don't want them to have a screenshot on that.",* (PX10[119]). This reinforces the need for the interfaces of the smart home to adapt based on the context of use and privacy preferences of the occupants.

Privacy concerns with smart homes: Some of the participants (N=5/23) raised privacy concerns with smart homes. For example, PX13 felt uncomfortable interacting with the smart home as it was sensing the smart home users to operate in the background. *"… if it's a passive thing because it's checking on his smartphone that he's meditating. I don't know if I'm so […] comfortable with that.",* (PX13[118]). Five of the participants (PX10, PX11, PX13, PX15 and PX23) stated that they don't trust smart home devices due to privacy concerns. These concerns have led the users to minimise their interaction with smart home devices: *"... I don't have any smart devices in my house because […] it feels privacy invasive to me...",* (PX10[19]).

Lack of concern regarding real-time privacy control: A quarter of the participants (N=6/23) showed lack of concern over real-time privacy control: *"I do not feel that I'm in control, that I agree, but I don't care. Because it makes my life easier.",* (PX19[106]).

10.4.3.1.2 User's Other Preferences/Attitudes

Immaturity of smart homes: A couple of participants (N=2/23) was with the impression that smart homes are not matured enough. PX10 stated that AUI could be useful after smart homes become matured: *"it's just an idea that still is very early because this smart home stuff is still sort of in its infancy in a way. But I can see potential there and I do think it's worth considering this kind of stuff.",* (PX10[195]).

10.4.3.2 Connecting

10.4.3.2.1 Familiarity

AUI is novel: Four participants (N=4/23) stated that AUI is novel – e.g., *"I've never seen this kind of technology before. So, it seems very innovative, advanced and quite exciting...."*, (PX1[31]). PX7 highlighted the novelty of the privacy protection capability of the smart home AUI: *"It's something I haven't seen before, way of automatically protecting people's privacy while you're in a call."*, (PX7[150]). PX1 thought the use cases depicted in the study are novel: *"First of all, that was very cool. I would not have thought about that kind of a scenario"*, (PX1[116, 117]). Furthermore, PX1 was quite excited about the novel interaction affordances that it created for the user: *"Oh, well, I've never thought to this extent, what technology is capable of? Yeah, cuz all I think of to preserve privacy is to put headphones on. not listen to the music at all…"*, (PX1[69]).

AUI is strange: Three participants (N=3/23) found the AUI to be strange. PX16 stated that she found smart home's activity detection feature to be strange: *"I have no idea how the system got to know that someone is meditating. So that was a bit strange."*, (PX16[7]). PX6 and PX13 found the AUI's half blurring technology to be unfamiliar: *"…I found it that having only half of the screen blurred was a bit visually strange. […] my brain was processing it, was expecting that to happen, but I was instead betting that to happen fully blurred or having something on the person only, […] half of it may be kind of like surprised me."*, (PX6[45]).

10.4.3.2.2 Instant Positive Emotions

Impressed with AUI: A few of the participants (N=3/23) stated that they were impressed by the different features of the AUI. PX1 and PX7 were quite fascinated by the quick reaction times and predictive nature of it: *"but in some of the scenarios where a person was not in a room, it almost felt very like, like very predictive […] it happens so invisibly…"*, (PX1[182]). Furthermore, PX1 and PX2 stated that they were impressed about the adaptive blurring feature: *"I thought that was very innovative because I could choose to have my background shown, but at specific times, to just switch it on and off. And I think that's what I really like about this tool is that it's able to pre-empt those things."*, (PX1[203]).

10.4.3.3 Interpreting

10.4.3.3.1 Ease of Navigation

Multi-user support and accessibility: Some of the participants (N=5/23) stated that the AUI was supportive to any kind of a user, hence easier to use. Three participants (PX1, PX10 and PX23) mentioned that it was helpful to a differently-abled person: *"I think that's fantastic, especially for users with a disability who may not be able to verbalise commands. So, I think to preserve their privacy what was considered was fantastic."*, (PX1[119]). Furthermore, PX6 and PX15 told that it

enabled multiple smart home users: *"…was collaborative in a sense that both the people were able to achieve their task."*, (PX15[30]).

10.4.3.3.2 Unease of Navigation

The *unease of navigation* explores how participants found the AUI to be difficult to use. A few of the participants mentioned that AUI could have configuration overheads, and that the AUI is non-intuitive for specific scenarios. One participant also described a possible moral dilemma, making them think before continuing the interaction as it reminded them of the privacy violation.

Configuration overhead: A couple of participants (N=2/23) thought the AUI could have too much configuration overhead: *"…it's just one thing like Oh darn, I didn't forget to do it. It's one more thing you have to remember potentially to set up and you know…", (*PX10[135]).

Non intuitive: Three participants (N=3/23) thought the scenario where the main user opened a cupboard using a gesture was non-intuitive: *"I think unconventional. I'm not sure it feels like the [...] most intuitive way to open a cupboard […] I think there's quicker ways of doing this."*, (PX17[57]). It is important note that, this comment was specifically made for the scenario with the smart gesture (Table 6.1: OPN scenario). Therefore, it is not a generalisable finding.

10.4.3.3.3 Captivity

Privacy enforcement: Two participants (N=2/23) thought that the AUI enforcing the main user to take care of the co-occupant's privacy all the time can be a way of losing control. *"…it forced me not to disrupt them. So that would be my reasoning and I did not feel I'm in control while using this smart home..."*, (PX7[37])

Unclear mental model: Two participants felt they were not in control while using the smart home because they were not sure how the AUI worked. PX23 was uncertain of its activity recognition: *"…I did not feel that I'm in control, […] I do not know what a smart system perceives as studying…", (*PX23[133]).

10.4.3.3.4 AUI capabilities

Automation: Most of the participants (N=13/23) mentioned that the AUI automatically protected the privacy of the users: *"… I feel like I could just ask Alexa and I can rely on the fact […] if there's anyone to be disturbed that will be avoided because it will just take care of it for me…"*, (PX4[176]).

Timeliness: Quite a few participants (N=5/23) highlighted the timeliness of the AUI. PX15 stated that the AUI intervened at the right time to protect the privacy: *"he wanted to hear the music, but the technology told him to be mindful […] and taught him to be mindful and intervene at the right time or made a suggestion at the right time."*, (PX15[13]).

10.4.3.4 Reflecting

10.4.3.4.1 Conceptual Appreciation

Smart: Some of the participants (N=3/23) mentioned that the AUI was smart. PX6 thought adaptive blurring is a smart way to protect privacy: *"…it's a really smart way to do it. […] someone walking behind you, you blurred the screen…",* (PX6[73]). Furthermore, mentioned that an AUI infused home defines a smart home: *"…That's really smart. That's like what I would expect is smart home to be…",* (PX6[118]).

10.4.3.4.2 General Appreciation

In this context, *general appreciation* refers how participants expressed their satisfaction towards the AUI. Participants were impressed with it as well as reporting that they liked it.

Many of the participants (N=11/23) stated that they liked the AUI. PX1 stated that she really liked it as it was novel: *"…I really like it because it's something very new I haven't seen before…",* (PX1[178]). PX2 was appreciative of the AUI: *"I'm generally quite positive I think that the scenarios were quite good at demonstrating why you might actually want them...",* (PX2[222]). PX14 liked its automatic privacy protection: *"desirable as it did not compromise the password. there's no [Boss button?] […] I don't have to invoke anything. It's watching out for me...",* (PX14[63]). Furthermore, PX6 appreciated AUI's adaptive technology: *"…is a really a nice adaptive technology to use, that it / […] protect everybody, but […] it's not a blanket, it […] is adaptive towards something, like the person entering the room…",* (PX6[91]). Lastly, some of the participants mentioned that they were impressed (PX1, PX6, PX7, PX8, PX9, PX14 and PX21) with it. PX14 mentioned that the AUI was a brilliant way to handle the situation: *" I thought that was a brilliant way to handle it…",* (PX14[119]).

10.4.3.4.3 Value

In the context of this work, *value* refers to how participants evaluated the AUI's value. Participants highlighted the importance of the AUI and its research.

Some of the participants (N=5/23) stated that the AUI was essential. PX11 thought it was essential as it protected sensitive information: *"essential because it's a matter of preserving access to the service without disruption but also not forcing the user to expose secret information.",* (PX11[54]). PX8 thought it was essential as it was the only way they could interact with the system in certain situations: *"…essential and reliable in the sense that, well maybe this should be the only way of having, of allowing people to input their details, sensitive details…",* (PX8). A few of the participants (PX9, PX21 and PX21) highlighted the value of AUI research. PX9 thought AUI research is quite important: *"… I think these things are very nice to have, I think the most of these smart devices lack these kind of privacy protection mechanisms nowadays. I think what you're doing is really nicely.",* (PX9[178]).

10.4.3.4.4 Efficacy

AUI is effective: The majority of the participants (N=17/23(a)) stated that the AUI was very effective. Out of those participants, the majority (N= 13) highlighted that it protected information privacy. PX18 mentioned that in the scenario where the main user was watching Netflix when a co-occupant enters the room (Table 6.1: NFX scenario), it adapted to protect the privacy in a timely manner: *"...I think it happened timely, […] the second person thought that the person was watching something other than cartoons…"*, (PX18[241]). PX15 stated in the scenario where the main user was asking the smart speaker for health information when a co-occupant suddenly enters the room (Table 6.1: HLT scenario)that the AUI protected the privacy in an effective and seamless manner: *"...I think right at the time I could have revealed private information or even a message could have been have come, but other person enters then at that point of time the system adapted in a in a very seamless manner…"*, (PX15[99]).

Furthermore, most of the participants (N=12/23) stated that UI protected physical privacy as well. PX15 stated that it protected the physical privacy of the second user in the scenario where the co-occupant was meditating when the main user was trying to play music via the smart speaker (Table 6.1: MED scenario): *"from the secondary user's point of view, of course, this helped him to continue having his meditation and to have this non-disruptive environment and actually it preserves the privacy of the second person..."*, (PX15[13]). PX4 stated that it protected the physical privacy of the second user in the scenario where the main user was trying to access football news via the smart speaker (Table 6.1: FBL scenario): *"…the secondary user's point of view they only heard me asking Alexa for sports results and they weren't disturbed by the sports results…"*, (PX4[169]).Participants shared similar experiences on the effectiveness of the AUI in other scenarios that they were presented.

AUI is efficient: Some of the participants (N=5/23) found the AUI to be efficient. In the Netflix scenario (Table 6.1: NFX scenario), PX22 thought it was quite efficient in privacy protection: *"it was very efficient because then happened before the person entered. And probably the person didn't even realise that something happened again, from smart home point of view. So yeah, it was very efficient."*, (PX22[63]).

AUI enhances the UX: Three participants (N=3/23) mentioned that the AUI enhanced the user experience. PX14 mentioned that it enhanced the user experience as it protected the privacy of the users: *"I strongly disagree that it actually obstructed any part of the user experience, I think it enhances the user experience by preserving the privacy."*, (PX14[113]).

10.4.3.4.5 Ineffectiveness

Possibility to violate privacy: Two participants (N=2/23) stated that the choice based-AUI could be overridden to violate privacy. PX1 highlighted how the main-user has the ability to violate the physical privacy of the co-occupant: *"I thought that last option was interesting, where you give the*

user the option to actually listen to it out loud […] system it's not entirely restricting you? But it also contradicts the purpose of the software as well.", (PX1[97]).

10.4.3.4.6 Fairness

Reasonable: Four participants (N=4/23) found the AUI to be reasonable. PX4 mentioned that it was reasonable as it was consistent with his preference: *"I would have accepted them because they're totally reasonable given that the person is there. And this is the preference that I set"*, (PX4).

10.4.3.4.7 Enhance Relationships

Promoting mutual respect: A couple of participants (N=2/23) reported that the AUI promoted respect towards co-occupants and how it made the users mindful. PX2 highlighted how it made them compassionate and respectful towards other smart home users: *"…this is an adaptation that is like kind and caring and compassionate that you don't want to disturb your, your friend and so you're slightly inconveniencing yourself, or and the Smart Home is facilitating that. So that you can be respectful and kind to the other person..."*, (PX2[145]). PX15 reported that it made the main user mindful: *"…he wanted to hear the music but the technology told him to be mindful and […] intervene at the right time…"*, (PX15[13]).

10.4.3.5 Appropriating

10.4.3.5.1 Comparison

In the following section I report how participants compared the AUI with existing smart home devices. Participants identified AUI's features such as privacy protection, context sensing and personalisation to be better than existing smart home devices. Furthermore, they mentioned how AUI made them realise the improvements that needs to happen in existing smart home devices.

Privacy protection: Some of the participants (N=5/23) highlighted the AUI's capabilities to protect privacy compared to existing smart home devices. PX9 mentioned how his personal smart speaker is unable to protect his privacy as the AUI did: *"… most of these smart devices lacks these kind of privacy protection mechanisms nowadays …"*, (PX9[178]). Furthermore, PX2 and PX14 reported how the AUI's adaptive blurring technology is better compared to existing video conferencing tool's privacy. *"… there is a blur feature in Jitsi meet, you have to remember to turn it on. […] I think that while it's something I'd still accept, it's not as good as this…"*, (PX14[116]).

Personalisation: A couple of participants (N=2/23) highlighted the AUI's capabilities to personalise according to the user. PX7 highlighted how it was adapting according to the user where with the existing smart home devices, users adapt according to the device: *"…smart home interfaces are having increasing relevance, and maybe I already adapt my behaviour and the way I*

would use them. […] these kinds of interventions may increase the likelihood that I would use these kinds of interfaces at all times […] the system will adapt and protect my privacy.", (PX7[173]).

Context sensing: Two participants (N=2/23) compared the AUI's context sensing abilities with current smart home devices. PX9 stated that existing smart speakers are unable to detect context changes: *"…when […] some outside person is at my home, […] Alexa is not aware about those things...",* (PX9[52]).

General comparison: Some of the participants (N=4/23) reported that the AUI showed a gap in the existing Smart home research. PX21 stated that the AUI made him realise of the improvements required in the existing Smart home devices: *"…I just realised […]improvements that need to be made on these areas[…], like making smart environments really smart...",* (PX21[75]).

10.4.3.5.2 Impact on Self

In this section I report how the experience of the AUI impacted the participants. They reported the study made them aware of the interpersonal-cyber-physical privacy. Furthermore, they thought it gave them ideas on how to improve their lives and some of the participants mentioned that it increased the chance of them purchasing smart home devices in the future.

User-awareness of problems: A couple of participants (N=2/23) stated that the AUI made them aware of interpersonal-cyber-physical privacy violations: *"…to be honest, and now I've thought about these problems and they think you know, the problem is very interesting…",* (PX12[109]).

Improvement to life: A few of the participants (N=3/23) mentioned that the AUI inspired them on how to improve their lives. PX22 stated that it made them realise about existing problems in the Smart home and AUIs were a solution: *"… I never thought about these things to improve […], my experiences using smart home devices. …",* (PX22[82]).

Using in the future: A couple of participants (N=2/23) reported that they would like to use Smart home devices with AUIs: *"…these kinds of interventions may increase the likelihood that I would use these kinds of interfaces at all times…"* , (PX7[173]).

10.4.3.6 Recounting

10.4.3.6.1 Suggestions

Reversibility: Some of the participants (N=3/23) stated that the AUI should provide the ability to revert back or to customise the adaptation. *"…I would add the option to override it …",* (PX11[68]).

10.4.3.6.2 Adverse Effects of AUI

Restricting critical interactions: A couple of participants (N=2/23) highlighted the risk of AUI to critical interactions. PX23 thought it could block the main user's goal of getting medicine in a critical situation if there is a privacy violation: *"imagine a scenario where you're supposed to take the medications […] and now Alexa stops you from taking that medication at that time…"*, (PX23[11]).

10.4.3.6.3 Applicability and Beyond

In this section I report how participants thought the AUI could be applied in areas beyond smart homes. Participants thought it could be used in smart cars and a couple of participants highlighted AUI's commercial value in domains such as conference calling, legal and health section. Apart from that, a participant mentioned how an AUI can be used in online courts to mask witnesses identify where another participant mentioned how it could be used in a smart office setting.

Usage in smart cars: A couple of participants (N=2/23) stated that AUI can be used in smart cars. According to PX21 smart cars is a good use case for the PASHI framework due to smart technologies and multiple occupancies: *"…cars have smart assistants, voice assistants, and they display a lot of data and people share cars […] these kinds of things can really be relevant…"*, (PX21[69]).

Commercial value: A couple of participants (N=2/23) highlighted the commercial value of an AUI. P15 highlighted the commercial value of an AUI in the video conferencing domain: *"…Maybe Skype will buy the concepts…"*, (PX15[174]). PX14 thought it would be a great feature for the legal and healthcare professionals due to its ability to protect privacy: *"…I'm working with legal and health professionals […] there's a lot of things that would probably benefit from the tenets of what you're presenting here…"*, (PX14[139]).